United States of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 117th CONGRESS, FIRST SESSION

Vol. 167 WASHINGTON, THURSDAY, NOVEMBER 18, 2021 No. 201

Senate

The Senate met at 10 a.m. and was called to order by the Honorable JACKY ROSEN, a Senator from the State of Nevada.

PRAYER

The Chaplain, Dr. Barry C. Black, offered the following prayer:

Let us pray.

O God our Father, we want to serve You as You desire. Lord, make us alert to the needs of those You seek to touch, providing us with opportunities to transform hurting people.

Use our lawmakers to do Your will on Earth as You empower them to be ambassadors of reconciliation. Lord, give them such winsome dispositions that they will bless even those who are hard of heart and withered in spirit. May our legislators comfort those who are brought low by sorrow and lift those who are bowed by life's burdens.

Lord, during this season of Thanksgiving, inspire each of us to be grateful every day.

We pray in Your precious Name. Amen.

PLEDGE OF ALLEGIANCE

The Presiding Officer led the Pledge of Allegiance, as follows:

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one nation under God, indivisible, with liberty and justice for all.

APPOINTMENT OF ACTING PRESIDENT PRO TEMPORE

The PRESIDING OFFICER. The clerk will please read a communication to the Senate from the President pro tempore (Mr. LEAHY).

The senior assistant legislative clerk read the following letter:

U.S. SENATE,
PRESIDENT PRO TEMPORE,
Washington, DC, November 18, 2021.

To the Senate:

Under the provisions of rule I, paragraph 3, of the Standing Rules of the Senate, I hereby appoint the Honorable JACKY ROSEN, a Senator from the State of Nevada, to perform the duties of the Chair.

PATRICK J. LEAHY,
President pro tempore.

Ms. ROSEN thereupon assumed the Chair as Acting President pro tempore.

RESERVATION OF LEADER TIME

The ACTING PRESIDENT pro tempore. Under the previous order, the leadership time is reserved.

CONCLUSION OF MORNING BUSINESS

The ACTING PRESIDENT pro tempore. Morning business is closed.

LEGISLATIVE SESSION

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022—Motion to Proceed—Resumed

The ACTING PRESIDENT pro tempore. Under the previous order, the Senate will resume consideration of the motion to proceed to H.R. 4350, which the clerk will report.

The senior assistant legislative clerk read as follows:

Motion to proceed to Calendar No. 144, H.R. 4350, a bill to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

RECOGNITION OF THE MAJORITY LEADER

The ACTING PRESIDENT pro tempore. The majority leader is recognized.

NATIONAL DEFENSE AUTHORIZATION ACT

Mr. SCHUMER. Madam President, on NDAA, last night, the Senate began the process to debate, amend, and ultimately pass our annual Defense spending bill. With Republican cooperation, we can adopt the motion to proceed and begin voting on amendments early today.

Let me say it again. With Republican cooperation, we can adopt the motion to proceed and begin voting on amendments today. We should work together and complete this important bill before the Thanksgiving holiday.

Last night's vote was overwhelmingly bipartisan, so there is no reason we can't come to an agreement very soon to begin debating amendments.

And there is already one important amendment that I want to mention: repealing the 2002 Iraq AUMF. This bipartisan measure was reported out of the Senate Foreign Relations Committee earlier this year, and I said months ago that the Senate should hold a vote on it. The NDAA is a logical place to do so.

The Iraq war has been over for over a decade. An authorization passed in 2002 is no longer necessary for keeping Americans safe in 2021. It has been nearly 10 years since this particular authorization has been cited as a primary justification for a military operation, and there is a real danger to letting these legal authorities persist indefinitely. Repealing this AUMF will in no way hinder our national defense, nor will it impact our relationship with the people of Iraq.

I want to thank Chairman MENENDEZ, Senator KAINE, Senator YOUNG, and every Republican and Democratic cosponsor of the bill for working to bring this issue to the floor. And in the coming days, I hope we can come to an agreement on other commonsense amendments to strengthen the Defense bill so we can get it passed through the Senate as soon as possible.

BUILD BACK BETTER AGENDA

Madam President, on Build Back Better, now that President Biden has enacted his once-in-a-generation infrastructure bill, Democrats are taking the next steps toward passing the rest of his Build Back Better plan.

● This "bullet" symbol identifies statements or insertions which are not spoken by a Member of the Senate on the floor.

Printed on recycled paper.

The last year and a half have been unlike any in modern U.S. history. We have had a once-in-a-century pandemic, followed by the worst economic crisis since the Great Depression.

We have come a long way this year as we have lifted our country out of the depths of these crises, but the challenges, of course, aren't over.

Americans right now want us to lower costs for things like healthcare, prescription drugs, childcare. We have a responsibility to pass legislation that will cut costs and improve American lives. That is why we need to keep working on passing Build Back Better. We know that passing this critical legislation will lower costs for some of the most basic and essential things in everyday life. And as economists from leading rating agencies said yesterday, Build Back Better will not add to the inflationary pressures in the U.S. economy.

The childcare provision could alone save families thousands of dollars each year. Families, on average, spend $10,000 annually on childcare for each child under 4. A generation ago, this was unheard of. Build Back Better will dramatically lower costs for millions of families by providing the largest investment in childcare in American history.

The same goes for prescription drugs. If you are one of the roughly 10 million Americans who relies on insulin to manage your diabetes, chances are you have been spending more and more as the cost of this once-affordable drug has skyrocketed. It is truly one of the perplexing and frustrating trends of the past two decades.

Well, Build Back Better will make it so Americans with diabetes don't pay more than $35 per month on insulin by enabling Medicare to directly negotiate prices in Part B and Part D—again, lowering costs, improving the lives of millions of families.

Examples go on and on of how people will have more money in their pocket given their expenses.

Build Back Better cuts taxes for parents raising kids. It makes pre-K universal for the first time ever. It will provide help for small businesses to invest within the United States and hire American workers.

And, ultimately, it is the best thing we can do to recapture that sunny American optimism that has been the key to our country's success. Creating jobs, lowering costs, fighting inflation, keeping more money in people's pockets—these are things Americans want and what Americans need, and it is what BBB does.

We are going to keep working on this important legislation until we get it done.

NOMINATION OF DILAWAR SYED

Madam President, now, on a much sadder note, Mr. Syed.

The Republican fixation on blocking qualified, uncontroversial, and essential nominees to fill roles in the Biden administration has hit a new and shameful low.

Yesterday, every single Republican on the Small Business Committee boycotted a hearing that would have held a vote on Dilawar Syed's nomination for the No. 2 spot at the Small Business Administration.

If confirmed, Mr. Syed would be the highest ranking Muslim American in government. This is the fifth time—the fifth time—that Republicans have failed to show up to a committee hearing for Mr. Syed.

To date—to date—we have yet heard a single legitimate reason for their opposition. At one point, some of my colleagues seemed to question Mr. Syed's allegiance because of his affiliation with a Muslim voter education group. That is repugnant, and after those objections provoked fierce criticism, Republicans came up with entirely new fabrications for their resistance.

But at no point have Republicans explained why Mr. Syed is not qualified for the job. Frankly, they can't because Mr. Syed is the definition of a qualified candidate. His nomination has been praised by hundreds of business groups, including the U.S. Chamber of Commerce, hardly a liberal crowd.

It is shameful; it is unacceptable; it is ridiculous for Republicans to keep stalling on Mr. Syed's nomination. He is eminently qualified to serve in the SBA.

Why are Senate Republicans opposing Mr. Syed's nomination? And let me ask this again because the question resonates. Why are Senate Republicans opposing Mr. Syed's nomination?

I ask my Republican colleagues to drop their resistance and allow this excellent and straightforward nominee to receive confirmation.

I yield the floor.

I suggest the absence of a quorum.

The ACTING PRESIDENT pro tempore. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. MCCONNELL. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

RECOGNITION OF THE MINORITY LEADER

The minority leader is recognized.

NATIONAL DEFENSE AUTHORIZATION ACT

Mr. MCCONNELL. Well, at long last the Senate will officially turn to the NDAA. Every day, world events remind us that America faces serious rolling threats. In too many cases President Biden's decisions have actually made things worse, so our annual opportunity for the Senate to have its say is as important this year as it has ever been.

Over in Russia, Putin is preparing to escalate military hostilities along the border with Ukraine, and he is using Europe's reliance on natural gas to bully our friends. But President Biden actually removed obstacles to Putin's brandnew pipeline that will further extend his leverage and further enrich his cronies.

So I hope the Senate will consider an NDAA amendment to sanction this project and to provide additional lethal support to Ukraine. These initiatives have previously won bipartisan support, so I would hope Democrats would join Republicans in pushing back on Moscow.

China is flaunting major military innovations, like hypersonic weapons systems, stepping up airspace intrusions over Taiwan, and blaming America for their bad behavior. But while President Biden and our colleagues like to talk a good game about China, they have yet to really walk the walk. President Biden's budget request for our military and defense does not even keep pace with President Biden's inflation.

In addition, while Russia openly threatens its neighbors and China builds up its conventional and nuclear forces, there are reports that Democrats are considering unprecedented new constraints on America's own nuclear options through a ''no first use'' or ''sole purpose'' policy.

Our allies have strong concerns about this. I hope the Senate will use the NDAA process to demonstrate bipartisan support for finally modernizing our nuclear triad. That is the bedrock of deterrence and our strongest defense against these serious threats.

So, what about terrorism?

Following President Biden's Afghanistan disaster, we are facing new and growing threats there as well. The new Taliban government has made cabinet ministers out of terrorists whom the Obama-Biden administration let out of Guantanamo Bay. But the Biden-Harris administration still naively acted like these characters care one bit about international norms.

That is why Republicans have an amendment to ensure that none of the funding for Afghanistan aid can flow to the Taliban. It is an indictment of President Biden's policy that such an amendment is even necessary, but yet that is where we are.

In the Middle East, Iranian-backed terrorists are rampaging from Yemen to Iraq to Syria. They are emboldened as our deterrence has eroded. Given the multiple attacks on U.S. forces and facilities, we are fortunate more Americans haven't been killed. It may only be a matter of time before we see U.S. casualties at the hands of Iranian-backed terrorists.

However, in the wake of these growing threats, Democrats want to use the NDAA—a bill that should strengthen our national defense—as an occasion to weaken the authorities that support our military's presence and operational flexibility by repealing the 2002 AUMF. I expect a robust debate about that.

I am glad we will finally be able to have these debates and these votes. America needs a course correction, and the Senate needs to supply it.

THE ECONOMY

Madam President, on an entirely different matter, American families are

dealing with painful inflation every single day. They have been fighting this daily battle for months now.

A few months ago, a grandfather raising four grandkids in Missouri told reporters he had to cancel summer camp for his 8-year-old and his 6-year-old in order to keep affording diapers for their twin younger brothers.

One Maryland woman told the local news she had gone to the grocery store to buy meat for her family, but was turned away by the pricetag and had to leave with a $2 loaf of bread instead.

One man in Massachusetts, who cares for his elderly mother, told reporters that his 94-year-old mom needs the house kept warm, so they are getting absolutely crushed—crushed—by runaway heating costs. Here's what he had to say about it:

> Before, you'd go to the store, and if you had a $100, you could buy four bags of groceries and be happy. Now you are lucky to get a bag. Milk, orange juice, eggs. Plus the oil for the house, the water bills. It's just crazy. It's so much money. How is someone supposed to survive?

This persistent and painful inflation has been directly fueled by the reckless spending spree that Democrats rammed through in March. Even if Washington Democrats didn't inflict more new damage, economists still say ''we're going to see inflation get worse before it gets better.''

The Democratic leader said on March 12: ''I do not think the dangers of inflation, at least in the near-term, are very real.''

He was catastrophically wrong. And these same people want yet another multitrillion-dollar bite at the apple.

Look, American families know the spending part of Democrats' reckless tax-and-spending spree would spell disaster. Sixty-seven percent just told a survey that Washington should cut back on printing and spending because of inflation and rising costs.

And then there is the taxing part of their reckless taxing-and-spending spree. The bill that Democrats are writing behind closed doors would hike taxes on the American people by an estimated $1.5 trillion—a trillion and a half dollars in tax increases.

Democrats have already turned a strong economy into a shaky economy. Now they want to add the biggest tax hikes in a generation. A huge chunk of that is hundreds of billions of dollars for tax hikes on American industries and employers, because the Biden administration has become enamored with a global scheme where countries around the world supposedly all agree to hike their tax rates together.

This is an awful idea. Remember, in 2019, Republican policies had set up the best economy for working Americans in a generation. This is in large part because we just cut taxes substantially. We made America a more attractive place to do business.

So President Biden wants to do just the opposite of that: thrust America into some kind of global noncompete agreement. We are supposed to promise Europe and Asia that we won't make America an especially attractive place to bring jobs and prosperity.

Let me say that again. We are in the process of promising Europe and Asia that we won't make America an especially attractive place to bring jobs and prosperity.

Look, it gets worse. President Biden and Secretary Yellen want America to leap over the cliff first, tax the heck out of American industries while we just wait and see if our competitors actually follow suit.

Well, you better believe China would be just thrilled to see the Democrats' bill drain hundreds of billions of dollars out of our own private sector as a symbolic gesture to the rest of the world.

Democrats' tax policies are just like their energy policies. They won't build back better. They will build back Beijing. They won't build back better. They will build back Beijing.

This is just one part of a $1.5 trillion job-killing tax hike. There are all kinds of tax increases that would hit major employers, Main Street small businesses, and American families. Nonpartisan experts have confirmed the Democrats' bill would completely break the President's promise not to raise ''a single penny more,'' he said, in taxes on middle-class households.

They even want to send tens of billions in extra funding to the IRS so they can hire an army of new agents to snoop and audit their way across the country. But less than 3 percent of the huge IRS windfall would fund better customer service for taxpayers.

Finally, in the midst of all these tax hikes, Democrats from New York, New Jersey, and California have managed to include—listen to this—a massive tax cut for wealthy people who choose to reside in high-tax blue States. This bonanza for blue State millionaires and billionaires would cost almost $300 billion on its own.

Even the Washington Post could only marvel at the audacity of this. Here's their headline: ''The second-biggest program in the Democrats' spending plan gives billions to the rich.'' That is the Washington Post's assessment of it.

In fact, even though Democrats want to hike taxes by $1.5 trillion, their bill still manages to give a net tax cut to 89 percent of people making between $500,000 and $1 million, and 69 percent of households making over $1 million.

This bears repeating. Even though Democrats want to hike taxes by $1.5 trillion, their bill still manages to give a net tax cut to 89 percent of people making between $500,000 and $1 million, and 69 percent of households making over $1 million.

All of this is a huge blow to American competitiveness: job-killing tax hikes. But Democrats make sure to look out for the ultrawealthy out on the coasts. A supermajority of them get tax cuts. I am almost impressed our colleagues have found a way to be this out of touch.

I suggest the absence of a quorum.

The ACTING PRESIDENT pro tempore. The clerk will call the roll.

The senior assistant bill clerk proceeded to call the roll.

Mr. THUNE. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

BORDER SECURITY

Mr. THUNE. Madam President, the Biden border crisis continues to rage. Last month, U.S. Customs and Border Protection encountered 164,303 individuals attempting to illegally cross our southern border. That is more than twice the number of encounters Customs and Border Protection had the previous October and the highest October number ever recorded by Customs and Border Protection. In all, more than 1.7 million migrants were apprehended attempting to cross our southern border in fiscal year 2021—the highest number ever.

We are in the midst of a very serious crisis, and the response from Democrats and the administration? Well, mostly crickets. Democrats seem to hope that ignoring the border situation will make it go away or at least ensure that no one pays attention. I am pretty sure the President and his administration spent more time earlier this year fighting against the use of the word ''crisis'' to describe the situation at the border than they did actually thinking about how they might deal with the influx. Apparently, the administration is still—still—trying to avoid the ''crisis'' label judging by a recent hearing wherein the President's nominee to head Customs and Border Protection seemed to carefully avoid referring to the situation at the border as a ''crisis.''

If the highest number of border encounters ever recorded isn't a crisis, I am not sure what is. The situation at our southern border is out of control. It is a security crisis, it is a manpower and enforcement crisis, and it is a humanitarian crisis—although, again, you would never guess it from the Democrats' behavior.

Despite the fact that this crisis has been raging for the best part of a year now, Democrats and the administration have taken essentially no meaningful action to address the situation, and that is not the worst of it. The Democrats' policies are actually making the situation worse.

Among other things, the President has significantly limited the ability of Immigration and Customs Enforcement and Customs and Border Protection to enforce immigration laws, and arrests in the interior of the country dropped steeply under this administration. The Washington Post recently reported:

> Immigration arrests in the interior of the United States fell in fiscal 2021 to the lowest level in more than a decade.

The practical effect of the President's immigration policies has been to encourage new waves of illegal immigration. It is hardly surprising. If you think that your chances of staying in the United States are good, even if you are here illegally, you are likely much more inclined to undertake the journey in the first place.

The administration's actions—or lack thereof—have been compounded by the actions of Democrats in Congress who have been doing their best to guarantee widespread amnesty. Democrats have repeatedly attempted to include some form of amnesty in their tax-and-spending spree. While they have been partially foiled by the rulings of the Senate Parliamentarian, the latest version of their bill still contains provisions to grant de facto amnesty to many illegal immigrants.

Their spending spree also deliberately lacks restrictions on Federal funding going to individuals in the country illegally, which means that illegal immigrants could end up receiving the $3,000-per-year child allowance, housing vouchers, and more. One analysis suggests that illegal immigrants could collect $10.5 billion in child allowance payments next year.

I haven't even mentioned reports that the Biden administration has apparently been contemplating settling lawsuits brought by individuals, who came here illegally, with payments of up to $450,000 per person—$450,000. That is right. That is more than four times as much as the government gives to the families of soldiers killed in action and nine times—nine times—as much as the government gives to an individual wrongly imprisoned for 1 year. The administration has suggested that payments will not actually be that high, but even a settlement half that size would dwarf the payments that we give to the families of fallen soldiers.

Immigrants have helped make this country what it is today, and I am a strong supporter of legal immigration, including temporary worker visas, like H–2B visas, which help South Dakota employers and many others address hiring challenges, but, again, immigration has to be legal. Encouraging illegal immigration, as the Democrats are doing, presents a serious security risk because it makes it easier for everyone from terrorists to drug traffickers to enter the country unidentified, to say nothing of drugs like fentanyl and other illegal items.

Encouraging illegal immigration through lax immigration enforcement and amnesty also undermines respect for the rule of law. The area of immigration should not be an exception to the principle that the law has to be followed and respected. Yet that is basically what Democrats' policies are saying—that the law doesn't matter when it comes to immigration.

Finally, we need to get away from any idea that there is anything compassionate about policies that encourage individuals to come here illegally. Attempting to enter the country illegally is fraught with danger, from natural perils like weather, disease, and exposure, to exploitation by smugglers and traffickers. Amnesty and lax enforcement policies encourage thousands more individuals and families to expose themselves to the dangers of an illegal border crossing.

President Biden and Democrats could help stem this crisis right now by making it clear that immigration law will be enforced and that the only acceptable way to enter the United States is to come here legally. Unfortunately, it seems much more likely that the President will continue to ignore this crisis and deemphasize immigration enforcement while Democrats in Congress will continue to push for amnesty. It is a serious failure of responsibility on the President's part and one that will continue to have serious and sometimes deadly consequences.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. BOOKER). The clerk will call the roll.

The senior assistant bill clerk proceeded to call the roll.

Mr. DURBIN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

THE GETTYSBURG ADDRESS

Mr. DURBIN. Mr. President, it was 158 years ago tomorrow that Abraham Lincoln delivered what I believe was the greatest speech ever uttered by an American. He had been asked to say ''a few words'' at the dedication at the Soldiers' National Cemetery in Gettysburg, PA.

Four months had passed since the great armies of the North and South had clashed on that hallowed ground. They had fought for 3 days in the searing July heat. When the slaughter finally ended, the battlefield lay covered with the bodies of 50,000 dead and wounded soldiers and officers. It was the bloodiest battle in the hellish Civil War.

What good could come from butchery and sorrow? What great purpose had been worth such staggering loss? Those were the questions which Abraham Lincoln pondered on his train ride to answer in Gettysburg.

He spoke for less than 3 minutes—just 272 words. In those 3 minutes, he redefined the war as not a battle for territory or property, but for human dignity and human equality.

He gave us a profound, simple, new definition of democracy: ''Government of the people, by the people, and for the people.'' He said the fallen soldiers had done all they could do. They had given their ''last full measure of devotion'' to ensure democracy did not perish from this Earth.

Now, Lincoln said, it was left to us, the living, to ''advance their unfinished work''—in his words, to salvage from all of that death a new birth of freedom.

He said that our Civil War was testing ''whether a nation, conceived in liberty, and dedicated to the proposition that all men are created equal . . . can long endure.''

Can our democracy endure? It is a question that Lincoln pondered not just at Gettysburg but throughout his life.

Twenty-five years before Gettysburg, he had considered that question in a speech at the Young Men's Lyceum in Springfield, IL. He was a young lawyer and a newly elected State legislator, just 29 years old.

It was a challenging time in America, as it is today. Anxiety was high following a stock market panic the previous year. There was growing violence in America. Abolitionists were being killed by pro-slavery defenders. Blacks and others were being lynched with alarming frequency in the South. Lincoln feared that what he called ''the justice of the mob'' might replace the rule of law. Sound familiar?

In a time of such anxiety, he questioned whether people might elect a despot who would use his power to tear down the institutions of our democracy, rather than preserve them.

In his most famous passage, he warned that if American democracy were ever to perish, ''it must spring up amongst us; it cannot come from abroad. If destruction be our lot, we must ourselves be its author and finisher.''

I heard those words quoted by a thoughtful Member of the House of Representatives on the night of January 6, 2021, after the mob that attacked this Capitol had gone and Congress had returned to complete our duty to certify the electoral ballots and declare Joe Biden the President of the United States.

The weapons and military programs that we will debate in the coming days are important. They are essential to protect America. But weapons alone cannot save us if we don't understand what we are fighting to defend. There is only one sure way to preserve American democracy, Lincoln told us. We must know our history. We should study the Declaration of Independence and the Constitution, he said, as if they were a Bible, so that we revere the principles upon which our democracy is built.

Our democracy can't survive if we reject the great proposition for which so many died at Gettysburg: that all people are created equal. Our democracy cannot survive if we abide by the rule of law only when it suits us. And it will not endure if we see each other as enemies rather than as friends and citizens of one Nation that we all love.

We have seen a demonstration of that particular issue this week in the House of Representatives.

In his book, ''Lincoln at Gettysburg,'' Garry Wills wrote that ''Up to the Civil War, the United States was referred to as a plural noun. 'The United States are a free country.' After

Gettysburg, it became singular, 'The United States is a free country.'''

As it says above your head, Mr. President, ''e pluribus unum.''

As we look forward to celebrating our national holiday of Thanksgiving, perhaps we could try a little harder to hear the ''mystic chords of memory''—what a phrase—that unite us.

I think about that Gettysburg Address, and I was asked to give a speech about the Gettysburg Address at Gettysburg many years ago. I tried to set out whatever I had to say in 272 words. I think I did a fair job, but I would give myself a passing grade, at best. But it was a complete shock to my audience when I stopped at 272 words, and Lincoln said that a speech doesn't have to be eternal to be immortal.

In our lives as public servants, we are called on to speak very often. And I am reminded, time and again, the impact that Lincoln had with so few words, to capture the moment, to give people hope, and to craft phrases which still endure to this day as some of the most masterful uses of the English language one can imagine.

Tomorrow, I hope we can take a moment to recall our childhood education, when we were taught the Gettysburg Address and perhaps recite what we can of it. And I hope we will remember, even in these dark times, that we have faced harder times than this and we were delivered and this Nation endured.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

Mr. REED. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

NATIONAL DEFENSE AUTHORIZATION ACT

Mr. REED. Mr. President, I rise to discuss the fiscal year 2022 National Defense Authorization Act.

Over the coming days, the Senate will consider this bill, which the Armed Services Committee passed by a broad bipartisan margin of 23 to 3 in July.

I look forward to debating and improving this bill, as we all work toward ensuring our military has the right tools and capabilities to combat threats around the globe and keep Americans safe.

First, I would like to acknowledge Ranking Member INHOFE, whose leadership on this committee and this body has been invaluable. His commitment to our men and women in uniform is unwavering, and he was instrumental in helping to produce this bipartisan legislation.

As we debate the NDAA, we must keep in mind that the United States is engaged in a strategic competition with China and Russia. These near-peer rivals do not accept U.S. global leadership or the international norms that have helped keep the peace for the better part of a century.

This strategic competition is likely to intensify due to shifts in the military balance of power and diverging views of governance. And it is unfolding amidst climate change and the emergence of highly disruptive technologies.

The interconnected nature of these threats will drive how we transform our tools of national power to respond. The passage of the FY2022 NDAA will be a critical step in meeting the complex challenges before us.

Turning to the specifics of this year's Defense bill, the NDAA authorizes $740 billion for the Department of Defense and $27 billion for national security programs within the Department of Energy.

For the first time in years, this legislation, like the President's budget request, does not include a separate overseas contingency fund, or OCO, request. Any war-related costs are included in the base budget.

This bill contains a number of important provisions that I would like to highlight.

To begin, we have a duty to ensure that the United States can outcompete, deter, and prevail against near-peer rivals. The NDAA supports the Department of Defense in this endeavor by providing the resources needed by the combatant commanders to carry out the national defense strategy, or NDS.

Every 4 years, the Department reports the NDS to outline the national security objectives of the administration. The 2018 NDS provided a framework, and the DOD will release a new strategy in the coming months.

In this regard, this bill creates a commission on the national defense strategy for the forthcoming NDS in order to boost our military advantage. Last year, the Armed Service Committee created the Pacific Deterrence Initiative—or PDI—to better align DOD resources in support of military-to-military partnerships to address the challenges posed by China.

This year's bill extends and modifies the PDI and reiterates the committee's intent to improve our force posture in the Indo-Pacific, to increase readiness and presence, and to build the capabilities of our partners and allies to counter these threats.

Future investments under PDI should focus on military and nonmilitary infrastructure in the Indo-Pacific region. This will assist in distributed military operations, and it will be more effective in countering predatory Chinese infrastructure development practices.

The bill also requires the Secretary of Defense to provide recurring briefings on efforts to deter Chinese aggression and military coercion. It compels a briefing on the advisability and feasibility of increasing United States defense cooperation with Taiwan. It is important we help Taiwan improve its overall readiness and acquire asymmetric capabilities most likely to make the Chinese Government question their ability to take the island by force.

I want to emphasize, however, that our Nation's ability to deter China cannot be based on military might alone. We must strengthen our network of allies and partners, which will be essential to any strategy for the Indo-Pacific region. We must also ensure that, as we shift our focus to the Indo-Pacific, we do not lose sight of priorities in other areas, like Europe.

This year's bill authorizes the continuation of the European Deterrence Initiative—or the EDI—recognizing the continued need to invest in support for our European allies and partners as we work toward the shared goal of deterring Russian aggression, addressing strategic competition, and mitigating shared security concerns, the most recent one being the amassing of Russian troops on the border of Ukraine.

Turning to personnel, the key factor that makes the United States the greatest military power in the world is its people. We need to ensure that our uniformed personnel know every day how much we appreciate what they do and that we have their backs.

Congress has done a good job in providing benefits to the military and their families, and this year's Defense bill continues to do that. But our military is showing the strain of two decades of continuous deployments, and I am concerned that there has been a dangerous erosion of trust within the chain of command; and issues such as racism, extremism, sexual harassment, and sexual assault have been allowed to fester and create friction and division.

The Department of Defense is addressing those issues, but Congress must provide guidance and resources. To this end, the bill strengthens the All-Volunteer Force and improves the quality of life of the men and women of the total force: the Active Duty, the National Guard, and the Reserves; their families; and, importantly, the Department of Defense civilian employees, who contribute significantly to the effectiveness of our operations.

It reinforces the principles of a strong, diverse, inclusive force and that force cohesion requires a command climate that does not tolerate extremism or sexual assault misconduct or racism; and that quality healthcare is a fundamental necessity for servicemembers and their families.

Importantly, this NDAA includes the funding necessary to support a 2.7 percent pay raise for both military servicemembers and the DOD civilian workforce. We have also included a provision that would amend the Military Selective Service Act to require the registration of women for Selective Service. I am proud of this position, which passed the Armed Services Committee on a broad bipartisan basis.

Society, the military, and the nature of warfare itself have evolved significantly since the 1948 Military Selective Service Act passed. Back then, women were denied the opportunity to serve in

combat roles and key leadership positions, and entire technologies and platforms didn't even exist.

Today, all military occupations, including combat roles, are open to women, and military success depends heavily on servicemembers with advanced education and technical skills in STEM, cyber, medicine, languages, and more.

To be clear, I am hopeful that we will never have to draft again. If we do, however, it will be under circumstances so dire and existential that to voluntarily choose to enter the fight with anything less than our very best would be supremely foolish and potentially fatal. If we are going to have a Selective Service System, women must be a part of it. Basic equality and military readiness demand parity between the sexes to protect our country and uphold our values. In the meantime, it is time to end outdated sex discrimination and remove it from official policy and Federal law.

The bill also creates a new category of bereavement leave for military personnel that would permit servicemembers to take up to 2 weeks of leave in connection with the death of a spouse or a child. Similarly, in an effort to provide greater care and support to our military men and women, it increases parental leave to 12 weeks for all servicemembers for the birth, adoption, or foster care placement of a child. It establishes a basic needs allowance to ensure that all servicemembers can meet the basic needs of their families, and it requires parity and special and incentive pays for members of the Reserve and the active components.

In addition, I am proud that this bill makes historic changes to the military justice system to combat and discourage sexual assault and related misconduct within the military. Sexual assault is an unconscionable crime and a pervasive problem in the U.S. military and American society writ large.

When it comes to the military, one of the basic ethics is that one must protect your comrades and your subordinates; one cannot exploit them. Sexual assault and sexual harassment is an example of unconscionable exploitation, and it must be eliminated. We must take comprehensive action to halt sexual misconduct, hold offenders accountable, and support survivors. While the military has tried to stop sexual assault in the ranks, it simply hasn't been enough.

I commend President Biden, the Department of Defense, and the Independent Review Commission for their work on proposals, which we have considered during our markup and which are reflected in the bill. We will continue to work with the administration and the House to move toward enacting this momentous change.

Turning now to the areas of air, land, and sea power, with respect to our services, we have taken steps to improve their capabilities, their readiness, and their ability to fight and win.

This bill makes significant efforts to improve the readiness of the Navy and Marine Corps aircraft, ships, and weapons systems. It provides considerable investments in our next-generation Arleigh Burke-class destroyers, including an increase of $1.7 billion to restore a second guided missile destroyer to this year's budget and $125 million for long lead material for our destroyer in fiscal year 2023.

The bill authorizes $4.8 billion for the Columbia-class submarine program and for industrial-based development and expansion in support of the Virginia and Columbia shipbuilding programs, an increase of $130 million.

I was up at Quonset Point, RI, recently, where all submarines start their construction. Along with the Deputy Secretary of Defense, Secretary Hicks, we saw the progress that we are making to build two Virginia-class submarines a year and turning out the first Columbia-class ballistic missile ship to replace the Ohio class.

We are moving forward. And, frankly, many believe—as I do—that undersea strength is the best form of deterrence that we have. And as we deploy more submarines, we will have a greater ability to deter potential conflict.

This bill also increases the Landing Helicopter Assault replacement funding by $350 million and the Expeditionary Fast Transport vessel program by $270 million.

Growing our surface and undersea warfare capabilities will be vital to our success in the Indo-Pacific region, and this NDAA makes important progress in this area. It is consistent with our defense strategy of shifting our focus to the Pacific, which requires a shift of resources to the Navy and Marine Corps.

Similarly, the bill authorizes funding to strengthen naval aviation, including five additional F–35 fighter variants, one additional E–2D Hawkeye aircraft, two additional C–130J Hercules aircraft, an additional KC–130J tanker, two additional CH–53K helicopters, and two MQ–4C Triton unmanned aerial systems.

Now, with respect to the Air Force, the bill increases authorization funding by providing an additional F–35A fighter, five additional F–15 fighters, and extensions on the minimal capacity of several Air Force platforms.

With respect to the Army, I am pleased that the bill advances research and development in important future technologies and makes broad investments in generational Army modernization efforts and continues to upgrade significant enduring capabilities.

Our bill focuses on filling critical deficiencies and increasing investments in rapidly evolving demands. Further, it funds rapid development and fielding of land-based, long-range fires, including the precision strike missile, medium-range capability, and long-range hypersonic weapons.

It also provides funding for future long-range assault aircraft and future attack reconnaissance aircraft, increased funding for the future tactical unmanned aircraft system, and authorizes full funding for the AH–64 Apache attack helicopters and the UH–60 Black Hawk utility helicopters.

We are at a critical junction in a technological race with our near-peer competitors. We have enjoyed a technological lead over the last many decades. That lead is shrinking, and we have to not only develop the best of new technologies; we have to get them in the hands of our troops as quickly as possible. And that is what we are trying to do in this legislation.

Again, the issue is deterrence first, and what will help deter any conflict will be the realization of our adversaries that they are going up against the most sophisticated, technologically capable military in the world, manned by the most dedicated and skillful women and men in the world. That is what we are hoping to encourage.

Likewise, with respect to the Army, the bill supports the modernization of its ground combat vehicles, including the M1 Abrams tanks, Bradley Fighting Vehicles, Paladin self-propelled howitzer, tactical-type vehicles.

Having the platforms and the personnel is critical, but they have got to be ready to go, and we have taken great pride in trying to improve the readiness of our forces.

This NDAA authorizes more than $2.8 billion for additional military construction projects after funding other large projects in the budget request. This bill also includes a number of provisions that will help acquisition outcomes by strengthening the ability of DOD to analyze the defense industrial base, evaluate acquisition programs, and implement acquisition reform efforts.

It also streamlines processes to allow the Pentagon to invest in and incorporate advanced commercial technologies to support defense missions and strengthen DOD small business programs to allow partnerships with innovative, high-tech companies.

From post-World War II until very recently, we were really in an industrial age, and the United States led the world. We have now moved to a post-industrial age where the new technologies, the new innovations aren't coming out of government labs or the Bell Labs; they are coming out of small business; they are coming out of young people who have come up with great ideas.

And what we want to do and what we want to empower the Department of Defense to do is to be able to get those ideas, develop them, and incorporate them rapidly into our military forces.

That means we have to develop partnerships with small business and think in a different way. We have to think about a more entrepreneurial acquisition system rather than ''this is the way we have always done it and are going to keep doing it.''

We also have another area that we have to pay attention to, and that is

the area of the modernization of our nuclear triad. I recognize the concerns voiced by some of my colleagues about the cost of, and genuine disagreements about, our Nation's nuclear policy. From my perspective, nuclear deterrence is the bedrock of our national defense. For our nuclear deterrent to be credible and to ensure these weapons never need to be used, they must be capable and ready for use.

The deterrence that we have enjoyed for many, many decades has been gained by the acknowledgement by all other nuclear powers that we are more than capable to respond. Our allies and partners depend on the U.S. nuclear umbrella. That is one of the reasons why the proliferation which President Kennedy thought would be almost universal has not developed. And modernization of our strategic forces is necessary to ensure their dependability.

One thing I think everyone agrees on, and I think often gets lost in the discussion, is another factor: arms control and modernization of our nuclear forces are inherently linked together. We must reinvigorate our efforts on arms control so that we do not have a situation where the proliferation issue becomes more obvious and more dangerous. So even as we modernize, we should seek ways to promote strategic stability, like the extension of the New START agreement and follow-on talks to cover new strategic weapons and further reduce nuclear stockpiles. The best way to reduce nuclear weapons is through negotiated mutual arms reductions rather than unilateral actions. That has been the history of the Cold War, which with the Soviets and the United States we were able, with every Presidency, to come up with some type of agreement. Unfortunately, we took, I think, a less aggressive posture in the last administration, but we have to renew significantly our arms control efforts and make them clear that it is mutual interest of Russia but also China because China is a growing nuclear power with a very deliberate plan to increase significantly their nuclear arsenals.

We have to get a situation where there is at least a trilateral negotiation between the United States, China, and Russia for our own mutual benefit. And part of that is also not just looking at numbers but looking at the safeguards that each country places on the use of nuclear weapons.

We do not want a situation where there is an accidental launch that triggers a catastrophic response. We have much to do. But I will emphasize again that simply rebuilding our triad without rebuilding our diplomacy is not the best path forward.

What we have tried to do in this bill is to enhance deterrence through a number of factors, including recapitalizing the nuclear triad; ensuring the safety and security and reliability of our nuclear stockpile, our delivery systems, and our infrastructure; increasing capacity in theater and homeland missile defense; and strengthening nonproliferation programs.

We have—particularly our land-based missile systems—installations that were built in the 1960s. They are roughly 60 years old. They are showing wear and tear. And the delivery vehicles are also old. That is part of our modernization program. The Columbia class is the first of our new ballistic missile submarines. We have to replace the Ohio class because, frankly, that fleet will literally wear out. They won't be capable to go to sea at some point in the future. And that is why we are beginning right now. We are also looking at a new, sophisticated armor that will complement the other two legs of the triad.

And because this involves the Department of Energy and the National Nuclear Security Administration, we authorized $20 billion for this effort. We have funded the Department of Energy's other defense activities at $920 million and its nuclear energy activities at $149.8 million. This is all part of having an effective deterrence.

Now, as we have seen, our adversaries are developing other capabilities at an alarming rate. With regard to hypersonics, it is especially clear that China is working to develop capabilities that evade current missile defense capabilities possessed by the United States and our allies. To address these threats, the bill authorizes the Missile Defense Agency to develop a highly reliable missile defense interceptor for the Ground-Based Midcourse Defense System. It also authorizes the procurement of the Iron Dome short-range rocket defense system, David's Sling Weapon System, and Arrow 3 Upper Tier Interceptor Program to support our closest ally in the Middle East, Israel.

There was a barrage emanating from Israel's neighbors of approximately 4,500 missiles over the last year. And Iron Dome, which was created by the Israeli Government, knocked down a significant number of those missiles protecting the State of Israel. So this is not an academic exercise; this is supporting a close ally.

And it is also clear, as I mentioned before, China is expanding its nuclear weapons stockpile at a faster rate than we have seen from any other nation. It appears that China is seeking to at least reach parity with the United States and Russia in its efforts to become a world-class military. To respond to this and other countries' proliferation efforts, the NDAA authorizes $239.84 million for Cooperative Threat Reduction Programs to stop the proliferation of nuclear, chemical, and biological threats around the world.

If you take those three aspects—improving our military capability, invigorating our diplomacy, and actively using Cooperative Threat Reduction—to lower the ability and capability of those that have nuclear weapons, that is the best path ahead.

Now, we have understood over the last several years that what is causing a great deal of destruction in this world in every aspect is technology, including cyber space activities. And we, again, are trying to hone and invigorate our technological innovation in this area.

Innovation has long given us the strongest economy and military in the world. But it must be nurtured and maintained through careful investments and strong leadership in both the public and private sectors.

I believe we have an advantage because we have such a great educational system, a great entrepreneurial system, the creativity and talent of the American people, but we have to focus on needs for our military and national priorities.

And our top priority for Congress must be maintaining strong investments in technology areas that we know will shape future conflicts. This year's NDAA includes multiple provisions to accelerate the modernization of the Department of Defense by investing in research and development of cutting-edge technologies and delivering them in a timely manner to the force. Specifically, it authorizes an increase of more than $1 billion for science and technology programs that fund cutting-edge research and prototyping activities at universities, small businesses, defense labs, and industry, including in critical areas such as artificial intelligence, microelectronics, advanced materials, 5G, and biotechnology.

The bill also authorizes an increase of more than $500 million in funding for DARPA, the Defense Advanced Projects Agency. DARPA has been conducting high-risk, high-payoff research for years, including such areas as quantum computing and assisting with universities to accelerate their research. Importantly, the implements a number of recommendations from the National Security Commission on Artificial Intelligence, which the Armed Services Committee established in a previous NDAA. The $500 million of funding for DARPA will be extremely critical to the future and will produce, I think, some breakthrough technologies that not only DOD will use but will become commercial products for our national economy.

And recognizing, again, the competition between the United States and China on certain militarily-relevant technologies, the bill strengthens the language of the CHIPS Act to ensure the national network for microelectronics research and development to support the development of world-leading domestic microelectronics technology and manufacturing capabilities.

Now, I mentioned one of our problems is that we are moving from an industrial age, in which we were the dominant power in every dimension, to a new post-industrial age, where technological innovation has been distributed. Other countries, because of the

nature of cyber and other technologies, are beginning to catch up with it and, in some cases, pass us. Often, and especially in the Department of Defense, one of our problems has been procurement and acquisition practices. The Department's approach has been convoluted, poorly communicated, and burdened with inertia that makes partnering with private industry far too difficult. As America confronts threats around the globe that are evolving at unprecedented speeds, we must find a better way to identify our defense needs, communicate them, and deliver them in a timely manner.

There are several areas that, if transformed, could allow DOD to more effectively do this. The fiscal year 2022 NDAA makes important progress by establishing an independent commission to review and assess the planning, programming, budgeting, and execution—or PPBE—process and identify areas for reform.

The PPBE process has, for many decades, since the 1960s, given DOD leaders a way to evaluate the resources they need and to deliver them to the troops. However, as I mention consistently, it is a bit of a relic of the industrial age.

It came in 1961 under Secretary of Defense Robert McNamara, the former chief executive of the Ford Company. And at that time, it was the most sophisticated way to manage resources and do research, but that was the height of the industrial age.

We are now in a situation much different. So we need to modernize the procurement system and the acquisition system that we have in place. We have to make it more rapid, more agile, more capable of absorbing new products and getting them into the hands of the troops.

So in addition to establishing this independent review commission, the NDAA requires the DOD Comptroller, along with the DOD's Chief Information Officer and the Chief Data Officer, to submit a plan to consolidate the IT systems used to manage data and support the PPBE process.

One of the things we have discovered is there is no really integrated data plan in the Department of Defense—the largest Federal entity. There are multiple different brands of software systems, different brand of hardware. Some can talk to others, some can't. There is no successful company today that has such a, shall we say, slightly immature information processing system, and we have got to change it.

Similarly, management transformation is badly needed with the Department. As I said, it is one of the largest bureaucracies in the world, and the Government Accountability Office has put the Pentagon's approach to business management on its high-risk list, citing its vulnerability to waste, fraud, and abuse, inability to pass a financial audit, and a culture that remains resistant to change. To spur transformation, this NDAA requires the Secretary of Defense to improve Pentagon management by leveraging best practices and expertise from commercial industry, public administration, and business schools.

I am confident these steps will allow us to leverage the best of American ingenuity and market talent that drives innovation. At the end of the day, we should think about management as a defense capability like any other. We hope we are opening up a new day of more efficient and sophisticated management, more integrated communication, and doing it in a way that will produce results that will get the best technology into the hands of our fighting men and women.

One factor that we all are aware of every day is the challenge of cyber security. The cyber domain impacts everything we do, so there is absolutely no surprise that it has impacted the Defense Department and its industrial base. We need to ensure that our industrial base has improved cyber security, that they are not the back door through which our adversaries will use to enter and gain access to even more critical elements of our national security. As the recent SolarWinds, Microsoft Exchange Server, and Colonial Pipeline breaches painfully illustrated, traditional ''perimeter-based'' cyber defenses are simply inadequate to deal with sophisticated threats. Our adversaries are clearly advantaged in cyber domain and are likely to succeed in penetrating static defenses. Therefore, this NDAA requires the development of a joint ''zero trust'' cyber security strategy and a model architecture for the Department of Defense information network. It also authorizes an increase of $268.4 million across DOD to support cyber security efforts.

We all recognize that cyber is a persistent threat to everything we do. As one very thoughtful gentleman said years ago at a function I was at, ''Breakthrough technology like cyber has two effects. It makes good things better and bad things worse.'' And that is exactly what we are witnessing every day. So we have to exploit the good things and get them into our system and be much more vigilant at protecting us from the bad things.

Similarly, as the COVID crisis has made clear, we need a coordinated industrial policy to ensure that we have a robust, secure, and reliable technology and industrial base, especially in critical and emerging technology.

We need to give the DOD the tools and expertise to understand its supply chain and its physical security challenges, its financial challenges, and influence from commercial market trends. To that end, this bill directs the Comptroller General to conduct a comprehensive assessment of research, development, test, and evaluation authorities and other similar authorities and brief Congress on its findings.

The pandemic has shown many interesting things. Many companies and suppliers to our defense thought their products were coming from the United States, only to discover that critical components came from elsewhere and sometimes countries that were not particularly friendly to us. So we have to look seriously at our supply chain.

Finally, while I spent most of my time speaking about future challenges and how we prepare the Department of Defense to face them, we cannot lose sight of the events surrounding our withdrawal from Afghanistan.

After nearly 20 years of war, enormous sacrifice by American and coalition military, diplomatic, and intelligence personnel and vast U.S. investment, the Afghan state has failed, and the Taliban has taken control.

The Armed Services Committee has undertaken a series of hearings seeking to understand the collapse of the Afghan National Defense and Security Forces. While there is temptation to close the book on Afghanistan and simply move on to long-term strategic competition with China and Russia, we must learn the lessons of the last two decades to ensure that our future counterterrorism efforts in Afghanistan or anyplace else continue to hold violent extremists at bay.

The top-line defense number in this bill, together with the allocations set by Chairman LEAHY for defense and nondefense funding across the 12 appropriations bills, provides a realistic balance for funding the military and the rest of the Federal Government.

Once we have completed work on this important authorization bill, we need to complete the appropriations process. It would be a tremendous mistake and harmful for our national security, our economic prosperity, and our public health to resort to a continuing resolution to fund the government for an extensive period.

I have calculated, roughly, that if we go into a yearlong continuing resolution, the Department of Defense will lose $36 billion, and the consequences of that would be staggering, particularly at this moment where we face challenges across the globe.

We have near-peer competition with Russia and China, dangerous developments in East Africa, and situations across the board where we need to be ready to go looking at the threats, not looking internally at how we are going to pay to keep the lights on.

Again, to avoid this self-inflicted damage, we have to pass a budget, as well as this authorization bill.

Let me conclude by once again thanking Ranking Member INHOFE and my colleagues on the committee for working thoughtfully on a bipartisan basis to develop this important piece of legislation.

I would also like to thank the staff who worked tirelessly on this bill throughout the year—and tirelessly is an understatement. While we were leaving after our last vote, they were staying hours later to get this bill in shape to pass and then to begin our dialogue with the House. It is the staff of both sides. I salute my Republican

colleagues' staffers and my staffers for their job.

I look forward to a thoughtful debate on the issues as we go forward.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER (Mr. SCHATZ). The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. INHOFE. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. INHOFE. Mr. President, I ask unanimous consent that I be recognized for such time as I shall consume.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. INHOFE. First of all, this is a big deal, what we are embarking on now. It is something that—people understand it is the most important thing we do around here.

Let me just say that my partner JACK REED and I have been doing this a long time. I have often said how fortunate I am. You know, we hear all year out there in the real world about how everybody hates everybody in Washington; we want to compete with each other. But, you know, every year when we do the NDAA—that means the National Defense Authorization Act—it is the biggest and the most important bill of the year. Even though people think it is all happening inside this 2- or 3-day period, it is not. It is something that goes on all year long, and we have gotten to know each other very well. We know there are some areas where we have differences, but very rarely do we have differences that would impair our mission, and our mission is the most important mission that we have year-round.

So I appreciate very much Chairman REED, what he has been doing along with me, what we have done together. The NDAA has a long history of bipartisanship, and Senator REED and I have worked together to get this bill through the committee with an overwhelming, bipartisan, 23-to-3 vote to bring it to the floor. That is where we are today. That is something you don't hear about in Washington, that you can pass something out of a committee by a vote of 23 to 3, but we did, and we did it because this is a bill that is done by the Members.

The world is getting more dangerous by the day. We know that is the case. One notable example is what is happening now at the Ukraine border. Just weeks after conducting its largest military exercise in 40 years, Russia came dancing in, advancing a huge military buildup on the border. In fact, the Defense Minister from Ukraine was in my office this morning and was talking about all the things that are going on there.

According to the image that we have by satellite, we are seeing tanks, we are seeing missiles, and we are seeing artillery. Here is why I am really concerned: We are seeing even military ambulances. Why would Putin be putting in military ambulances if he was not expecting casualties? The answer is, he wouldn't. So we have an idea what is going to happen.

In addition to this equipment, the experts are reporting that 90,000 Russian combat troops are amassed along Ukraine's border. These troops are in a more threatening posture than they have ever been before. They are in the south and in the north. They are knocking on the door of Kyiv. All that is going on right now.

It might sound crazy that Russia would want to deploy so many forces now in November to a region where the winters are brutally cold, but there is something not many people really think about; that is, frozen ground is easier to move around heavy equipment like tanks and artillery.

I am not the only one who is sounding the alarm on this. Earlier this year, Senator ROUNDS and Congressman TRENT KELLY and I visited Romania, which, like Ukraine, sits on the frontlines of Russian aggression. At that time, Romanian military officials warned us that Russia was moving from a defensive to an offensive posture in the Black Sea. We are seeing that now. Everything we have predicted is happening now, and that assessment of the shift was actually right.

Putin is capitalizing on what he perceives as U.S. weakness. He knows that our NATO allies are disturbed by the catastrophe in Afghanistan and that many of the European nations fear that the United States is no longer interested in trans-Atlantic security.

The President shouldn't have done what he did, and we all—I think most Americans know that. It was a disaster, the way he put this thing together in Afghanistan, and now we know where we are on this. It is tempting to say that we have seen this before, but I don't think we have just like this.

So this is about Americans, NATO, the credibility and the capability, and that is why the NDAA is so important every year but especially this year. But, first, let's be frank: Russia is far from our only threat. In 2008—this is a document that a lot of people have looked at and thought, why didn't we do this before? This was back, I think, in—what was it? About 5 years ago, it was put together. We had what we considered to be the top six Democrats and the top six Republicans on defense, and they put this book together. It is a very brief book, but we have been—this has been our Bible. We have been doing this now for a long time, and the things that we were predicting at that time are actually becoming a reality.

It tells us for the first time—and this is significant. People don't understand this. For the first time, we have two major adversaries at the same time. This hasn't happened before. And, you know, we are talking about Russia. Yes, that is significant, and you have heard me say this before—the Chinese Communist Party has been investing heavily in modernizing its military. Over the last two decades, their military spending has gone up 450 percent—just in the last two decades. Now, we are not doing that over here.

You know, I have to say—and everyone realizes this—these communist countries have a great advantage. They can move and move quickly, and they don't seem to have any limitations. Now, we are seeing the results of that investment. They have tested hypersonic missiles that we don't even have anymore. I have to say that again. Hypersonic missiles are something they have and they are using. They have tested. We have seen it. We don't even have it, and we don't have any counter to that. They are leapfrogging us in other critical areas, like artificial intelligence, and they are rapidly expanding their nuclear arsenal and infrastructure.

These investments in military capability are done with real purpose. They are a threat to Taiwan and other allies in the Indo-Pacific. Ambassador Bikhim Hsiao was in my office this morning—Ambassador from Taiwan—and we were looking at things that are going on there, just like we are looking at from the Russian area.

But the threat China poses to our own interests can't be overstated or underestimated.

Meanwhile, North Korea—so it is not just those two countries. North Korea is out there. Iran is out there. They are also continuing their threatening behavior. North Korea is conducting missile tests of its own, and Iran continues to back proxies striking at U.S. troops and our interests—most recently, we have seen in Syria.

The terrorist threat in Afghanistan is also resurging thanks to the disastrous drawdown that continues to undermine U.S. credibility. We know that ISIS-K and al-Qaida have the desire and intent to strike our homeland. This is something that a lot of people don't understand. A lot of people don't believe the threat that is out there. Now we know when they will be able to strike us, and it is closer than you think. As soon as 6 months from now, the Senate Armed Services Committee was told just last month this could happen.

So I don't say this to be dramatic. This is a reality, plain and simple. The world is more dangerous than it has ever been in my lifetime—by the way, people have reminded me over and over again yesterday and today, since it was my birthday, how long that lifetime has been—and we have seen a lot, but we haven't seen anything like this before.

National security needs to be the top priority. Without a strong military defending our way of life, nothing else matters. We can talk about other things, but it doesn't really matter if we can't do that.

Since World War II, we have ensured peace through the world by projecting strength. Our military should and must serve as a strong deterrent to our adversaries, and they have to know that they can't beat us. Some people are questioning that, but they have to know that they can't beat us, and we have to show them that they can't. Yet we are fully aware that they have things we don't have. They have technology we don't have. This is something we haven't dealt with before.

President Biden's inadequate defense budget request, the irresponsible drawdown in Afghanistan—something he shouldn't have done; the administration should not have done—and the lack of commitment to shared nuclear security are calling that into question. It is evidence that we aren't prioritizing national defense, and we already have seen what happens when we don't prioritize national defense. We see upticks in destabilizing, threatening behavior—exactly what Putin is doing right now. Just imagine what would happen if Putin and Xi thought they stood a chance to beat us if we didn't turn things around, and that could happen.

It is a reality today that people don't understand and should understand. Americans take for granted the idea that our military is the best. You know, when I go back to not just my State of Oklahoma but all around the country, people assume that.

You know, I am old enough to remember what was happening at the tail end of World War II. We learned a lesson. We learned to be prepared, and for a long period of time, we had the best of everything. We had the best modern equipment, all of this, and that isn't the case today. Americans take for granted that we have the best of everything, but we don't. It is just not true anymore.

Don't just take my word for it, you know, just take it from me; a couple of weeks ago, our Nation's No. 2 military adviser, General Hyten—no one disagreed—I don't know of anyone who would actually argue with General Hyten. He was explaining how China is on pace to surpass us if we don't do something to change what is going on today. That is General Hyten. I don't know a more knowledgeable person anywhere in America or elsewhere.

We can meet these challenges. We can put our country back on the right track. That is going to take real investment and real strategy. Congress has a very important role to play here. We pass the National Defense Authorization Act and Defense appropriations each year, and every year, we give our military what it needs to set this thing right.

Now, I am proud to say that this year's NDAA goes a long ways to making our country more secure. I am not saying it is perfect, but it is very good and a necessary start. And that is what this is all about now. It is what we are going to be passing—I am talking about tomorrow or the next day—and going into this long process that includes both the House and the Senate.

So let's start with one of the biggest ways to strengthen our national defense: authorizing an additional $25 billion in funding for the Department of Defense. This is just a floor for defense spending.

Now, it is important that we understand this President has not been a good President in terms of building the national defense. He just isn't. You know, his budget request shortchanged our national defense. In fact, if you put his budget numbers in terms of defense and nondefense, the amount that goes to nondefense averages about a 16-percent increase, and the amount that goes to defense is a 1.6-percent increase. Now, that is the President's budget. It is not my budget. It is not our budget. It hasn't passed, but nonetheless, that gives you an idea of where we are right now. The emphasis is not on defense. It should be, and it is not.

President Biden's budget request shortchanged the national defense. It didn't even keep pace with out-of-control inflation. Inflation right now—the figure is above the 1.6 percent, and that is where we are today. It actually cut funding for our military even as we face the growing threats that I mentioned. And we are talking about the—compared to the inflation thing that is happening right now. So I am glad the Armed Services Committee almost unanimously adopted my amendment to increase the Department of Defense's budget top line. This is the bare minimum of what we need to meet the threats that we face. This is what underscores everything we do.

The bill also makes sure this money is spent the right way. As we have for the past few years, we are using the 2018 national defense strategy—that is this book I referenced just a minute ago—as kind of our roadmap, and we are using this for that.

The NDAA focuses on the Indo-Pacific, which is our priority theater, by emphasizing investment in the region through the Pacific Deterrence Initiative, the PDI, which we started in last year's bill.

The way this works is we are—it is continuing as time goes by. We have a bill, and the bill is activated, usually in December, but then we are already into the next year. So while this seems—people say: You are only talking about one bill a year. It doesn't really work out that way.

It strengthens our supply chain so we are not reliant upon China, but we are doing that right now. It addresses the threats posed from information warfare, and it deters the foreign malign influence. It also stands strong against Russia.

Perhaps most importantly, it provides critical lethal aid to Ukraine, and we know that these things are working. While radios and cold-weather gear are needed, they won't deter Putin's strategy and his ambitions. Weapons like the Javelin anti-tank missiles, on the other hand, remind him that invading and annexing Kyiv will have real and concrete costs.

We know Russia and China are expanding their nuclear arsenals. Our nuclear stockpile serves as the cornerstone for our deterrent, so we have to keep it safe, secure, and effective. That is why the NDAA supports the nuclear modernization our military commanders say is their top priority.

It provides support for our allies and partners around the world. Unfortunately, our allies and partners are questioning our commitment right now after what happened in Afghanistan, and they are feeling like they were being told and not consulted. They didn't even know—that withdrawal that should not have taken place but did take place in Afghanistan is one that they were not even aware of.

It provides the reassurance of American credibility that they desperately need to rebuild and cement those relationships. With strong allies and partners around the world, we will ensure the balance of power in our favor, but we are not there yet.

When it comes to hard power, this bill makes serious investments in equipment we need to fight and win wars now—growing our naval fleet, expanding next-generation fighter capability, and providing for the largest investment in military construction in a decade.

It looks to the future too. We know that we need to accelerate innovation and develop the technology that is going to help defeat whatever our enemies might throw our way. Yet, in many of these emerging technologies, we risk falling behind. In some cases, we already have fallen behind. It is kind of hard for us to accept that in America, as we went through several decades—I think since the Second World War—not falling behind, but we have now. So this year's NDAA invests in defense technology that would put us back ahead of our competitors. That is our goal. Things like microelectronics, artificial intelligence, hypersonic weapons, 5G—these are the areas that we are working on to get back in the driver's seat. We have fallen behind. It is hard to say that, that America is falling behind.

You know, General Hyten said recently something that I really think is important for everyone to hear. He said that we must ''focus on speed and reinserting speed back in the process of the Pentagon . . . and that means taking risk, and that means learning from failures, and that means failing fast and moving fast.''

I have to say that General Hyten is certainly one of the greatest warriors of our time. We should be listening to him.

We have serious problems. We have to get policies and authorities in place to let the Pentagon move quickly and, as General Hyten put it, ''fail fast.'' As he retires this week, I think it is clear

why he is a national hero. He knows what is going on.

Now, too much is hampered by bureaucracy at the Pentagon. The NDAA encourages the Pentagon to move faster, to take risks, and to jumpstart the innovation that we need to succeed, but we have to realize the impact.

This is really the most important thing this bill does. We take care of our troops. People talk all the time about how much we spend on military. I hear a lot of people around who don't think we need a strong military. A lot of them talk about why we spend more on our military than Russia and China put together.

Yes, that is true; but we have costs that others don't have. Communist countries don't have the cost of taking care of their people. In fact, the most important thing we do is take care of our troops. Even though China and Russia are building up and modernizing their militaries, they don't take care of their people—they don't claim to take care of their people—and we do. The most expensive thing we do in our military is to take care of our military. We take care of the schools and the people who are out there taking the risk.

This bill takes care of our troops in so many ways. It improves their healthcare. It provides education and childcare for their children, and makes sure their spouses can have meaningful employment as they move from area to area. It is a unique problem that our spouses do have, as they are moving around the country.

And so, again, we are competing with China and Russia and other countries, and none of them have this problem. This is the greatest expense that we do. Our servicemembers represent the very best in the country. If they do have to go into harm's way, it is our responsibility that they are the best prepared, best equipped, and the best led forces in the battlefield, and the bill does that.

But we don't want them to go to war. We want to prevent those wars from happening. As I said earlier, the best way we do that is by projecting strength, sending a message to our adversaries that there is no chance that they can beat us.

The NDAA is the major way that we send that message. And that is why the NDAA—the National Defense Authorization Act, the most significant bill of the year—has been enacted into law every year for the past 60 years. This will be the 61st year.

So we are going to get it passed, but it almost never comes up this late in the year. This is the disadvantage we are working from, but it always gets done eventually. We still have a lot of work left to do after this and not a lot of time to do it.

You know, we can't afford late starts. If you do late starts, sometimes it ends up being just down to four people. Both my partner and I have been in this situation where we have been down to what they call the big four, making all these decisions ourselves. That is not what we are supposed to be doing. That is not what we want to do. But that is why the NDAA has been enacted into law every year for 60 years.

We built this bill around Member requests. This is unique. This is something people need to understand. We are getting our requests from the Members that are serving with us here in the Senate. We are going to have an open amendment process. We are going to have an open amendment process, and this is what we have committed ourselves to do, to make sure we are doing. So you will get another chance to mark up this bill.

So what we are doing right now is very important. You got to keep in mind, it is going to be done by the House; it is going to be done by the Senate. It is going to be something that is the most significant thing that is happening this year. But we could never work too hard or too long for our troops and national defense.

I know some of my colleagues are concerned about one provision we've got—that we have in this bill at this time, which was added in markup and included in the House bill too. Now, I oppose the addition of this provision, which changes the military draft—what the military draft does. And I want you to hear this because, if enacted, it would expand the draft so that it is not just about finding combat replacements to serve on the frontlines; it also requires women to register for the Selective Service, not just men.

I've always said, as a product of the draft myself, I know what the draft is. I was there and I served. I have always said that I understand that and I think the draft is essential. It changed my life, certainly. But I am strongly opposed to drafting our daughters and our granddaughters. So this is going to be coming up. We are going to be talking about this. Everything is going to be out in the open. Get ready for that fight, because that fight is coming, OK?

That is why I submitted an amendment to strike this provision from the underlying bill, and I will work to get it out of any conference report as well, OK?

Last week, we marked Veterans Day, and that should be a reminder to all of us why we do this. In fact, we have got 2.2 million reasons to do this—2.2 million future veterans—our volunteer force, who put their lives in harm's way and who rely on this bill getting done. And that doesn't even include their families, who are sacrificing so much. So that's out there, we know, and that is going to happen.

I know my colleagues understand this. I know they understand our responsibility to our troops and to the American people. And so I look forward to our debate on this bill, and then passing it in the traditional, bipartisan way, as we always do; and, together, we are going to fulfill our constitutional duty and meet these challenges that we face, and we have little time to waste in doing this.

So this is the most significant bill of the year. That is what we are going to do. We are going to get it done. And let's go do it right, OK?

I yield the floor.

The PRESIDING OFFICER. The Senator from Montana.

Mr. TESTER. Mr. President, I am pleased that the Senate has taken up the National Defense Authorization Act.

There is a 60-year tradition in this body of getting this bill done because the importance of this bill transcends partisanship. In fact, 81 Senators of both parties joined forces earlier this year to override a senseless veto of this important bill by the former President.

Now, while both sides of the aisle can work cooperatively to get this defense policy done, we are now seeing unprecedented—unprecedented—obstruction by the minority party for passing a budget that will fund the programs that our military and our veterans need.

Now, look, if Republicans succeed in this obstruction, I am going to tell you that the government will be forced to go to a full-year continuing resolution. That is not workable. The result will be frozen spending levels for the Department of Defense and for the Department of Veterans Affairs, which amounts to a $70 billion cut in spending for those two Agencies alone, compared to the appropriations bills prepared in the U.S. Senate.

I serve as chairman of the Senate Veterans' Affairs Committee, and let me tell you what is at stake for America's veterans and their families. Funding will be blocked for priorities like expanding veterans' access to lifesaving mental healthcare services, enhancing women veterans' healthcare, providing housing assistance, and expediting the delivery of benefits and care for those suffering from toxic exposure.

Let me say this again.

If we go to a 1-year continuing resolution, that means we go off of last year's budget, last year's spending bill. We will block priorities like expanding access to mental health services for our veterans. We will block services for expanding women veterans' healthcare. We will block services for housing assistance and for expediting what is one of the most serious issues coming out of the conflict of 20 years in the Middle East, and that is care for those that are suffering from toxic exposure.

The bottom line is this would keep the VA from properly addressing a whole host of issues on behalf of those who would put their lives on the line for this country, and they are going to continue to pay the price for us not doing our job.

As chairman of the Defense Appropriations Subcommittee, I was able to draft a bill that provided a $31 billion increase for defense compared to last year. This military bill is consistent with the spending levels approved by

the bill we are working on today. In fact, in an amendment offered by Senator INHOFE, that amendment passed 25 to 1, which will plus-up this bill.

So why isn't the defense appropriations bill flying through this Senate just like the NDAA?

Well, I will tell you. In September, the Republicans on the Appropriations Committee announced they would vote against all appropriations bills in part because Senator INHOFE's bill doesn't increase defense with enough spending. So the idea here is, just take money and throw it at the wall and hope that it's spent right.

The bottom line is there needs to be plans and there needs to be planning. And I am going to tell you, the last time I checked, the $31 billion increase is a pretty good chunk of dough.

So it is simple. Do we want to fund the VA? Do we want to fund the military? Do we want to fund this country's government?

Or do we want to go back to last year's funding? Which, by the way, would be totally inadequate, but it is what some on the other side of the aisle are advocating right now.

Look, guys, we are in a continuing resolution right now. It expires on December 3. If, in fact, we had a budget deal today, we couldn't get an omnibus out for nearly 5 weeks.

So what I am saying is this: no more finger pointing, no more changing the rules of the game, no more foot dragging. Do what the gang of 10 did on the bipartisan infrastructure package. Let's go into negotiations to get to yes. Let's all work together. Let's not play irresponsible political games with our military and with our veterans and with everybody else who lives in this country.

What are we here for? Are we here to advocate for this country? Or are we here to advocate for a political party?

I am telling you the appropriations bills should have been done last September. We should be sitting at the table today. I am ready to roll up my sleeves and help in any way that I possibly can to make sure these bills get through this body and to the President's desk so we can fund our veterans and fund the needs that they have, so we can fund our military and deal with the threats that are facing us around the world.

It is time, folks. It is time to quit talking, and it is time to start doing.

I yield the floor.

The PRESIDING OFFICER. The Senator from Iowa.

Mr. GRASSLEY. Mr. President, my fellow Senators: On November 4 of this year, I introduced an amendment to this year's national defense bill. This amendment focuses on the Office of Net Assessment. That office is within the Pentagon.

The Office of Net Assessment's purpose is to produce an annual net assessment, which is a long-term look at our military capabilities and those of our greatest adversaries.

In 2019, when I began to look at Stefan Halper's contracting work for the Office of Net Assessment, something didn't look right. So I asked the inspector general to look into it.

For those who are unaware, Halper was a central figure in the debunked Russia collusion investigation. And I don't have to explain the Russia collusion investigation; everybody in the U.S. Senate knows something about that and they know what it refers to.

Halper secretly, at that time, recorded Trump campaign officials during Crossfire Hurricane.

Halper also received over 1 million taxpayer dollars from the Office of Net Assessment for several research projects. But the question is: Were they really research projects?

But the inspector general found some problems with his contract:

The Office of Net Assessment didn't require Halper to submit evidence that he actually talked to the people he cited in his work, which included Russian intelligence officers.

Secondly, the Office of Net Assessment couldn't provide sufficient documentation that Halper conducted all of his work in accordance with the law.

Thirdly, the Office of Net Assessment didn't maintain sufficient documents to comply with all of the Federal contracting requirements and OMB's guidelines.

The inspector general also found that these problems weren't unique to Halper's contract. This is the inspector general speaking up on this. I am reporting what he said. So these findings indicate systemic issues within the Office of Net Assessment in the Pentagon.

Moreover, this office has spent taxpayers' money on research projects unconnected to net assessments. In other words, they are spending money and wasting money that doesn't deal very closely with our national defense.

Two cases in point: The office funded a report titled ''On the Nature of Americans as a Warlike People: Workshop Report.''

Now, that report highlighted the ''level of American belligerency which is the result of the persistence of Scotch-Irish culture in America.''

That ought to get a lot of your attention. What does that have to do with the assessment of the capability of us to deliver on the constitutional responsibility of the Federal Government to the defense of the American people? Or what does that have to do with our assessing the capability of our enemies?

Yet another report focused on Vladimir Putin's neurological development and potential Asperger's diagnosis.

Now, I have highlighted these reports for the Pentagon, and I have asked for records from the Office of Net Assessment relating to some of its other work as well. To date, they still haven't been able to provide all of the records that they ought to provide to the Congress of the United States, under our constitutional responsibility, to see that money is faithfully spent according to congressional intent and that the laws are faithfully executed.

While the Office of Net Assessment was busy wasting taxpayers' money and not responding to congressional requests, China built its hypersonic missile program.

Are we on top of that program? It has got something to do with our enemy's capability.

As a result of all of these failures, then, like I told you, I introduced my amendment to the defense bill on November 4. The amendment would require the Government Accountability Office to determine how much taxpayer money this unit actually uses for net assessment—the reason they were set up.

Are they doing their job? Are they following the law? Are they spending the taxpayers' money responsibly?

I think I have shown, in some instances, where they have not.

The amendment would filter out taxpayer-funded research that has nothing to do with net assessment. In other words, the Office of Net Assessment ought to be doing net assessment, and that deals with the capability of the U.S. Government to do the No. 1 responsibility of the Federal Government: the national defense of the American people.

The second responsibility of this Agency is to determine the capability of our enemies to do damage to us. In other words, it is time that we find out how much money the Office of Net Assessment needs to actually do its job instead of acting like a slush fund for irrelevant or political research projects.

Of course, if this happens and the taxpayers' money is spent properly, this, in turn, will save the taxpayers, potentially, millions of dollars a year.

I encourage my colleagues to support the amendment.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. CORNYN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

THE ECONOMY

Mr. CORNYN. Mr. President, families back home in Texas are planning their Thanksgiving menus, but they are also bracing for steep grocery bills. Prices are up for just about every part of a typical Thanksgiving meal. The cost of a frozen turkey is the highest in history. Things like potatoes, butter, pumpkin pies, even salt, cost more than they did a year ago.

It is not just going to cost more to eat; it is going to cost more to cook. Appliance prices have skyrocketed over the past year, as have electricity bills, and family members will have to

pay a lot more just to visit their friends and relatives because gas prices are up 60 percent from last year.

As families are being pummeled by higher prices and inflation, our Democratic colleagues are planning to hand major savings to a select group of Americans, just not the ones you think and certainly not the ones who need the help.

Despite their cries of taxing the rich, the Democrats are plotting an absolutely massive handout to the wealthiest Americans. This windfall is not distributed through stimulus checks or lower tax rates. That would be far too obvious. Instead, our Democratic colleagues are relying on a range of gimmicky sunsets and expirations to dole out the millionaire tax break.

If they thought no one would notice, well, they would be wrong. For example, The Washington Post headline says it all. It reads: ''The second-biggest program in the Democrats' spending plan gives billions to the rich.''

That is not how our colleagues have tried to brand their legislation. They would portray themselves as modern-day Robin Hoods—stealing from the rich to give to the poor.

Strange in that it is really just the opposite. They talk about the wealthy paying their fair share and giving working families free programs, but the reality of the situation is far different from the picture they paint, and the wealthiest Americans stand to reap big benefits under this legislation.

For example, the Democrats have included a provision that will allow millionaires and billionaires in blue States to pay less in Federal taxes. As the headline notes, this handout comes with a big pricetag of $285 billion in tax breaks for the wealthiest Americans. It is more expensive than the clean energy and climate provisions in their bill; more expensive than paid family leave; more expensive than the combined cost of the child tax credit and home-based services.

And there is no denying that the beneficiaries of this ultraexpensive provision are the wealthiest Americans. According to the Tax Policy Center, about 70 percent of the benefit goes to the top 5 percent of wage earners—70 percent goes to the top 5 percent. That is people making more than $366,000 a year, roughly six times the median household income of Texans. We were not talking about saving a few dollars here and there. The top 1 percent would save an average of $14,900 next year, and the bottom 40 percent of taxpayers wouldn't be given a dime's worth of a break in their taxes.

The rich in America who stand to gain the most from this change are those who live in blue States, like New York and California that have higher State and local taxes. They would, under this legislation, get to deduct up to $80,000 in their State and local taxes from next year's Federal tax return, leaving everybody else to fill up the gap.

Working families in Texas should not have to subsidize the tax bill for Manhattan millionaires. If the wealthiest people in New York or California think their State and local taxes are too high, there is a pretty simple solution: Tell your elected officials to cut taxes or you can do like many people are doing these days, vote with your feet and move to places like Texas.

Over the last decade, Californians have flocked to my State by the hundreds of thousands. People do vote with their feet, and they clearly support what we are doing in Texas.

We have been happy to welcome folks from all around the country who are in search of lower taxes, affordable homes, and a better standard of living.

Blue State millionaires can't expect my constituents to subsidize their tax bills. They need to either pay their taxes or maybe they need to decide to move to someplace where they are not taxed at such a high rate.

Under this bill, two-thirds of those making more than $1 million will receive a tax cut next year. Let me say that again. The vast majority of millionaires will, under the Democratic legislation, receive a tax break, and nearly 90 percent of those earning between $500,000 and $1 million will receive a tax cut. This is a sharp contrast from how middle-class working families are treated.

Less than a third of those earning between $20 and $100,000 a year will receive a significant tax cut. And the following year, 2023, those savings dramatically decrease.

Year over year, the tax provisions in this bill change dramatically. In fact, there is not a single year over the next decade in which each tax provision will be used at the same time.

Democrats aren't rewriting the Tax Code to make millionaires pay their fair share; they are gaming it to create the illusion of fairness.

Some programs begin immediately and end after 1 year. Some don't even take effect for a couple of years. These are plain budgetary gimmicks. After all, they can't afford to give billionaires a tax break and dole out increased social welfare programs. The fact of the matter is, the millionaire tax break in their legislation is the largest handout for wealthy Americans. But it is not the only one in the bill.

This legislation would allow people earning hundreds of thousands of dollars to receive up to $12,500 from the taxpayers if they buy an electric vehicle. They also can receive up to $900 to purchase an e-bike, which is obviously less green than a good old-fashioned regular bike.

The Democrats' reckless tax-and-spending bill also creates handouts for union bosses, trials lawyers, wealthy media corporations, and a host of powerful friends of the Democratic Party. All of these handouts may appease some of our colleagues' wealthiest supporters, but it will only make life harder for working families.

Families earning just over the median household income, which is just under $62,000 in Texas, could see their childcare costs soar by as much as $13,000.

And the climate policies in this bill are sure to drive energy prices even higher. Gasoline already costs 60 percent more today than it did a year ago. That is a combination of inflation and the policies of this administration which attack the very energy industry that we depend upon to provide affordable energy.

If the Democrats manage to get this grab bag of radical climate policies signed into law, prices at the pump will go even higher.

So this bill will not, as advertised, help America to build back better. It will ensure that we never reach the prepandemic recovery that was the envy of the world.

No public relations campaign can hide the truth about this bill. This is a reckless tax-and-spending spree that will benefit the wealthiest of Americans at the cost of working families.

The last thing we need to do is to line the pockets of wealthy Americans while driving up the costs of the middle class.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. LEE. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

UNANIMOUS CONSENT REQUEST—S. 3243

Mr. LEE. Mr. President, this is now the 17th time I have come to the Senate Chamber specifically to speak against President Biden's vaccine mandate.

I have pledged before, and I pledge again today, to continue this fight until we beat the mandate.

Now, thankfully, progress has been made on this front. The U.S. Court of Appeals for the Fifth Circuit last week halted enforcement of President Biden's general mandate. It did so directing their rulings specifically to the OSHA portion of the mandate. This is the one that applies to all workers everywhere and any place of employment with more than 100 workers.

I, along with millions of Americans, am grateful that the U.S. court system performed its role in protecting the separation of powers and otherwise protecting the limits on government written into our laws and our Constitution.

It is also encouraging to see the government Agency charged with enforcing the general mandate; that is, OSHA, has now halted the enforcement of the mandate and is complying with the order issued by the U.S. Court of Appeals for the Fifth Circuit.

This, however, does not end President Biden's vaccine mandates. That

mandate in particular remains the subject of ongoing litigation, and there are other requirements placed on other specific groups of workers outside of the OSHA mandate and, therefore, outside the scope of the order issued by the Fifth Circuit.

Now, I have spoken previously on the situation that members of our Armed Forces face and on things that people who work in the healthcare profession face—difficult things, challenging things, things that threaten their livelihoods and cause a lot of problems for workers.

I have offered various bills to help those groups of Americans keep their jobs and make sure that they have the right to make their own medical decisions.

I am fighting against the mandate. I am not fighting against the vaccines. I support the vaccines. I am vaccinated. I have encouraged others to be vaccinated. I see the development of these vaccines as something of a modern medical miracle, one that is protecting so many millions of Americans from the harms of COVID.

But this one-size-fits-all dictate from Washington certainly isn't the answer and, under our system of government, can't be. I have heard from hundreds of Utahns who are personally at risk of losing their jobs and their livelihoods due to this mandate. Many of these Utahns have religious or health concerns about the vaccine.

President Biden promised these mandates would include exemptions for those people in those categories specifically, but in reality they are being dismissed or placed on unpaid leave or pushed into retirement with reduced benefits.

These are good people, everyday people. Many are dedicated frontline workers. Far too many are just trying to make ends meet and feed their families. It shouldn't be too much to ask to allow them to continue doing that unencumbered by their own government in their efforts to do that.

These mandates will just push people out of work and make many of them not only unemployed but unemployable outcasts in their chosen professions, professions for which they have spent years studying and learning and receiving certifications just in order to work. What a tragedy.

This wouldn't just harm those affected directly by the mandates. It absolutely would harm those directly affected by them, but the harm extends much further than those directly affected. It would affect all of us, in fact.

The American economy is currently facing a labor shortage the likes of which we haven't seen in decades. Businesses across the country are struggling to find enough workers just to keep their doors open, let alone produce and serve at full efficiency. President Biden's mandate will add to our high unemployment and our low labor force participation rates, and it will put even more pressure on inflation—inflation that is making it harder for Americans everywhere, especially the poor and middle-class Americans, people living paycheck to paycheck who find that every dollar they earn is buying less of everything, from gas to groceries, from housing to healthcare.

Federal Reserve Chairman Jay Powell recently warned that ''hiring difficulties and other constraints could continue to limit how quickly supply can adjust, raising the possibility that inflation could turn out to be higher and more persistent than we expected.''

The mandate is only worsening the problem.

Now, I believe the Biden administration recognizes the harms this mandate will cause for our workforce. It is evident in the administration's date of compliance extension to January 4 that this is the case.

Now, I have to ask an obvious question here—or one that I think should be obvious, should be intuitive. If the forced vaccination of our entire Federal workforce, including employees and contractors and subcontractors—if forcing the vaccination of every one of these workers—were truly an emergency so drastic that all workers, contractors, and subcontractors, even those working remotely in their own homes, must be vaccinated immediately, then why would they risk delaying compliance?

They can't have it both ways. If they want to say that this is an emergency; this is dire, so dire that we have to force every contractor, subcontractor, and Federal employee to get vaccinated immediately and we have to fire them if they don't—if that is truly so emergent—then why delay it to January 4? Why delay it at all?

Now, to be sure, it would be bad. And, to be sure, I am glad they have extended it. Perhaps, maybe, this means they are reconsidering this awful, horrible step, this horrible thing that they are inflicting on those who can least afford to absorb something like this. But it really does undercut the emergent nature of the situation, and it undercuts their underlying reasoning that this has to happen immediately, so immediately that we have to fire all of them if they won't submit to Presidential medical orthodoxy.

This mandate is even so drastic that it includes all workers and all contractors, including all those who work remotely, who don't even go into a workplace. And it also includes even those who have natural immunity from a previous case of COVID–19, something that some studies have indicated will provide 27 times the immunity of a vaccine.

Again, vaccines are great. I have been vaccinated. I have encouraged others to do the same. Vaccines are protecting hundreds of millions of Americans right now. But why not take into account their natural immunity, and why on earth would you fire someone who already has natural immunity or who works from home? That makes absolutely no sense.

This mandate simply goes far beyond what is reasonable. It begs all sorts of questions. Why are you doing this?

So, today, I am offering a bill to help another group—yet another group of people—a group consisting of people not protected by the Fifth Circuit's halting of the general vaccine mandate. Federal workers are still facing a vaccine requirement from the Biden administration. Almost 3 million workers in this country are employed by the Federal Government. Many of them have reached out to me and my office and are concerned about losing their jobs due to this mandate. I know I am not the only one. I know that every single Member of this body has received phone calls, letters, emails, and other pleas for help from people who don't want to lose their jobs.

This is a response to them. This is an effort to try to help them and part of my ongoing effort to reemphasize the fact that it doesn't have to be this way. My bill, the Protecting Our Federal Workforce from Forced COVID–19 Vaccination Act, would prohibit an executive Agency from requiring its employees to receive a COVID–19 vaccine. It is a simple solution to prevent more unemployment and to protect countless Americans from being forced out of the workforce.

This bill will help protect Americans' right to make their own medical decisions and will help protect our economy as it strains under multiple crises and as the holiday season comes around.

I encourage and sincerely implore all of my colleagues to support it.

To that end, Mr. President, I ask unanimous consent that the Senate proceed to the immediate consideration of S. 3243, which is at the desk. I further ask that the bill be considered read a third time and passed and that the motion to reconsider be considered made and laid upon the table.

The PRESIDING OFFICER (Mr. KING). Is there objection?

Mr. PETERS. Reserving the right to object.

The PRESIDING OFFICER. The Senator from Michigan.

Mr. PETERS. Mr. President, in an ideal world we would not need a vaccine mandate. In the ideal world the vast majority of people who can get vaccinated would heed the advice of scientists and of public health officials and take the very simple step to get vaccinated so that we can get this pandemic under control.

But, unfortunately, our reality is very different. We have been working to contain this virus and manage this unprecedented health crisis for nearly 2 years now. It has cost us more than 765,000 American lives, and millions of other Americans have been infected and may face lifelong health challenges as a result.

It doesn't have to be this way. We have safe, effective, and lifesaving vaccines that are now, thankfully, available to a significant number of Americans.

Vaccines are our best tool to finally get this pandemic under control, and requiring the folks who are able to get vaccinated is just simply common sense. We are all tired of this pandemic, and we all want it to end. We are tired of wearing masks because some folks refuse to get vaccinated. We are tired of wondering if we could unknowingly be exposing our vulnerable family members who are taking every precaution. We are tired of waiting for enough people to get vaccinated so that our schools and our businesses and our daily lives can just get back to normal.

And we are tired of emergency rooms and healthcare workers getting overrun by COVID cases from people who are not vaccinated, when we already have the best tool to prevent the spread in the first place. Our frontline healthcare workers are being crushed by the consistently high number of cases, and public health experts are predicting that yet another spike will likely hit this winter unless people get vaccinated.

In my home State of Michigan, the number of unvaccinated patients hospitalized with COVID is once again climbing. A headline from today noted that Michigan has just reached a new pandemic record with the highest COVID case average in the Nation and that deaths across the State continue to rise. Emergency rooms are packed, and in some areas patients are forced to wait for hours or for days to be admitted.

There is one key factor that is driving this horrific scenario: 88 percent of the cases, 88 percent of the hospitalizations, and 88 percent of the tragic deaths were all people who were unvaccinated.

We can put an end to this nightmare by getting more Americans vaccinated.

You know, we require so many preventive measures to keep ourselves and others safe. We wear seatbelts in our cars. We require hardhats on construction sites. We get vaccinated to protect ourselves against a whole number of health risks. And we do it because we know it saves lives and it keeps people healthy.

The answer is simple: Get vaccinated.

Mr. President, I object.

The PRESIDING OFFICER. Objection is heard.

The Senator from Utah.

Mr. LEE. Mr. President, I appreciate the thoughtful remarks and the insights of my friend and distinguished colleague the Senator from Michigan. He is someone with whom I enjoy working, and one of the many things I appreciate about him is that he puts a lot of thought into everything he does. And I have always known him to be considerate, and I appreciate that about him.

I also am in agreement with the fact that in an ideal world people would be getting vaccinated more than they are. And in that world, if more people got vaccinated, I do think there would be fewer hospitalizations, fewer deaths, and fewer COVID infections. And there are a lot of data sources supporting that.

I also agree that we are all tired as a country, as individuals, as families, regardless of what State we live in. We are tired of the pandemic, of the ERs being overcrowded, and things like that. These are all things we want to do away with. And I also agree with my colleague from Michigan that those things really would be alleviated if more people got vaccinated.

In my mind, the question that we are discussing here isn't about a disagreement over the objectives that we have got; it is more about how to get there, who has authority to take what action and what consequences might attach to government actions.

Notwithstanding the fact that my friend from Michigan and I both agree that the American people, to the extent they have been vaccinated, are benefiting as a whole from being vaccinated, it doesn't mean that everyone is going to agree.

It doesn't get rid of disagreements that exist, in some cases, because of our religious belief or other moral conviction—one that I don't happen to share and probably most of us in this body don't happen to share, but that some people have.

There are some people who, for religious or moral reasons, believe that they shouldn't be vaccinated. There are others who have a specific medical condition that has involved receiving medical advice from board-certified medical doctors that someone shouldn't get this particular vaccine.

I am not a doctor. I am not a scientist. I don't purport to understand these things. But I do know what I hear from Utahns, which is that a number of them have cited medical conditions of one sort or another; previous personal or family medical history that has signaled particular sensitivity to vaccines in general; or, in some cases, when people have autoimmune conditions of one sort or another or a combination of them.

In some cases, doctors are concerned about inflaming that condition, inflaming the immune system of particular patients, and on that basis advise their patients with particular, somewhat unusual medical histories not to be vaccinated.

There are others, still, who might not fit into either of these categories, but might consist of people who have already had the coronavirus and have recovered from it at some point over the last 18 months.

There are studies indicating that natural immunity is real, and that have suggested that natural immunity can convey comparable immunity to that available under the vaccine. Some of the studies have indicated that that immunity could not only be as strong as, but, in some cases, 27 times stronger than that conferred by the vaccine.

I had both. I had the coronavirus over a year ago and I still chose to be vaccinated in addition to that. My own experience with the coronavirus wasn't all that pleasant. It wasn't an experience that I care to relive. In consultation with my doctor, I concluded that it was a good thing for me to get it. I was willing to get it, especially upon learning that it might help protect me even further if I also had the vaccine in addition to having natural immunity.

But, you know, not everyone is going to reach the same conclusions. And one of the struggles that we have had as a country involves difficult questions that people face when they disagree—when they have a genuine disagreement. We have to be careful about how we use government power because the government power necessarily involves the use of force.

Most of the time, mercifully, it doesn't have to involve the direct actual use of force. It can involve the implicit or implied or future or prospective use of force. In other words, you comply with this or that law or regulation or government dictate of one sort of another, then you are fine. If you don't, you know that at some point there will be consequences.

A lot of people comply voluntarily after they received—I don't know—a notice from a law enforcement officer or agent. Or maybe they wait until someone has sued them, and then they get a court order. But they know that at some point, if they refuse to comply, the government can enforce what it is requiring.

So whenever we involve government in these kinds of decisions, we have to be able to defend the actual or threatened or potential use of force in order to justify what we are doing. And we have to ask: Is this moral? Is this an appropriate case to use violence?

Because if it is not an appropriate case to use violence for something, there is kind of a problem with putting government into the equation, because ultimately you have to rely on government to be willing to threaten violence and carry out violence; meaning to show up at somebody's house with a summons, an arrest warrant, or something like that and take them away.

All that involves force. And again, mercifully, most of the time it doesn't have to come to that. Most of the time, Americans, you know, comply with the law just because it is a good thing to comply with the law.

But we really should ask the question whether a government action is morally justified in any circumstance to such a degree that the use of violence would be warranted if it came to that.

I struggle to accept the proposition that it is OK to use violence to force someone to get a COVID–19 vaccine. As

much as I love the fact that the vaccines are available and are a real blessing—something of a modern medical miracle—I can't get comfortable with the idea of using violence to force people, who have another opinion, to comply.

It seems morally problematic and morally unjustified—for that matter, indefensible—for the government to tell someone, ''If you don't get this shot, you will get fired;'' and, in fact, to tell their employer, ''You must fire this person if this person doesn't get the vaccine, even if this person has a good-faith religious belief against it, even if this person has natural immunity or has some particular medical condition causing his or her board-certified medical doctor to advise against receiving the jab.''

That isn't moral to say to that person, ''You didn't comply with a Presidential medical edict, so you are fired;'' and to tell the employer, ''If you don't fire that person, you are going to be the subject of punitive fines that will cripple any business.''

And I literally mean any business. I don't think there is a business in America subject to these mandates that could survive the crippling, deliberately cruel fines that are levied under them—not a one.

This isn't right. It is not moral. Deep down we know it.

In fact, according to a recent poll conducted and reported by Axios—hardly a rightwing publication—it involved a question, and the poll question was something along the lines of: Should a person who declines to be vaccinated be fired for not being vaccinated?

And 14 percent agreed that that is OK—14 percent. Only 14 out of 100 Americans said: Yeah, that makes sense, that is OK; fire this person, fire him, fire her. They don't matter.

It is compounded when you look at the tragedies imposed by the individual circumstances. The soldier; the sailor; the airman; the marine; the TSA worker; the Federal contractor; the employee of a subcontractor of a company with one Federal contract who does mostly non-Federal work; the mom, the dad working in a factory, in a school, in a floral shop—if any of those either have a Federal contract or have more than 99 employees, all of those people are having their livelihoods threatened.

It is not just a job. It is, in many cases—as is the case in the healthcare industry, for example—people who have spent a lifetime acquiring the skills and professional certifications, the degrees, the training, the education necessary in order to participate in that profession.

Many of these people, by the way, throughout the darkest hours of the pandemic, were the people working hardest to protect Americans, to make sure they had access to the healthcare they needed.

Those same people are now being told: You are not good enough. You don't deserve a job. You are going to be fired, even if you have a medical condition that precludes it.

Even if this could be morally justified, which it can't, one must ask the question asked by the U.S. Court of Appeals for the Fifth Circuit: Does Congress, does the Federal Government, have the power to order such a widespread vaccine mandate?

It doesn't.

The OSHA mandate, for example, constitutionally, it would have to be predicated on Congress's authority under the Commerce Clause, which gives us the power to regulate trade or commerce between the States, with foreign nations, and with the Indian Tribes.

Even as that provision of the Constitution has been interpreted really broadly since 1937—even under that broad interpretation, one that has seen only three acts of Congress over the last 84 years being deemed outside of Congress's authority under the Commerce Clause—when you have to almost try hard to pass legislation predicated on Commerce Clause authority that doesn't fall within it, but even under that, this doesn't pass the test.

It is not, by its nature, economic activity. In fact, it is not activity. You are punishing nonactivity.

Even under these high watermark precedents from the New Deal era establishing a very deferential standard of review for exercises of Commerce Clause authority by Congress, this doesn't even pass that. And even if it did, which it doesn't, you would still have to identify the case of the OSHA mandate a definable delegation of authority from Commerce using some intelligible principle authorizing this kind of action.

You will not find that. It is not there. I have reviewed upside down, sideways, backwards, forwards the statutory text at issue with regard to OSHA. It does not provide this authority. The moral authority is lacking. The constitutional authority is lacking. There is no power delegated by the Congress to OSHA to do this. It is not defensible.

I am glad that delays on some of these mandates have been imposed. I am glad that OSHA is at least agreeing to comply with the order of the U.S. Court of Appeals for the Fifth Circuit; and, at least for the duration of that litigation, enforcement will be halted.

I hope and I fully expect that the ultimate resolution of that case will be consistent with what the Fifth Circuit ruled last week. In fact, I have little doubt that it will be.

This is, in some ways, the most brazen act of Presidential overreach that we have seen in a single directive, since President Harry Truman, on April 8, 1952, issued an order seizing every steel mill in the United States for steel production related to the Korean war effort. Mercifully, the U.S. Supreme Court was able to intervene and, within a couple of months, invalidated that action.

This one is even clearer than that; but, more importantly, this one is more emotionally compelling than that.

That unconstitutional act of Presidential overreach affected a handful of steel companies. It certainly affected thousands upon thousands of workers. It didn't have the ability to affect directly or indirectly every single man, woman, and child in America. This one does.

That is one of the reasons why these moral and statutory and constitutional questions matter so much. That is why I have been coming to the floor every day, and why I will continue to do so indefinitely as long as it takes.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mrs. MURRAY. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. VAN HOLLEN). Without objection, it is so ordered.

The Senator from Washington is recognized.

Mrs. MURRAY. I ask unanimous consent to speak as if in morning business for 5 minutes.

The PRESIDING OFFICER. Without objection, it is so ordered.

NATIVE AMERICAN HERITAGE MONTH

Mrs. MURRAY. Mr. President, I rise today in recognition of Native American Heritage Month. As a Senator from Washington State, I am proud to represent 29 federally recognized Tribes.

In Washington, we understand the importance of the sovereignty of Tribal Governments. And anyone who knows me knows, I believe a commitment is more than just words. It is about action.

At the start of this year, when we passed the American Rescue Plan to get America up and running again, it was the single largest Federal investment in Tribes ever—more than $32 billion for Tribal Nations.

Since then, I have spoken to many Tribal leaders in Washington State about what this has meant for our Tribal communities.

A housing grant to the Muckleshoot Indian Tribe helped provide homes for an additional 25 families.

The Lummi Nation created new opportunities for education and job retraining.

The American Rescue Plan helped the Tulalip keep Tulalip-owned businesses, who have been struggling since the pandemic, afloat.

Action on our commitment has helped Tribal members in my home State stay housed, get back to work, keep their small businesses open, and continues to make a difference in a thousand different ways.

Now, these outcomes weren't inevitable. They happened because of intentional and specific policy decisions this

Congress made to support Tribal Nations.

So if we are serious about showing a real commitment to Tribal communities during Native American Heritage Month, then we need to continue to prioritize Tribal communities in all of our policymaking.

Infrastructure in Indian Country—everything from roads to bridges, to broadband—has been underfunded for too long. The bipartisan infrastructure bill, which is now signed into law, will make $13 billion in direct investments in Indian Country, with tens of billions more in Federal grants and future funding opportunities. This will mean clean drinking water, access to high-speed internet, transit to connect communities, and more.

Now we have another opportunity to show our commitment to Tribal communities with the Build Back Better Act. Just like everywhere else in this country, childcare is a crisis for Native communities. Right now, about one out of every four Native Americans in this country is experiencing poverty. That is higher than any other group. So when 1 in 10 Native American parents have to quit or change their job because they can't find or afford childcare, we are making a tough situation worse.

My childcare proposal in Build Back Better is going to cut the cost of childcare by thousands for Tribal families—with many paying nothing at all for childcare—and it is going to help get more slots open everywhere we need them, so parents won't be stuck on waiting lists for months on end.

It is our government's duty to make investments like this one in Indian Country because if we really believe in Tribal sovereignty and acknowledging the role our government has played in centuries of persecution Native peoples in this country have faced, we must also take action to create real opportunity for people; action on quality, affordable childcare, housing, home care, and more.

Build Back Better is going to make a big difference for Native communities, but there is more we need to do to address the specific needs of Native communities.

We have to build on President Biden's Executive action to address the epidemic of missing or murdered indigenous peoples, especially to protect Native women and girls. We must reauthorize the Violence Against Women Act and strengthen that legislation to empower Tribal Nations to hold perpetrators of crimes committed on Tribal lands accountable. And living up to our commitments is also about representation and a seat at the table.

I was overjoyed to strongly support the confirmation of Deb Haaland, who is already blazing a trail as a historic Secretary of the Interior and a powerful voice for Tribal interests.

I was proud to recommend Lauren King, a citizen of the Muscogee Nation and a Tribal law expert to serve a lifetime appointment as a Federal court judge in Washington State—the first Native American Federal judge in my State's history and just the sixth ever in American history. And I am glad to see more than 50 Native Americans serving in key political positions throughout the Biden administration. I look forward to seeing many more.

So, on this Native American Heritage Month, let's resolve to build on the important work this Congress has done so far to support our Native communities.

As a voice for Washington State Tribes in the U.S. Senate, I will always advocate for Indian Country and fight to ensure the Federal Government lives up to its sacred commitment to indigenous people across the country.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. BROWN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

CHILD TAX CREDIT

Mr. BROWN. Mr. President, this week, for the fifth month in a row—and the Presiding Officer has been standing with us on this important issue—parents in Ohio and Maryland and all over the country, once again, see $250 or $300 or, if they have two children, $600 in tax cuts directly into their bank accounts.

Think about this: 90 percent of Ohio children, this year, will have at least a $3,000 tax cut, not a deduction. This is real money in people's pockets. This is 90 percent of Ohio families who will get at least a $3,000 tax cut, and that is if they have one child. If they have more, they will get a bigger tax cut.

You know, we know how hard parents work at their jobs and at raising their kids. Any parent knows how much work it is to take care of children, especially young children. It has gotten only harder and harder over the last year and a half.

I hear some of my colleagues, especially on that side of the aisle, say—you know, they forget what hard work it is to raise children. And I watched what we were able to do on this with the chairman of the Finance Committee, who just walked in, Senator WYDEN, and his leadership on this largest tax cut for working families in my lifetime.

So often, we know hard work doesn't pay off. Think about the past few decades: The stock market went up; productivity went up; executive compensation has been stratospheric; yet, essentially, wages for most workers in this country have been flat.

And you know how expensive it is to raise kids. Healthcare, school lunches, diapers, clothes, school supplies, braces, sports' fees, camp fees—the list never seems to end. And one of the biggest expenses for so many families is childcare. So parents feel like they are stuck. The more they work, the more expensive childcare gets.

One of the reasons that people haven't returned to the workplace as much as some academicians or some professors or somebody predicted—it is not because we were providing unemployment compensation. That just kept them alive. It is because they can't find affordable, accessible, safe childcare. So that is why parents feel like they are stuck. It is why we passed the child tax credit—as I said, the largest tax cut for working families ever. It is about finally, finally making hard work pay off so you can keep up with the cost of raising a family.

One of the joys of this job—and I know that the Senator from Oregon and the Senator from Maryland share this because they do things like this—is we put on our website: What does the monthly child tax credit mean to you?

We started this in July. We voted on it, on this floor, on March 6. Five days later, President Biden signed the law. We all went to talk to Secretary Yellen about getting these checks out quickly. On July 15, 4 months after we voted for it—not even 4. Help me with my math. Three months after we voted for it, these checks started showing up.

In my State, it was 2.1 million checks that went out. There were 2.1 million individuals who got this child tax credit—you know, a million-and-some families because, obviously, some have more than one child in a family in many cases. Then they got a check on August 15; September 15; in October; and just this week, on November 15.

We know it cut the rate of child poverty by 40 percent. We also know that it helped families with school expenses or with, maybe, putting a little bit of money aside for Bowie State or Stark State, a community college in Ohio.

Maybe it was just a way that families—I mean, we know how there are so many families who are really anxious at the end of the month. Maybe we don't talk to enough families like this around here, but for families who are anxious at the end of the month, getting this $200 or $300 or $600 check in the middle of the month relieves the anxiety so many families have just to pay the rent because we know so many families, in that last week of the month, cut back on food a little bit, cut back on trying to figure out a way to get through the month so they can pay their rent at the beginning of the next month.

So, on this website, when we ask people what this means to you, we just get the most wonderful stories.

Lisa said the tax cuts help her afford ''diapers and school supplies . . . and [now] we [can] put a little into starting a 529 college fund.'' It is so exciting. Now we can finally ''save for education.''

Lin from Columbus: ''It kicked in right at a time when kid birthdays were happening for us, plus back to

school shopping, and several unexpected vehicle repairs were needed as well—it's made a very helpful impact.''

The Presiding Officer, Senator VAN HOLLEN, sits on the Banking and Housing Committee with me. He knows that, before the pandemic, 25 percent of renters in this country paid more than half of their income in rent, and if one thing goes wrong—your car breaks down; you get sick; your child gets sick; you miss a few days of work—you can be evicted. This will stop that from happening in many cases.

Jeff from Cincinnati said it helps him afford ''car insurance for a 17-year-old,'' a 17-year-old who has a part-time job after school.

The story we hear over and over is how expensive childcare is, how parents use this money to afford childcare so they can go back to work or, maybe, work more hours than they are working.

CeCe said her tax cut helps her pay for daycare. ''Daycare is the same amount as my mortgage payment for 4 days a week! So this is so, so helpful,'' she said.

Sarah said: ''It has been critical as I started my unpaid maternity leave at the end of July.''

I mean, we want people to be able to give birth and then stay with their child, their newborn, for a period of time. Many, many, many people in Baltimore, in Cleveland, in Portland don't have any kind of leave—and how important it is that they can, maybe, stay a little longer with a newborn child and bond with her or him.

Courtney, from Athens, near the Ohio River, said the CTC is ''slightly more than half the cost of part time daycare tuition per month—much appreciated help getting kiddo back into childcare and keeping [my husband and me] in the workforce.''

These tax cuts mean more parents can afford to work and can afford to keep up with the extra cost of raising kids.

When these tax cuts are fundamentally stripped down from everything else, it is about the dignity of work. All work has dignity, whether you punch a clock or swipe a badge; whether you work for tips; whether you are on salary; whether you are raising children or caring for an aging parent. Raising children is work. We never should forget that: raising children is work.

It is a hell of a lot more work than moving money from one overseas bank account to another, as this body falls all over itself over the years giving tax cuts to rich people.

It didn't stop Senator MCCONNELL from rewarding the wealthiest CEOs and hedge fund managers and Swiss bank account holders. We remember what happened. When they did their tax cut 4 years ago, everybody in our—I mean, look at the difference. Four years ago, they passed the tax cut. You could see the lobbyists lined up in the hall outside Senator MCCONNELL's office. Four years ago, we passed the tax cut. Almost all Republicans voted yes; almost all Democrats voted no. Seventy percent of that tax cut went to the richest 1 percent.

Earlier this year, we passed the largest tax cut for working families everywhere. Everybody on this side voted yes; everybody on that side voted no. I mean, whose side are you on? Apparently, we know that. Senator MCCONNELL and his crowd—they are always for the billionaires, they are always for giving more tax cuts, while Senator WYDEN and the Finance Committee are fighting for middle-class tax cuts.

They then promised—and we all heard this—they promised that these big tax cuts for billionaires would trickle down, and they would hire more people, and they would pay higher wages, and the economy would grow. Well, it didn't exactly work that way. They kept so much of it for themselves. They spent that money on stock buybacks, and we know what happened then.

So the question is, Do you want tax cuts for billionaires and corporations or do you want tax cuts for working families? We want tax cuts for working families, and so do Americans from all over the country overwhelmingly from all kinds of backgrounds, from Chillicothe to Xenia, to Springfield, to Portsmouth, to Ravenna—all over the country.

Every single month now, we are showing parents and workers we are on your side. We will not stop fighting to make sure parents' hard work pays off for years to come.

The child tax credit—we will make it permanent. It may not be this year, but we will make it permanent. As Senator WYDEN has said, it will become a lot like Social Security. It will be transformational. Americans will love it the way Americans have gotten used to and depend on and love Social Security. It is part of who we are as a nation.

I yield the floor.

The PRESIDING OFFICER. The Senator from Oregon.

UNANIMOUS CONSENT REQUEST—EXECUTIVE CALENDAR

Mr. WYDEN. Mr. President, in a few moments, I intend to put forward a request for the Senate to take up and approve the nomination of a very special Oregonian; that is, my friend Chuck Sams, President Biden's choice to lead the extraordinarily important National Park Service. I am just going to take a few minutes to talk about Chuck Sams and make sure the Senate understands why this is the right person for this very important job.

First of all, I would say to the Senate, we have heard the national parks described as America's best idea. That is because they form a network of treasures that no other country can match. But the fact is, the National Park Service is not only about the views and the photo-ops; the Director of the National Park Service is in charge of an organization of over 22,000 employees and almost a quarter-million volunteers. The Park Service generates tens of billions of dollars of economic activity. The people of my State, Oregonians from one corner of the State to the other, particularly understand how critical outdoor treasures are for rural economies and rural jobs.

There are park units in every State in the Nation—urban parks, rural parks, historic American buildings, ancient archeological sites. And the personnel at the Park Service—what incredible people. They do it all, from education to preservation to maintenance, and they are also now doing more resilience against wildfires.

That is why it is so important we have strong leadership at the National Park Service, because when you have employees taking on such diversified challenges and you have the Park Service woven into the fabric of every State and so many communities, you need somebody at the top, the leader, to be capable and ready to take on these enormous challenges. Chuck Sams is that person, there is no question about it.

I want the Senate to know that I have known Chuck Sams for years, and I have personally seen in action his dedication to communities and to the outdoors. He has been a longtime Umatilla Tribal leader and a key member of the Northwest Power and Conservation Council, working with officials from across our region. He is also a veteran of the U.S. Navy. I know Chuck Sams to be a role model in the stewardship of America's lands, our waters, our wildlife, and our history.

The Congress and parkgoers are going to be able to count on him in the months and years ahead, after he is confirmed, because we know the Park Service faces some very big challenges. There is, for example, a multibillion-dollar maintenance backlog. The parks are often very crowded. They are confronting the effects of the climate crisis, whether it is wildfire, floods, or droughts. The list goes on and on. There has been for too long—too long—a workforce culture fraught with gender discrimination and harassment.

For almost 5 years, the Park Service has been without a Senate-confirmed Director. The reason why I am here is, I would say to the Presiding Officer and to my colleagues, I am here to make sure that the Senate doesn't wait another single day after 5 years to confirm a capable leader, Chuck Sams, as the Director to address these challenges I have described. He is the right nominee at the right time. I want Senators to know I base this not on reading a bunch of resumes or bios about Chuck Sams. I have seen it myself. I have seen Chuck at work in our State. He is committed. I support him 110 percent.

Therefore, Mr. President, I ask unanimous consent that the Senate proceed to executive session to consider the following nomination: Calendar No. 508,

Charles F. Sams III, of Oregon, to be Director of the National Park Service; that the nomination be confirmed, the motion to reconsider be considered made and laid upon the table with no intervening action or debate; that no further motions be in order with respect to this nomination; that the President be immediately notified of the Senate's action; and that the Senate then resume legislative session.

The PRESIDING OFFICER. Is there objection?

The Senator from Alaska.

Mr. SULLIVAN. Mr. President, reserving the right to object, I want to commend my colleague from Oregon and his comments. As a matter of fact, I don't disagree with pretty much anything he said.

I had my first good meeting with Mr. Sams this morning, and I would agree, I think he is qualified. I am particularly impressed with his background as a Native American, as a veteran.

One thing I like to talk a lot about is how our Alaskan Native American populations serve at higher rates in the military than any other ethnic group in the country—special patriotism. Mr. Sams certainly carries that tradition on quite well.

And I have already talked to Senator WYDEN. I intend to work with him and Mr. Sams just on a few more issues, a few more discussions. Again, we had a very good conversation this morning.

This is nothing about his qualifications, but I wanted to make sure the administration is aware of some issues, at very high levels, as it relates to this position, this job. And, again, I agree with my colleague from Oregon; this is an extraordinarily important Federal Agency. As a matter of fact, it is so important for my State that I want to explain a little bit to my colleagues, many of whom don't really know what the National Park Service does. But to my State, it is enormously important; it is powerful; and it can touch on people's lives in huge ways.

Let me just give you a little bit of the numbers. The Federal Government manages roughly 66 percent of the lands in Alaska. Of that, the Park Service controls 55 million acres. Two-thirds of all National Park Service land—two-thirds of the land that Mr. Sams will be in charge of is in my State. A lot of people don't recognize that. A lot of people don't understand that. Alaskans understand that—two-thirds.

So he is one of the big, important landlords of the great State of Alaska. And, as you can imagine, this Agency has outsized influence in Alaska beyond what these numbers represent—for hunting, for fishing, for transportation, for culture, and for people's livelihoods.

And this has been an Agency, to be quite frank, that has been abusing its power in Alaska for decades—Democrat administrations and Republican administrations.

In 1980, this body passed the Alaska National Interest Lands Conservation Act—what we call in Alaska ANILCA. The Congress took 100 million acres of Alaska lands. We weren't supportive, by the way, Alaska—100 million acres. That is bigger than almost any State represented in the U.S. Senate, bigger than two Minnesotas.

And a huge part of ANILCA laid out how the National Park Service would interact with Alaskans. For decades, Alaskans were saying that the way in which the National Park Service was treating Alaskans—by the way, Alaska Natives in particular—was not according to the law, was not according to ANILCA.

And it wasn't just Alaskans saying this. In the last 4 years, there have been two U.S. Supreme Court decisions—they are referred to as the ''Sturgeon'' decisions—where an Alaskan who wanted to go hunting sued the National Park Service, and it went all the way to the Supreme Court. And the U.S. Supreme Court twice in the last 4 years, 9 to 0—9 to 0—agreed with Alaskans that the National Park Service was not following the law as it related to ANILCA.

As Justice Kagan, who wrote one of the opinions, said, ''Alaska is often the exception, not the rule'' to issues relating to Federal lands and access.

Now, as you can imagine, the National Park Service did not like getting slammed by the U.S. Supreme Court twice 9-zip, but we liked it. It was a vindication of what Alaskans, for decades, have been saying about the abuse of power of the National Park Service.

So I want to work with Senator WYDEN and Mr. Sams on further conversations, soon—we are not trying to block this; I know the National Park Service needs leadership, and I think he would be a good leader—but to look at making sure the implementation of these two U.S. Supreme Court decisions, 9 to 0, are followed through by the entire bureaucracy. It is not much to ask.

These are topics I raised with Mr. Sams today. He seemed to be in agreement with me. But these issues are enormously important to the people I represent.

And I am going to mention one final thing, and it is not really in Mr. Sams' area of expertise, but I mentioned this to him as well.

All Americans have been experiencing economic, pandemic-related pain over the last 20 months. My State, I think, has been hit as hard as any other State, particularly on the economic side. And I want to just raise this topic right now because I am going to come down on the Senate floor and talk about it a lot more here. But it relates to some of these issues.

This administration, the Biden administration, in the last 10 months, has issued 19 Executive orders or Executive actions solely focused on my State—19. There is no other State in the country—not Maryland, not Oregon, no other State in the country—that is getting this kind of attention from the new administration, and it is attention that we don't want because almost every one of these Executive orders and Executive actions is hurting working families, is hurting our economy, is hurting access to our lands at a time when we are already hurting.

I just want to ask my colleagues, respectfully, especially on the other side of the aisle, could you imagine a Republican administration coming in and saying, ''We are going to issue 19 Executive orders and actions targeting Maryland or Delaware or Oregon or Massachusetts''? Senators would be on the floor, rightfully, sticking up for their State and their fellow citizens.

This is a challenging time right now. Working families are hurting with inflation, high energy costs, and we have an administration in the White House that thinks it is fine to target the great State of Alaska. Well, it is not fine. It is not fine. It is a war on working families in my State, and I would hope all of my colleagues would recognize that this isn't appropriate. This isn't appropriate.

And it is not just these actions. The White House has made it known that it has gone to financial institutions throughout the country—banks, insurance companies—saying: Don't invest in American energy projects in the Arctic—also known as Alaska.

So I am not going to hold this against Mr. Sams. My colleague from Oregon I have a lot of respect for. But, literally, every major project that is resource development, employs people, helps working families—by the way, there are some that aren't economic. There is a law that we passed in the U.S. Senate 3 years ago to help Alaska Native Vietnam veterans. It was my bill. I care deeply about these great warriors who were really screwed by their country when they came home from Vietnam.

The administration has delayed the implementation of that bill for 2 years. There will be Vietnam veterans—Alaska Native Vietnam vets—in my State who will die before they get the benefit because they just thought they could do another hit on Alaska.

So I ask my colleagues to just put yourself in my State's position. None of you would accept that. And I am going to start talking about it, and I am going to start raising these issues. And I hope I can get some of my colleagues—Republicans and Democrats—to maybe reach out to the White House, going: Hey, this really isn't appropriate. Alaska has had a rough time. Everybody has had a rough time in America, but really? Nineteen Executive orders and actions?

These are just the Alaska-specific ones. There are broader Federal ones that impact us too. But I want to work with Senator WYDEN. I want to work with Mr. Sams, particularly on that issue I raised earlier. I think he is

going to be very well qualified. I admire his desire to serve, his background, and especially his Navy background.

And I intend to lift my hold very soon, but right now I am objecting. But my goal would be to have this nominee, who is qualified, after further discussions with me and Senator WYDEN, moved to be confirmed by the U.S. Senate. But, for now, I object.

The PRESIDING OFFICER. The objection is heard.

The Senator from Oregon.

Mr. WYDEN. Mr. President, I just want to tell the Senate where we are now and what is ahead.

I have asked unanimous consent to confirm an Oregonian whom I have watched in action, Chuck Sams, to head the National Park Service, which has gone leaderless for 5 full years.

Now, my colleague has said, to his credit, that Chuck Sams is very well qualified, that he is a good man, that he had good discussions with him. And I would just say to the Senate and my colleague—my colleague and I have worked together often here in the Senate. I remember, as chairman of the Finance Committee, we had some issues on the budget. And we got together, and within 20 minutes we had it worked out.

So I would just say to my colleague, I am ready from this minute on to get together with you, to get together with Mr. Sams. We are going to be here, it sounds like, at least today, and then we will have to see.

But I just hope we can work this out because I listened to the Senator very carefully. And I have been to Alaska. I went with your colleague Senator MURKOWSKI when I was chairman of the Energy Committee. And I heard my colleague's concerns.

Well, to get those kind of concerns addressed—many of them—you have got to have a Director; you have got to have somebody you can hold accountable, somebody you can get on the phone and you can talk to about issues. Chuck Sams is exactly that kind of person.

So I want my colleague to know we are going to be here the rest of today and, it sounds like, some of tomorrow, but we will have to see. I hope that we can get this worked out, and I want to pledge to my colleague that I will, myself, be willing to work with him on issues he has with the State, just the way we did on those tax concerns with respect to the budget. And let's see if we can get this done before we leave this week because the longer we wait—I mean, just think of the Park Service here over the holiday. There are going to be a lot of people—because the Park Service is part of the treasures of America—who are going to want to enjoy those facilities.

So this has real-world consequences. I look forward to working with my colleague, and I hope—I hope—we can get this done before we leave, and I pledge to my colleague that I will work with him to respond to his concerns not just about this nominee in the context of this nominee but in the context of the concerns he has for his State.

I yield the floor.

The PRESIDING OFFICER. The Senator from Alaska.

Mr. SULLIVAN. Mr. President, I want to thank my colleague from Oregon, and I will commit to working with him to try and get this done before we head out to recess.

We know the treasures of Alaska. As I mentioned, two-thirds of all the Park Service in the country is in my State, which is why I want to make sure I am having followup conversations—I had a good one already with Mr. Sams—to get commitments on a few additional issues that matter deeply not just to the Park Service and for America but, really, to my State. But you have my commitment to work with you and Mr. Sams on a few more of these issues.

And, if I may, for all my colleagues, right—and I am glad to hear Senator WYDEN mention this—this shouldn't be happening with one State. There is a Biden White House war on the State of Alaska. No one is getting treatment like this, and it shouldn't be this way. If a Republican President were in attacking Maryland or Oregon like that, I would call the White House going: Hey, lay off, guys. Lay off.

So I sure hope some of my colleagues—Republican and Democrats—can send the message to Joe Biden, the President, that you know, the war on working families in Alaska is not really a good idea. They are Americans, too, and they have got a lot of resources to produce for our great Nation, which we need right now.

So with that, I yield the floor.

The PRESIDING OFFICER. The Senator from Oklahoma is recognized.

CORONAVIRUS

Mr. LANKFORD. Mr. President, on September 9, President Biden told the American people that he was losing patience with them and they needed to get vaccinated right now. He laid down a series of Executive orders on Federal employees, on Federal contractors, on companies that had—individuals that had 100 employees or more, on individuals that worked in any healthcare-related, anything that dealt with Medicare or Medicaid. It reached out to millions of people.

He set a date that was within 3 months, knowing full well it would take months to actually write the rule and it would create chaos across the country as everyone tried to figure out how to do this mandate.

I fully believe that was the purpose of setting a close deadline; it was because it would have that much chaos in the country dealing with the vaccine mandates. Well, mission accomplished. It has created chaos across our economy and across lots of families.

What is the situation right now in America dealing with COVID?

We are on the backside of our second peak. We have seen hundreds of thousands of people lose their lives to COVID. We have seen hospitals fill, get back to order; fill again, get back to order.

But in the meantime, three vaccines have been developed, multiple different treatments have been developed, a multitude of tests have been developed, which has been the primary issue that we have every year with the flu.

We don't panic every year on the flu because we have testing. We have treatment. We have vaccines. We now have, for COVID, testing, treatments, and vaccines. It becomes much more manageable.

In the meantime, right at 80 percent of all Americans who are 12 years old or over have already had at least one dose of one of the vaccines.

Let me run that past you again: 80 percent of Americans have had at least one dose of one of the three vaccines, of those 12 years old or older.

About 45 million Americans have recovered from COVID; had it, tested positive, and have recovered. The vast majority of Americans, by far—like, not even close—the vast majority of Americans have been vaccinated or have recovered from COVID or both.

But is the administration OK with that?

No, they are not. The administration has laid down their own law to say, if Americans do not get the vaccine—those 20 percent left that haven't gotten the vaccine that are 12 years old or older, if they don't get the vaccine, this administration is going to find some way for them to lose their job; which, for many people, will also mean lose their insurance; lose their pension; and, sometimes, lose their home.

But the President's response is: I don't care. Go get the shot. That is what I want you to do.

Well, Mr. President, mission accomplished.

Let me tell you a story of an individual that works in the eastern part of my State, who works for one of those companies that is 100 people or more. He didn't want to have the vaccine. The reason is not even important, but he said he didn't want to take the vaccine. So what happened in his company of 100 or more? They fired him a couple of weeks ago.

You are welcome, Mr. President. Thanks for firing him.

Oh, it gets better. He lost his house because he couldn't pay the mortgage, and this adult man has now moved in with his family while he tries to figure out what happens next for him.

Do you know why?

Because the President said he was losing patience and he didn't care if this guy lost his house, lost his job, lost his insurance. The President was just saying, go get it, or else.

Well, thanks. Right before Thanksgiving, he is experiencing the ''or else.''

One of my constituent's husband is facing termination. He is from another one of those large companies. He has worked for them for 30 years. He has a

secret clearance from the DOD. And his doctor gave him an exemption because his cardiac numbers fluctuate so much. And he is one of those high-risk individuals for blood clots, which can be a side effect of the vaccines. So his doctor has encouraged him not to take the vaccine.

So he went into his job. He asked for the medical exemption, and he was given two forms to sign. The first of the forms said he had to agree to take the vaccination or he would lose his job. The second form agreed that, if he took the vaccination, he would not sue the company if he had a negative reaction.

So here is a man who has to choose between taking the vaccine, knowing that his doctor has told him not to do it, and if he does take it, if he has a negative reaction, the company wants to be held harmless for it. And he has to sign a document saying the company will be held harmless for it or lose his job.

Do you know why?

Because President Biden said he was losing patience.

So this family gets to sit around over Thanksgiving not talking about football but talking about whether he is going to lose his job or possibly have a blood clot in the hospital.

Which would you like to have that conversation on over Thanksgiving?

There is a company that does electrical engineering that also has one of those Federal contracts they talk about. Some of the employees don't do the Federal contracting. They work for other issues. Fifty people of the 250 in the company have said they don't want to take the vaccine, and so they are in the process of losing their jobs. And that company will not be able to fulfill its Federal contract because hiring 50 more electricians is not that simple right now with the economy that we are currently in.

A constituent told us that her employer is going to lay her off on December 8 because she hasn't had the vaccine yet. So she will spend Thanksgiving discussing this with her family as she approaches the time where she is about to be laid off. She works in one of those companies that has a Federal contract. She reached out to her primary care doctor, who is at the VA, by the way, and the VA instructed her that they are not writing exemptions for medical exemptions.

She is on her own.

Why?

Because the President is losing patience, and he has decided he is going to throw all of these families in chaos or they are going to lose their job, because he said so.

Why have I been fighting this mandate since September 9 when the President actually announced it?

Because it was obvious to me what was coming. It was this.

Everyone could see it, apparently, but the White House. Americans are stubborn people. That is what has made us the most prosperous, freest people in the world. We are entrepreneurs. We take risks. We understand the consequences for our risks. But we also go do because we can; we are Americans.

And now the President of the United States has announced: I don't care; you are going to get this, or else.

So what is the real effect of this? All of this chaos?

Oh, this is just part of it. There is a whole lot more.

How about the EMS folks that are in rural Oklahoma, that are having a hard time actually keeping some of their drivers and folks in because they have chosen not to take the vaccine?

What happens in 3 weeks from now when people get sick at their house or have a heart attack and EMS can't respond because those folks got fired from their jobs because the President said, I am losing patience? What happens?

I will tell you what happens. People die. Other families are going to struggle through this process as they are figuring out where they are going to go to work because they lost their career, because the President said: I have lost patience with you.

Tell me this: For the person that is the JAG officer in the military, works in the National Guard, and for whatever reason—whether it is a religious accommodation, medical accommodation, or whatever it might be—they chose not to take this vaccine, when they get a dishonorable discharge, what happens to them?

They lose their law license is what happens to them. They are disbarred, and they are no longer practicing their profession.

What happens to the State trooper in Oklahoma that also serves on our National Guard?

When they get dishonorably discharged, they don't just lose their military career; they lose their civilian career.

What happens to the nurse or doctor that serves with the National Guard? When they get drummed out, what happens?

They lose their military career and their civilian career. That is what happens.

Do you know why?

Because the President decided he was losing patience with the American people and they have to do what he says to do, not what they want to do. That is why all this chaos is happening.

I heard from a constituent, 28 years of Federal service—28 years of Federal service. I am not going to give the administration that they work in, but they work behind the scenes in an exceptionally important, exceptionally difficult task—serving their neighbors as a Federal employee. She doesn't want to retire, but she doesn't want to take this vaccine either.

So do you know what she is doing?

She is retiring.

And what is going to happen in this agency in Oklahoma when they lose this cornerstone person at this Agency?

They will struggle to figure out what she did, how she did it. And people in Oklahoma will get less help in that Agency because a long-term, vital civil servant is about to get run out of civil service because President Biden decided he lost patience with her.

That wasn't in her civil service contract. That was never negotiated with any other collective bargaining rights agreements, never. There is no addition in any collective bargaining rights agreements for Federal employees that they have to get a vaccine mandate if the President decides that they do, but he decided—that is, President Biden decided—he was going to take this on.

And so she is going to be discussing over Thanksgiving what she is going to do post-retirement, wishing that she could stay a little longer to be able to build up a few more years, and thought she was going to be able to, but, instead, she got ran out because she and the President had a difference of opinion about a brandnew vaccine.

Now, I have said to this group before several times—and I will say it again—I have had the vaccine. I encourage others to take the vaccine. Eighty percent of Americans who are 12 years old or older have had the vaccine.

There are plenty of Americans who have had the vaccine who support the vaccine but do not want their next door neighbor to get fired because they disagree on the vaccine. In fact, I don't know a lot of people who do, though I have met some that are just that heartless to be able to say: I don't care what you think. I want to feel better forcing you to go get the vaccine.

I have met some of those folks, but I don't meet many of them. Most of them say: I freely made the decision; they should be able to freely make the decision, as well.

But apparently that is not where the President is and, unfortunately, that is not where some of my Democratic colleagues are because multiple times we have brought an end to the vaccine mandates to multiple committees in multiple places over the last several months and it gets knocked down every time.

Just this week, we filed a Congressional Review Act dealing with just the OSHA piece. We have another one coming dealing with all those on CMS to make a simple statement: We have got to stop this vaccine mandate. It is causing chaos in our families. It is causing chaos in our economy, and anyone who doesn't think it is is not talking to people at home.

So we will bring this in the next 18 days to the floor of this Senate, and we will force a vote on it and put everyone on record: Do you stand with the American people, who strongly affirm the vaccine but strongly oppose the mandate, or will you be one to say: I don't care. I stand with the President. I am losing patience with people, this 20 percent that haven't done the vaccine. I

am losing patience with them, and I am just going to force them to do it, as well—because that decision is coming to every single person in this body.

This could be turned off right now, and one section of it already is turned off. The Fifth Circuit Court reached in on the issue of private employers and said that this was way overly broad of the President. No kidding. It was unconstitutional for the President to reach into companies and to say: I don't care who it is, how important they are to the company. If you don't make them do the vaccine, you have to fire them.

The Fifth Circuit said you cannot do that. Thank you, Fifth Circuit, for finally joining in on that.

OSHA has now said that they are not going to enforce that, but there are lots of other companies that have done it anyway. And, I will tell you, for this individual in Eastern Oklahoma who has already been fired and lost his house, it is too late for him for suddenly the Biden team to say: Just kidding. We are going to pull that back. His life has already been wrecked by you.

What else is happening? I have reached out to multiple different Agencies to be able to talk this through. It has been fascinating to me, when I have talked to different Agencies. By the way, the Federal Agency mandate for all Federal employees is next week to be able to have that done. But when I talk to leaders of Agencies of multiple different Departments across this town, none of them seem to know how many of their employees have actually been vaccinated yet—none of them. They all say: Well, we think it is quite a few.

I say: How many folks have not been vaccinated?

We have x number of folks who have been reported to us, but they don't seem to know. It has become chaotic.

For Federal workers, their unions have finally stepped in—finally. I have been shocked at how slow the Federal unions were to this. They finally stepped up and asked for an extension of the President to say: Don't put the mandate down for next week. Give people more time because, literally, people are sitting around over Thanksgiving deciding whether they are going to keep their job or not.

And if 10 to 20 percent of the workforce across the Federal workforce leaves, we are in such chaos that there is no way we will be able to finish serving people as we desperately need to be able to do across the Federal Government.

What would I recommend? I had some very frank conversations with the Equal Employment Opportunity Commission, or the EEOC. It was interesting to me, when I visited with the EEOC. That is the group that protects workers—Federal workers or private—from discrimination and protects workers from inappropriate termination. When I talk to the EEOC, what I hear from them is that they weren't consulted through the process of developing this new vaccine mandate and all the exemptions that should be in place.

Can I just tell the workers of my State and the workers across the country a simple thing? If your employer will not accept your religious accommodation that you put in or your medical exemption that you put in—if they do not accept those—you need to go to the EEOC and file a complaint because the EEOC has rules about terminations that are inappropriate terminations. If individuals are being terminated from private companies, even if they are Federal contractors or Federal employees, I encourage you to go to the EEOC and file a complaint if they are not hearing your medical accommodation or your religious accommodation. That is your right as an American.

When the President of the United States is running over your rights, you have every right to be able to appeal that personally. You don't have to hire an attorney. You can file that complaint on your own to be able to make sure that your employer knows that you are filing an EEOC complaint against them for inappropriate termination, for not accepting your medical exemption and your religious accommodation.

Interestingly enough, when I approached the Office of Management and Budget a month ago about how they are going to handle religious accommodation, they said: It is not the business of Federal workers to decide and individuals' faith. We are just going to accept that.

But when the document came out, there was a six-part test of whether you are religious enough to be able to turn down the vaccine. They literally created a six-part test that every supervisor can go through and check to determine if you are religious enough to be able to turn this down.

This would be the first time that I know of that the Federal Government has actually reached into an entity, to individuals, and said: We are going to decide for you how religious you are.

That is how crazy this has become.

I encourage you, again, if individuals have said that you are not religious enough to be able to ask for this accommodation, go to the EEOC, file a complaint against your employer—whether that be a Federal Agency, whether that be a private entity—and make sure that they are well aware of what is going on.

If you work in a Federal Agency and you have an initial appeals process that actually goes through, go through that. Go through that process. But if you are denied or not heard, you do have rights as an American, and I would encourage you to be able to stand up for your rights as an American against unjust hiring and unjust firing in this process.

Let me read this last letter to you. As we have fought through this process and find every leverage point I can find for the people in my State to be able to make their own decisions, it has been difficult to be able to talk to people in the struggles that they have.

Let me read one. This gentleman wrote to me:

> I retired after 20 years of Active-Duty service in the military to enjoy time with my family and the supreme blessings of freedom and peace our country has secured at the expense beyond human measure. Now, many of our undaunted servicemembers and veterans alike face possible unemployment because we refuse to take a vaccine. Some are being coerced into taking it because they can't support their families while unemployed. The very people who risked their lives and the well-being of their children face persecution for a personal medical choice.

His comment to me: This is not American.

I agree. That is why we are fighting this. That is why we are continuing to push this. That is why we are bringing a Congressional Review Act up to put every single person in this body on record: Do you support forcing people to take a vaccine or be fired, or not?

I do not, and I hope that 99 other of my colleagues also do not.

I yield the floor.

The PRESIDING OFFICER (Ms. CORTEZ MASTO). The Senator from Kansas.

NOMINATION OF SAULE OMAROVA

Mr. MORAN. Madam President, I rise today to express my opposition to President Biden's nominee to be Comptroller of the Currency, Dr. Saule Omarova.

Although not the most publicly known office, the Comptroller of the Currency is a prominent and influential position that regulates and supervises all national banks. Given the undeniable importance of this office to the economy and to Americans, it has long been kept free of divisive politics and extreme views.

While I talk about the Office of the Comptroller of the Currency and I talk about banks, my concerns are certainly more than just the financial institutions that are in our country's economy. It is the people, their customers who are served, that bother me or worry me the most.

Rather than offer practical ideas for strengthening our Nation's banks, Dr. Omarova advocates for the elimination of all commercial banks—the very financial institutions she should be interested in partnering with. Instead, she wishes to replace them with one bank—one bank—the Federal Reserve.

While the Comptroller might not have direct control of the Federal Reserve's structure, the reach of the position cannot be understated. The Office of the Comptroller is a member of the Federal Financial Institutions Examination Council, the Financial Stability Oversight Council, and even the Board of the FDIC, an Agency Dr. Omarova hopes to eliminate.

Although the doctor claims to support community banks, her plan would relegate them to mere franchises of the

larger Federal Reserve, and her comments have alarmed many Kansas community bankers. They have grave concerns about her policies that would ''end banking as we know it.''

One Kansas banker says:

> I have severe concerns with the President's nominee to be the Comptroller of the Currency. Her support of moving the payment system entirely through the Federal Reserve and her commentary in favor of abolishing the FDIC moves the entire banking system toward a government-controlled financial system. Eliminating the dual banking system would be disastrous for entrepreneurs and consumers alike in the marketplace.

Another banker from Kansas said:

> We expect our regulator to supervise safety and soundness for banks in the system, not to propose and force feed social agenda items to us.

Local lenders—I certainly know this in the State of Kansas—are the cornerstone of many small towns, and the Comptroller should appreciate the value that community banking brings, what I call relationship banking. They provide crucial lending services for the underbanked populations in rural and urban areas alike. Eliminating the one-on-one, personal approach that allows community banks to thrive will do permanent damage to financial inclusivity and will further push people out of the financial system.

I have often said to my colleagues in Washington, DC, that economic development in many places in Kansas is whether or not there is a grocery store in town. It didn't take me too long to realize that that answer, of whether or not there is a grocery store in town, often revolves around whether or not there is a community bank—a relationship bank—in town, one that makes decisions, certainly, on the wellness and the ability of the loan to be paid, but what is in the best interest of the community? How can I make my community and my customers better off for the way this bank operates?

Another Kansas banker noted it appears that Dr. Omarova is comfortable with a banking model ''that lacks luster and the agility to serve the diverse nature of the American banking industry.''

With a banking model that would provide no incentive to create innovative new products, consumers would no longer benefit from the financial modernization that has brought so many people into the banking sector, so many customers to the banking sector. Consumers are best served by a financial system that offers competitively priced loans and lets lenders invest back in their local communities.

We must continuously work to improve our financial sector for everyone, but forcing consumers to bank with the government would do so much more harm than good. Kansans want less government in their lives, not more, as this would be.

Under Dr. Omarova's proposal, the government would have mandatory seats on bank boards and be able to control investments in ''socially suboptimal'' activities, a subjective definition that can be interpreted to stifle investment. She believes Federal bureaucrats should handpick who gains access to credit—all but ensuring leftist ideas would be funded.

Confirming her to this office would provide Dr. Omarova with ample opportunity to deny funding to industries she finds politically unfavorable, including bankrupting our domestic energy companies, something she spoke about.

While Dr. Omarova cheers on companies' bankruptcies, jobs disappear, families go without income, and that American dream that is so important to all of us is crushed.

Unfortunately, the doctor's confirmation hearing this morning only deepened my concerns. Her views have no place in the role of the Nation's top bank regulator.

She is entitled to her views. She is entitled to her radical views but not as the Nation's top bank regulator.

By nominating Dr. Omarova, President Biden looks to fundamentally reshape banking from a market-driven industry to a one-size-fits-all government entity. The thought of a centrally planned economy and a banking system like that is not only unworkable, but it is radical—radically wrong.

Even if these ideas are just for the sake of some academic thought, Dr. Omarova's suggestions have consequential impacts. This is a very powerful position, and we cannot—we would take her views lightly at our own risk.

I urge my colleagues to reject this nominee.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. CARDIN. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

REMEMBERING SERGEI MAGNITSKY

Mr. CARDIN. Madam President, 12 years ago this Tuesday, Russian tax lawyer Sergei Magnitsky died in Moscow at the hands of prison guards who, instead of treating him for the acute illness that his torturous, yearlong detention provoked, beat him for over an hour. He was found dead in his cell shortly thereafter. His ''crime'' was exposing the largest tax fraud in Russian history, perpetrated by government officials. He was 37 years old and left a loving family and many friends.

At the Helsinki Commission, which I chair, we had heard of Sergei's plight months earlier, and we were saddened and outraged that such a promising life had been cut short and that so few expected his murderers to be held to any account.

Impunity for the murder of journalists, activists, opposition politicians, and now simply an honest citizen was and remains a depressing cliché in Russia under Vladimir Putin's rule, while his regime often ruthlessly punishes people for minor infractions of the law. For those on the wrong side of the Kremlin, the message is clear and chilling. Even the most damning evidence will not suffice to convict the guilty, nor will the most exculpatory evidence spare the innocent.

The need for justice in Russia in this specific case has not diminished with the passage of time. Moreover, the doubling down on the coverup of Sergei's murder and the massive tax heist he exposed implicates a wider swath of Russian officials with the guilt of this heinous crime. It does not need to be this way, nor is it ever too late for a reckoning in this case in the very courtrooms that hosted the show trials that ultimately led to Sergei's death.

As sober as this occasion is, there is reason for hope. Vladimir Putin will not rule Russia forever, and every passing day brings us closer to that moment when someone new will occupy his post. Who that person will be and whether this transition will usher in a Government in Russia that respects the rights of its citizens and abides by its international commitments remain unclear. I hope it does. A Russian Government that returns to the fold of responsible, constructive European powers would increase global security, enhance the prosperity of its own citizens and trading partners, and bring new vigor to tackling complex international challenges such as climate change.

Sergei's work lives on in his many colleagues and friends who are gathering in London this week to celebrate his life and to recognize others like him who seek justice and peace in their countries, often facing and surmounting seemingly impossible obstacles. All too often, they pay a heavy price for their courageous integrity.

Sergei's heroic legacy is exemplified in the global movement for justice sparked by his death and in the raft of Magnitsky laws that began in this Chamber and have now spread to over a dozen countries, including allies like Canada, the United Kingdom, and the European Union. Even as these laws help protect our countries from the corrupting taint of blood money and deny abusers the privilege of traveling to our shores, they also remind those who suffer human rights abuses at the hands of their own governments that we have not forgotten them.

Sergei Magnitsky is a reminder to all of us that one person can make a difference. In choosing the truth over lies and sacrifice over comfort, Sergei made a difference that will never be forgotten.

Fifty-five years ago, Senator Robert F. Kennedy addressed the National Union of South African Students and spoke about human liberty. He spoke about freedom of speech and the right to ''affirm one's membership and allegiance to the body politic—to society.'' He also spoke about the commensurate

freedom to be heard, ''to share in the decisions of government which shape men's lives.'' He stated that government ''must be limited in its power to act against its people so there may be no . . . arbitrary imposition of pains or penalties on an ordinary citizen by officials high or low.''

Senator Kennedy went on to say:

> Each time a man stands up for an ideal, or acts to improve the lot of others, or strikes out against injustice, he sends forth a tiny ripple of hope, and crossing each other from a million different centers of energy and daring, those ripples build a current which can sweep down the mightiest walls of oppression and resistance.

Sergei Magnitsky stood up for an ideal. He acted to improve the lot of others. He struck at injustice. He was and remains a ripple of hope.

On this sad anniversary of Sergei Magnitsky's murder, let us all recommit ourselves to helping those in Russia and around the world who seek their rightful share in the governance of their own countries and who deserve the confidence of doing so without fear of harm. If we do this, Sergei will not have died in vain.

I am confident that one day there will be a monument in stone and bronze to Sergei in his native Russia. Until that day, the law that bears his name will serve as his memorial.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mrs. SHAHEEN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Mr. WARNOCK). Without objection, it is so ordered.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mrs. SHAHEEN. Mr. President, I ask unanimous consent that the Senate proceed to executive session to consider Executive Calendar No. 437, Julianne Smith, of Michigan, to be United States Permanent Representative on the Council of the North Atlantic Treaty Organization, and that the Senate vote on the nomination without intervening action or debate.

The PRESIDING OFFICER. Without objection, it is so ordered.

The clerk will report the nomination.

The bill clerk read the nomination of Julianne Smith, of Michigan, to be United States Permanent Representative on the Council of the North Atlantic Treaty Organization, with the rank and status of Ambassador Extraordinary and Plenipotentiary.

There being no objection, the Senate proceeded to consider the nomination.

The PRESIDING OFFICER. The question is, Will the Senate advise and consent to the Smith nomination?

The nomination was confirmed.

Mrs. SHAHEEN. Mr. President, I ask unanimous consent that the motion to reconsider be considered made and laid upon the table, all without intervening action or debate; that no further motions be in order to the nomination; that any statements related to the nomination be printed in the RECORD; that the President be immediately notified of the Senate's action; and that the Senate resume legislative session.

The PRESIDING OFFICER. Without objection, it is so ordered.

LEGISLATIVE SESSION

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022—MOTION TO PROCEED—Continued

The PRESIDING OFFICER. The Senate will now resume legislative session.

The Senator from New Hampshire.

CONFIRMATION OF JULIANNE SMITH

Mrs. SHAHEEN. Mr. President, I would also like to speak to Julie Smith and her qualifications to be Ambassador to NATO.

Julie is, really, very well qualified to represent the United States within our biggest and most significant security alliance. Her 25-year career has focused on transatlantic relations and security. She has served the country as Deputy National Security Advisor and Acting National Security Advisor to then-Vice President Biden.

In 2012, she was awarded the Office of the Secretary of Defense's Medal for Exceptional Public Service. She has worked at some of the country's most esteemed think tanks that address European issues.

As the U.S. confronts challenges around the world, we need to convey our firm commitment to our allies and our alliances. For this reason, it is absolutely critical that we put Julie Smith in place as Ambassador to NATO as soon as possible.

I am really very pleased that those who had a hold on her nomination have finally lifted those holds. It is unfortunate that it has taken so long because, as we look at what is happening in Eastern Europe in particular, and as we look at the migrants who are being used by Belarus—and I assume that Vladimir Putin is behind this, as well, to send those migrants to the Polish border as a way to distract from what is happening in Eastern Europe—clearly, the more equipped NATO is to help deal with those challenges, the better.

If we are going to participate with NATO, we need to have an Ambassador on the ground. It should have happened several months ago, when she was nominated. So I am very pleased that she is going to be able to assume her ambassadorship very soon. As co-chair of the Senate NATO Observer Group, I look forward to working with her in her new role.

But this should serve as a wake-up call to those people in this Chamber who continue to have holds on critical nominees who are important to this country's national security. As I talk to U.S. allies, it is clear that the delay in sending Ambassadors to posts around the world is having a real impact on our relations with our partners; and in the absence of U.S. representation, they are questioning our commitment to our bilateral relationships.

Now, I would like to think that my colleagues who have put these holds on our nominees aren't doing it in an effort to undermine America's security and to undermine this administration in protecting the United States, but, clearly, that is the impact of what they are doing.

I have heard from a lot of my colleagues over the last months about U.S. standing in the world after our withdrawal from Afghanistan. Yet, as they are blocking administration nominees who would work with our allies, who would engage in our shared priorities and values, who would listen to concerns, and who could work together, they are just exacerbating any issues that may exist.

I don't know why they are doing this, but, right now, there are 58 other State Department nominees who are awaiting confirmation on the floor. Every day that passes that we have no Ambassadors in place in countries around the world, our national security is compromised, and I have got a very close-to-home example.

Earlier today, I met with Diane Foley, the mother of James Foley, who was the first American killed by ISIS, and she has done yeoman's work with her foundation to try to help the families of hostages who are being held in countries around the world. She was talking about what we could do to help those families and to do everything to try and help them get their loved ones back—to free the hostages who are being wrongly held around the world.

Well, one of the things we talked about is the fact that, in many of those countries, we don't have Ambassadors because we have holds on those folks who are so important to help those families and to help address American interests in those countries. So what our colleagues are doing by holding up these nominees is undermining the national security of the United States. By grinding to a halt our State Department nominees, a small group of my Republican colleagues has allowed partisan brinkmanship to pervade a critical aspect of our national security.

You know, there was a very important principle established after World War II about partisan politics ending at the water's edge. It is unfortunate that my colleagues on the other side of the aisle are not continuing to support that principle.

We are stronger and safer when our diplomatic corps—those individuals who support Americans and U.S. foreign policy around the world—are supported by capable, Senate-vetted, and Senate-confirmed Ambassadors.

So I hope we will see in the coming weeks a willingness of those few people—it is only two or three people on the other side of the aisle who have held people up—to release those holds in the best interests of America and of our security.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Ms. WARREN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

NATIONAL DEFENSE AUTHORIZATION ACT

Ms. WARREN. Mr. President, I rise to speak in opposition to the National Defense Authorization Act.

As written, this legislation authorizes $778 billion in defense spending just for next year alone. That is more money than we spent on defense during the Korean or Vietnam wars. It is even more money than we spent at the height of the extraordinary Reagan defense buildup in the 1980s.

Now Congress is set to pass this bill with virtually no debate and with virtually no discussion about how much money we are spending. Congress keeps the spigot of cash wide open so long as it is for defense. And please note that not one single dollar of this huge defense budget will be offset either with new taxes or with new spending cuts someplace else.

Meanwhile, do you know how much money the President's Build Back Better plan will cost, on average, each year if Congress passes it? $175 billion. That is about one-fifth the size of this Defense bill. And unlike this Defense bill, every single dollar of the President's plan will be offset with new revenue or savings.

But here is the thing: When we want to invest $175 billion a year on childcare and paid family leave and expanding access to healthcare and fighting the climate crisis, and when we are going to offset every single dollar for those new expenses, everybody suddenly becomes so very concerned about spending. When we want to make investments that directly benefit people across this country, we are told ''that costs too much'' or ''that is socialism.'' But when we spend nearly five times that amount of money in the Defense bill, it is just a shrug of the shoulders. Look around this Chamber. It is empty.

And let's be clear where most of this defense money is going. It is largely going to the defense industry. The Pentagon will take this money and give approximately $400 billion to contractors. And nearly 40 percent of that will go to a handful of giant contractors.

This is a huge amount of money in an ordinary year, but 2 years into a global pandemic that has killed 765,000 Americans, it is irresponsible to spend this much money on stuff that isn't saving Americans from what is actually killing them. America's spending priorities are completely misaligned, and the threats Americans actually are facing, the things that are quite literally endangering their lives—like COVID–19 and the climate crisis—don't get this kind of attention.

Let me be clear. We can spend far less money on defense and still protect Americans and American interests. And you don't have to take my word for it. The Congressional Budget Office recently published a report outlining three different avenues for cutting $1 trillion in defense spending over the next decade. None of the three proposals were even close to radical. And, by the way, none of them achieved any savings from nuclear modernization, contract spending, and closing bases.

And before somebody cranks up the outrage machine, let me say I do not believe that we should spend nothing on defense. There are real threats to our Nation and real interests that we must defend. There are some situations that may require military solutions. But this Defense bill goes far beyond that threshold. This bill continues to feed into the wrongheaded idea that America's strength can only be measured by our military domination.

This bill is another example of Congress granting the Pentagon virtually unlimited resources while, at the exact same moment, pinching pennies on things that will make the American economy work for our children and for our seniors, for workers and students and retirees, for everyone who isn't part of a tiny little slice at the top.

These misplaced priorities chip away at the strength of our Nation, and, ironically, they undermine the foundation upon which our military is built. If we don't come to recognize this soon, then all this money will have been wasted, and the world's most powerful military will rest on a foundation of sand.

There are important and valuable provisions in this Defense bill. There are even places where we should spend more money, like on cyber defense, but it is long past time for us to rationalize the Pentagon's budget and align it with the threats we actually face. And this Defense bill, like so many before it, fails miserably to do that. For that reason, I will vote against it.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. GRASSLEY. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

DEPARTMENT OF DEFENSE AUDIT

Mr. GRASSLEY. Mr. President, on November 15, the Pentagon announced that it completed its fourth consecutive annual audit and received a fourth consecutive failing opinion.

This is what the Pentagon believes: If it somehow merely just conducts an audit, then somehow conducting that audit is a success despite the fact that it has been a requirement under the law for the last 30 years for Agencies—and that means all government Agencies—to conduct and pass an annual audit. The Department of Defense is about the only one that doesn't meet the requirements of the law.

The Department points to other signs of progress, such as that they were able to downgrade one material weakness from a previous audit and the closure of some 450 adverse findings. That, somehow, is progress. It is not progress—at least, it doesn't meet the demands of the law. However, the fact remains that the Department of Defense is unable to accurately account for billions of taxpayer dollars it spends each year.

Funding for the Department of Defense is crucial to our national security. Men and women who volunteer to wear the uniform and, hence, defend our country—these people deserve to be well paid and well equipped.

In light of the rising threats around the globe, it is more crucial than ever that not one dollar is lost to fraud, waste, and abuse. A clean audit, which the Defense Department has never had, is the key to whether Department of Defense money is spent responsibly.

A key underlying problem to the continued failed audits is the financial management systems used by the various military Departments. The Department of Defense uses hundreds of different financial systems that are outdated and are unable to communicate with each other. They cannot generate reliable transaction data and are not auditable.

There are inadequate internal controls in financial management systems, presenting an environment that is ripe for waste and fraud. Without internal controls at the transaction level, military leaders can never know how much things cost.

I have tried to work with leaders in the Department on this subject for years, but time and again, I have been disappointed.

The Defense Department's inability or its unwillingness to make necessary and overdue changes should be unacceptable to any Senator.

I filed an amendment to the bill before the Senate this year to address the root cause of the Pentagon's failed audits. The underlying bill provides for an independent Commission tasked with examining the budgeting and planning processes at the Pentagon. My amendment will require that very same Commission to also make recommendations on bringing financial management systems up to snuff.

The Department of Defense will never be able to get a clean audit opinion while these systems remain unfixed, and the Department of Defense has demonstrated an inability or unwillingness to deploy an accounting

system capable of capturing payment transactions and generating reliable data. If you can't follow the money, you will never be able to get a clean audit.

I am glad that my amendment has been included in the substitute amendment of the Defense bill before the U.S. Senate now, and I urge my colleagues to support this effort through to final passage to finally make real progress towards getting to a clean audit opinion. Fiscal accountability and military readiness are not mutually exclusive. It is not an either-or scenario. Earning a clean bill of fiscal health will strengthen military readiness and boost support for necessary increases to defense spending in Congress, and it would get the backing of the American people to a greater extent than it does today.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

(Whereupon, Mr. KAINE assumed the chair.)

(Whereupon, Mr. KELLY assumed the chair.)

Mr. REED. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER (Ms. BALDWIN). Without objection, it is so ordered.

UNANIMOUS CONSENT REQUESTS

Mr. REED. Madam President, I ask unanimous consent to yield back all remaining time on the motion to proceed to Calendar No. 144, H.R. 4350, the National Defense Authorization Act; that if the motion to proceed is agreed to, the Reed-Inhofe substitute amendment No. 3867, as modified with the changes at the desk, be called up and reported by number; further, that it be in order to call up the following amendments to the Reed-Inhofe substitute amendment No. 3867, as modified, in the order listed: 1, Reed No. 4775; 2, Hoeven No. 4482; 3, Sanders No. 4654; 4, Lee No. 4793; 5, Paul No. 4395; 6, Hawley No. 4140; 7, Peters-Portman No. 4799; 8, Scott of Florida, No. 4813 side-by-side to 4799; 9, Durbin-Lee No. 3939; 10, Cardin No. 3980; 11, Luján-Crapo No. 4260; 12, King-Sasse No. 4784; 13, Cruz No. 4656; 14, Kaine No. 4133; 15, Hassan No. 4255; 16, Menendez No. 4786; 17, Marshall No. 4093; 18, Kennedy No. 4660; 19, Sanders No. 4722; 20, Portman No. 4540; that with the exception of the Reed amendment No. 4775, the Senate vote at 9:30 p.m. today in relation to any first-degree amendment offered in the order listed above, with 60 affirmative votes required for adoption of amendments in this agreement, and 2 minutes of debate, equally divided in the usual form, prior to each vote.

The PRESIDING OFFICER. Is there objection?

Mr. RUBIO. Madam President.

The PRESIDING OFFICER. The senior Senator from Florida.

Mr. RUBIO. Reserving the right to object, I—what is missing from this list is the Uighur Forced Labor Prevention Act. In a moment, you are going to hear that it has this procedural problem—blue slips. For anyone who is not familiar with the lingo around here, that means that it is going to generate revenue, and therefore it has to originate in the House. That is what you are going to hear in a moment.

Here is what is so interesting about it. About, I don't know, 4, 5, 6 weeks ago, that very bill passed by unanimous consent in this very Senate.

This bill doesn't have a blue slip problem. It has a bunch of corporations who are making stuff in Xinjiang Province problem. That is what the problem is here. So everyone is aware—everyone here is aware, I hope. In the Xinjiang Province of China, Uighur Muslims are put into forced labor camps where they work as slaves—something that this administration and the previous one termed as ''genocide.''

They work as slaves making products, and there are American companies that are sourcing goods that end up on the shelves in this country. It is, in fact, almost certain that in this very Chamber there is some product that was manufactured by slave labor in China. We passed that bill in the Senate by unanimous consent. Not a single person objected to it. There was no blue slip problem then. Now all of a sudden there is.

This is because there is a bunch—that is why they are killing it in the House. A bunch of these corporations, lobbying against it, doing everything possible, and they know if it gets in this bill it is going to become law.

So I object, and I ask that the request be modified to include my amendment No. 4330.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. I object to the modification, Madam President.

The PRESIDING OFFICER. Objection is heard to the modification.

Is there objection to the original request?

Mr. RUBIO. I object.

Mr. REED. Madam President.

The PRESIDING OFFICER. The Senator from Rhode Island.

Mr. REED. I renew my request.

The PRESIDING OFFICER. Is there objection?

Mr. DAINES. Madam President.

The PRESIDING OFFICER. The junior Senator from Montana.

Mr. DAINES. Madam President, reserving the right to object, border security is national security. That is why I rise today to speak on my amendment No. 4236, to block President Biden's outrageous taxpayer-funded handouts to illegal immigrants who broke the law and entered our country illegally.

At a time when American families are struggling because of Bidenflation, when families are paying more for everything from gas to groceries, to heating their homes, the President wants to give up to hundreds of millions of your taxpayer dollars to illegal immigrants as a reward for breaking the law.

Don't forget, we still have a crisis on our southern border, and we should be doing all that we can to secure our southern border, not incentivize illegal immigration.

These taxpayer-funded handouts to illegal immigrants are outrageous, and I would urge my colleagues to allow a vote on my commonsense amendment.

Therefore, I ask unanimous consent to modify the request to include my amendment No. 4236.

Mr. REED. Madam President.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. I object to the modification.

The PRESIDING OFFICER. Objection is heard.

Is there objection to the original request?

Mr. DAINES. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I renew my request.

The PRESIDING OFFICER. Is there objection?

Mr. TOOMEY. Madam President.

The PRESIDING OFFICER. The junior Senator from Pennsylvania.

Mr. TOOMEY. Madam President, reserving the right to object, I would just like to bring to my colleagues' attention to the front page of the Wall Street Journal, the lead story, the headline above the fold today, ''Annual Drug Overdose Deaths Top 100,000, Setting Record.'' For the 12 months ending in April, alltime record number of fatalities—a big majority of them opioids, mostly synthetic opioids, driven primarily by fentanyl. Unbelievable. Think of 100,000 new families in the last 12 months that will have an empty seat at the Thanksgiving Day dinner next Thursday.

Pennsylvania has been hit as hard as any State, but every one of our States has been hit hard by this.

So why am I objecting to this?

Because I have an amendment that at least on the margins would help. It is simple, and it is common sense. It adds fentanyl to the majors list. The majors list is the list that includes the countries that the President has to identify as the largest producers of illicit fentanyl. That is China. Let's be clear. But once these countries—any country—is identified as a big producer of fentanyl, my bill would require those countries to prosecute drug traffickers and schedule fentanyl as a class, and if they do not, then they are not doing all they could and should be doing to keep fentanyl off our streets; in which case, under my amendment, the President would be authorized to withhold certain categories of foreign aid.

This bill is so noncontroversial and common sense, it has actually already passed this body just last year.

It is bipartisan. Senator MAGGIE HASSAN from New Hampshire, a Democrat, is my partner on the underlying bill.

And I would point out to my colleagues, I don't have any objection to anyone getting an amendment vote. I am not holding up anybody's votes, as long as we get this chance to reduce the flow of fentanyl coming into America.

So I ask to modify the request to include my amendment No. 3925.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. Madam President, I object to the modification.

The PRESIDING OFFICER. There is objection. Objection is heard.

Is there objection to the original request?

Mr. TOOMEY. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I renew my request.

The PRESIDING OFFICER. Is there objection?

Mr. RISCH. Madam President.

The PRESIDING OFFICER. The junior Senator from Idaho.

Mr. RISCH. Madam President, I am reserving the right to object.

I want to speak today on behalf of my amendment, Risch No. 4794, which is not included on that list, which I have introduced with cosponsors Senators PORTMAN, CRUZ, BARRASSO, JOHNSON, COTTON, DAINES, and WICKER.

This amendment is the Senate companion to bipartisan language that already is included in the House-passed NDAA which would sanction Nord Stream 2, Putin's premier energy weapon against Ukraine and Europe.

The timing could not be more important. Ukraine stands on the brink of an invasion, and Europe is in the throes of an energy crisis created by Russia.

There is a reason Ukraine's President Zelensky tweeted an urgent request last week regarding this amendment, which said:

> [A]ll friends of Ukraine and Europe in the US Senate [should] back this amendment.

We are now seeing the consequences of the administration's decision to waive mandatory PEESA sanctions and refusal to impose CAATSA sanctions.

Russia has deliberately cut gas transmission to Europe through Ukraine and is using high energy prices to pressure the EU into approving Nord Stream 2 as quickly as possible. Putin has publicly stated as such.

Meanwhile, Russian forces have built up along the border of Ukraine in preparation for what could be a full-scale invasion, just as they did to the Crimea.

Remember, Nord Stream 2 is designed to replace Ukraine's gas transit system, meaning Russia no longer has to worry about destroying its own infrastructure in the event of full-scale war.

We cannot allow Putin's blackmail to succeed. Nord Stream 2 has always been a bipartisan issue here in the Senate, and it should continue to be. Not a single Member of Congress supports the completion of this pipeline. I would like to think a similar number of us don't think we should ignore our friends in Europe, particularly Central and Eastern Europe, who stand to lose the most from Nord Stream 2.

Our amendment would impose mandatory sanctions against Nord Stream 2 AG, the company responsible for the project, as well as the companies involved in testing and certifying the pipeline before it can become operational.

We do provide the administration with a pathway to lifting these targeted sanctions, pending, of course, congressional review. This pathway is the exact same process for congressional input that 98 Senators voted for in CAATSA just a few years ago.

Nord Stream 2 is not set to become operational for months so there is still time to stop it, but we need to act quickly.

I urge my colleagues to join our distinguished colleagues in the House of Representatives on this important endeavor and to vote yes on this amendment.

Therefore, I ask unanimous consent to modify the request of the distinguished Senator REED and include my amendment No. 4794.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. Madam President, I object to the modification.

The PRESIDING OFFICER. Objection to the modification is heard.

Is there objection to the original request?

Mr. RISCH. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I renew my original request.

The PRESIDING OFFICER. Is there objection?

Mr. CRUZ. Madam President.

The PRESIDING OFFICER. The junior Senator from Texas.

Mr. CRUZ. Reserving the right to object, 2 years ago, I authored bipartisan legislation sanctioning any company that participated in building Nord Stream 2. That legislation passed Congress overwhelmingly, and Democrats and Republicans overwhelmingly supported it. That was passed on the NDAA, the National Defense Authorization Act.

A year ago, I authored a second set of bipartisan sanctions on Nord Stream 2. That second set of bipartisan sanctions again passed overwhelmingly with the support of Democrats and Republicans in this Chamber. That second set of bipartisan sanctions likewise passed on the National Defense Authorization Act.

Today, the Democrats are objecting to passing sanctions on Nord Stream 2.

What has changed?

Two things have changed. No. 1, today Joe Biden is President and not Donald Trump. And the Democrats were more than willing to stand up to Russia when Donald Trump was President, but when Joe Biden is President, suddenly it is untenable for Democrats to stand up to Russia.

But, secondly, it is even worse because what has also changed is that Joe Biden has utterly and completely capitulated to Vladimir Putin. He has waived the mandatory sanctions that this body passed. He has given a multi-billion-dollar generational gift to Putin. This strengthens Russia. Decades from now, successor dictators in Russia will reap billions of dollars that they will use for military aggression against Europe, against America, and it will be because Joe Biden utterly and completely capitulated.

So why are Senate Democrats objecting to a vote on Nord Stream 2?

Because they cannot defend Joe Biden's surrender to Putin on the merits. They don't want to vote on it because it would be politically inconvenient for this White House that has undermined the national security of the United States and has weakened our allies. Right now, energy prices are skyrocketing in Europe because Joe Biden surrendered to Vladimir Putin.

We have twice passed Nord Stream 2 sanctions on the NDAA. After Biden's surrender to Putin, we should do so again. My Democratic friends who have given speech after speech after speech against Nord Stream 2, against Russia, should demonstrate they mean what they say and that they are not simply interested in being political protectors for a Democratic President.

Accordingly—and I would note, by the way, in response to every amendment that has been called up, the Democrats have not seen fit to provide even a word of substantive argument in response. So I am going to predict you are not going to hear the President, Joe Biden, surrender to Russia. You are not going to hear any defense of Nord Stream 2. You haven't heard any substantive defense. You are going to hear two words—''I object''—because the Democrats are afraid of taking this vote.

I believe we are elected here to represent our constituents and the interests of the United States, and we should have the courage to do so. Therefore, I ask to modify the request to include amendment No. 4794.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. Madam President, I object.

The PRESIDING OFFICER. Objection to the modification is heard.

Is there objection to the original request?

Mr. CRUZ. My prediction was accurate, and I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I renew my original request.

The PRESIDING OFFICER. Is there objection?

The junior Senator from Alaska.

Mr. SULLIVAN. Madam President, in reserving the right to object, I am requesting a vote on my amendment No. 4329.

I am very disappointed that my Democratic colleagues will refuse to vote on this very simple, very important, very constitutionally correct amendment that also dramatically could impact military readiness, which is why it is so important to discuss it here as we are debating the NDAA.

My amendment is simple. It prohibits the Department of Defense from enforcing President Biden's vaccine mandate on contractors and subcontractors. That is it.

Why is this important?

Well, look, we all want to put the vaccine behind us. There is no doubt about that. We have all been vaccinated here. I think most of us have encouraged our constituents, in consultation with their physicians, to do the same.

First and foremost, as to this vaccine mandate, it is becoming increasingly clear it is not constitutionally based, and it is not based in statute, and I think the American people are seeing that on a daily basis. So it is an issue of not just the constitutional authority of the President, but it is an issue of the principle that got us all through the pandemic last year.

If you will remember, one of the most important principles that we had as we were working on COVID relief—whether in the CARES Act or other aspects of legislation that we had with regard to COVID relief for our citizens—was this: If you got relief, whether you were a small business, from the PPP, or were an airline or a defense contractor, the law said you had to keep your employees—that you had to keep them together—employers and employees together. That was the principle that all of us—Democrats and Republicans and the Trump administration—agreed on during the pandemic, and it worked. Many of these workers were on the front lines, helping us get through the pandemic.

This President, with his mandate, has taken a sledgehammer to that principle. Not only are we now saying employers and employees stick together; he is saying to employers: If you don't listen to the President, employers in America, you have to fire your employees.

Think about that. That is exactly the opposite of what we all agreed on last year as we were trying to get this Nation through the pandemic. So it is fairness. It is the principle that matters.

And here is the final thing—and I think we are going to see this. It is a readiness issue for our military.

I have been talking to the White House. I am trying to get them to rescind this mandate. They have consistently said: Well, it is only going to impact about 1 percent of the workforce. We can't afford anybody getting fired from their job, but they think it is about 1 percent.

I was home in Alaska last weekend. This could impact contractors, and 10, 15, 20 percent of their workforce might not be working—defense contractors—hurting readiness.

Again, during the pandemic, we were asking these Americans to show up at work and make sure our defense industries were strong, and now the President is telling these same contractors: Go fire your employees—oh, by the way, over the holidays.

So I think this is a very simple, reasonable amendment that will help readiness. Therefore, I ask to modify the request to include my amendment No. 4329.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. Madam President, I object to the modification.

The PRESIDING OFFICER. Objection to the modification is heard.

Is there objection to the original request?

Mr. SULLIVAN. Madam President, I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I renew my original request.

The PRESIDING OFFICER. Is there objection?

Mr. LANKFORD. Madam President, I object.

The PRESIDING OFFICER. The junior Senator from Oklahoma.

Mr. LANKFORD. Madam President, in reserving the right to object, this is an astounding thing. This is a conversation that has happened today about amendments to the National Defense Authorization Act.

Now, I haven't been here very long, but, typically, an NDAA takes about 2 weeks on the floor to be able to process, and there is a lot of conversation about different amendments. There are managers' packages; there are big groupings of packages that come together that are noncontroversial; and there will be a series of votes that are side by side with other votes. It has already been set up for 20 votes. That is terrific. That is a great start.

Then there is a request for some other things that are pretty typical, actually. There have been requests just in the last couple of minutes on military contractors and the vaccine mandate that will certainly affect our military readiness. That is certainly defense related.

There is human trafficking in China and whether products are coming through. That is pretty straightforward. In fact, that passed unanimously through this body. That doesn't seem that controversial to be able to be in here.

There are conversations about fentanyl and the origin of fentanyl, where that is coming from. That shouldn't be controversial to try to protect the country, but, suddenly, that amendment has been blocked.

Nord Stream 2—Ukraine and Russia—has not been a controversial issue for us. This body has laid down sanctions multiple times on the NDAA on this exact issue, and now it is being blocked. You can't even debate it.

Myself and Senator DAINES both brought up things tonight dealing with border security, which is certainly national security: 1.7 million people we know of have illegally crossed our southwest border this year. It is the highest number of illegal crossings in the history of our country—1.7 million. But, on January 20 of this year, President Biden stopped construction on the border wall—in many places, literally where they only had to hang the gates and install the electronic infrastructure there. That was all that was left, but it stopped.

Why is this connected to national security?

Well, certainly, border security is national security. Also, part of this funding did come out of defense funding. It is being done by the U.S. Army Corps of Engineers in many places.

On top of that, this year, so far—just so far this year—we have paid contractors $2 billion not to build the wall. These were contracts that had already been let out to do the construction. We are continuing to pay about $3 million a day to contractors not to complete the wall in sections, by the way, that career individuals had selected—that section and that design—and then had to prove that that was the right place and the right design to both Republican and Democrats in this body, which they did. Now we are wasting $2 billion to not do national security.

My amendment is very straightforward. We take the contracts that are already out there, and we complete those sections of the wall that have been approved by career individuals. Let's complete those sections and not just throw the money away and waste two billion of American taxpayer dollars, but actually use it for national security.

So, in saying that, I ask that the request be modified to include my amendment No. 4100.

The PRESIDING OFFICER. Is there objection to the modification?

Mr. REED. Madam President, I object to the modification.

The PRESIDING OFFICER. Objection to the modification is heard.

Is there objection to the original request?

Mr. LANKFORD. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I renew my original request.

The PRESIDING OFFICER. Is there objection?

Mr. RISCH. Madam President, I object.

The PRESIDING OFFICER. Objection is heard.

Mr. REED. Madam President, I believe I have the floor.

The PRESIDING OFFICER. The Senator has the floor.

Mr. REED. Madam President, we began this process for the National Defense Authorization Act months ago. In

July, in working closely with the ranking member and all of my colleagues on the committee, we passed a bipartisan National Defense Act which was focused on the fundamental rationale for our National Defense Act: the men and women of the Armed Forces; the equipment that they need; the new technology, which is absolutely necessary as we go forward; the family lives of these men and women and their development; along with the weapons that they will use.

This has been the focal point. As a result, we produced a committee report with a bipartisan majority of 23 to 3.

We continued this bipartisan approach as we came into the floor debate. We have already included in the substitute amendment, which will be offered, approximately 60 amendments, on a bipartisan basis, that cover a range of topics which have been agreed to by both sides. Again, everything we have done to this point has been on a bipartisan basis.

Indeed, this unanimous consent that I have proposed is bipartisan. It incorporates amendments from both my Republican colleagues and my Democrat colleagues. It does so, as we must, in a way that accommodates as many as we can, but we cannot and have never been able to guarantee that every amendment offered could be incorporated into the bill.

So what we have here is, in a way, a crossroads. We have tried since the very inception to produce a bipartisan bill and a bipartisan floor action and a bipartisan final vote on the National Defense Act in the U.S. Senate.

We have to get there because—again, I can hear my colleagues talk about Nord Stream, and that is very interesting and a very important issue; I can hear them talk about border security; I can hear them talk about forced labor in China; I can hear them talk about illegal immigrants.

Ultimately, this is about the men and women who wear the uniform of the United States, and we can't leave them behind. The proposals might be meritorious, but we have to move forward and give those men and women the tools they need to defend the Nation.

Again, I can't emphasize enough how, in working together with my colleagues and ranking member, we have tried at every juncture to be inclusive, to be bipartisan, to have recognized as many of the issues as we could. And we have to do that in the context, frankly, of the fact, in the Senate, as has been demonstrated tonight, one person can stand up and say: No, I didn't get what I want, and no one is going to get anything.

I think we have done a very good job, frankly—and I might not be objective—in producing a national defense act that, at this juncture and with these additional amendments, would be more than worthy for final consideration by the Senate.

But what is, again, somewhat disconcerting to me is that, by analogy, you can say everything is national defense. But the people who ultimately suffer, if we cannot get to passage and then deliberation with the House and then a final bill sent to the White House—it is not only that these problems that we have tried to address be unaddressed, but we will send a very powerful message to the men and women in the Armed Forces: We don't have your back. We are too busy squabbling amongst ourselves about issues of the border, Nord Stream, and other issues.

So I would hope that we could move forward. The regret is that at this juncture, we are abandoning approximately 20 amendments on a bipartisan basis that would have addressed many of the concerns of my colleagues in the Senate. Some are directly related to national defense and some are not, but they were agreed to by both sides, and they would be added to this legislation.

But at this juncture, our responsibility is—and it cannot be avoided—moving forward, of passing our defense bill, and then working with the House to send up to the President of the United States a bill worthy of the sacrifice and service of those who wear the uniform of the United States.

Mr. INHOFE. Would the Senator yield?

Mr. REED. With that, I would yield to the ranking member.

Mr. INHOFE. Let me thank my partner there for all the hard work that we have done together.

Not many people understand the process that we go through every year. It is an exhaustive process to get just to where we are today.

First of all, I would say that, out of all the amendments that were discussed, I support all of them. We didn't get a chance to really see who did and who didn't support them, but I support them all.

When we start one of these processes each year—we do this every year—the first thing we do is that we send a notice out. We send a notice out to each Member and ask each Member: What types of things are you interested in?

And we send this out to all—to each Member of the House and the Senate, and they send their notices in as to what they want, when they want it, and how they want it. Then we put them and marry them in with other Democrats and Republicans who want the same thing and try to get these lists shaved down a little bit. And we have been successful in doing it. Right now, there are 60 cleared amendments. That is 60. That is about the same number we had last year and the same number we had before.

I was disappointed that we had to waste a lot of time. My fellow Senator from Oklahoma, JAMES LANKFORD, made the comment that we should have been on this bill for 2 weeks or longer. I agree; we should have. We couldn't do it. We didn't have it.

I have to say that the leader—the Democratic leader—didn't allow this to come up so that we could do this. We didn't have a choice. As Republicans, we didn't have a choice, and we were united in wanting to get started earlier. As a result of that, a lot of Democrats and Republicans have lost their opportunity to get heard and to have amendments considered.

The system is good. It is one that has worked for a long time. This is going to work. When we stop to think about the number of hours that are spent wading through all of these amendments, this does take place.

I would compliment our chairman of the committee. We have worked very well together. We have gotten to this point. We will have to get this thing finished, and we will. But, nonetheless, we have an exhaustive policy that we have considered year after year after year. That is where we are today.

With that, I yield the floor.

Mr. REED. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. SCHUMER. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. SCHUMER. Madam President, Democrats have been working in good faith for several days—actually, for several months, really—to pass this defense legislation.

The bill before us was produced through a bipartisan committee process and included the input of at least three-fifths of Senators from both sides of the aisle. It is unfortunate that we cannot move forward tonight.

Yesterday, we agreed to delay the initial cloture vote after the Armed Services Committee's ranking member requested more time to work on a managers' package to include more input from Members. The managers' package now include 57—57—amendments; 27 from Republicans, 27 from Democrats, and 3 bipartisan amendments.

Further, we just proposed votes on 18 amendments, 3 of which are bipartisan and 8 of which are Republican-led amendments. We could start voting on them tonight, but unfortunately, the other side won't agree—or some on the other side won't agree.

Democrats have demonstrated all year that we are more than willing to work in good faith on amendments here on the floor. This year, more amendments have received rollcall votes than during any of the past 4 years. Members on both sides want to get this done. So these delays are unfortunate. There is no good reason to keep delaying. We should move the process forward.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. WYDEN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. WYDEN. Madam President, in a few moments, I will put forward a request to the Senate to take up and approve the nomination of an Oregonian, my friend Chuck Sams, President Biden's choice to lead the National Park Service.

I am just going to take a few minutes to talk about Chuck Sams and why he is the right person for this critical job.

Colleagues, we all know that the Park Service is often called America's best idea, and together those parks form a network of treasures that no other country can match.

The fact is, the National Park Service is not only about the views and the photo-ops. It is all about our country. It is what makes our country so special for so many.

The Director of the National Park Service is in charge of an organization of over 22,000 employees and almost a quarter million volunteers. The National Park System generates tens of millions of dollars of economic activity. The people of my State know particularly how important those critical outdoor treasures are for rural economies and rural jobs.

The fact also is that there are park units in every State in the country—urban parts, rural parts, historic American buildings, ancient archeological sites—and personnel at the Park Service do it all, from education to preservation, to maintenance, and even resilience against wildfire.

Chuck Sams has been a longtime Umatilla Tribal leader, and there he has served in a variety of roles. He is a member of the Northwest Power and Conservation Council, working with officials from across the Pacific Northwest. He is a veteran of the U.S. Navy. He is a role model—a role model—in so many respects, and particularly in the stewardship of America's lands, waters, wildlife, and history. And the Congress and the parkgoers are going to rely on him in the months and years ahead because we all know the Park Service faces big challenges.

I am going to wrap up and make my unanimous consent request, but, first, I want to commend my colleague from Alaska. My colleague and I have been working pretty much through the day.

I will be brief. I just want to thank the Senator from Alaska. We have been working throughout the day to resolve the whole issue of the Sams nomination.

This is a wonderful person who is going to give public service a really good name when he is confirmed.

My colleague from Alaska has raised a number of issues that he considers very important to his State. He and I have worked together on a variety of these issues, both from the standpoint of the Energy Committee and most recently as chairman of the Finance Committee, when we have worked on some tax issues. So I want to thank him for his cooperation that is going to make it possible for us to advance this nomination tonight.

Madam President, I ask unanimous consent that the Senate proceed to executive session to consider Executive Calendar No. 508, Charles F. Sams III, of Oregon, to be Director of the National Park Service, and that the Senate vote on the nomination without intervening action or debate.

The PRESIDING OFFICER. Is there objection?

Mr. SULLIVAN. Madam President.

The PRESIDING OFFICER. The Senator from Alaska.

Mr. SULLIVAN. Madam President, I just want to thank Senator WYDEN for his cooperation working on this nominee. Mr. Sams, I do agree, is qualified.

We had a long discussion this afternoon about some of the big issues that are impacting my State as it relates to the National Park Service.

You know, a lot of people love the National Park Service. Two-thirds of all National Park Service land in America is in Alaska—tens of millions of acres. It is bigger than almost every other State represented here on the Senate floor. That is just the National Park Service.

For decades, that Federal authority—the National Park Service authority in Alaska—has been abused. How do we know that it has been abused? Well, we recently had two—two—U.S. Supreme Court decisions that were 9-to-0 decisions, by the way, that essentially said the Park Service was not following the law in Alaska—two.

So my discussions with Mr. Sams and the commitments he made to me, I think, are going to help Alaska. I think they are going to help the National Park Service, and it is related to the National Park Service authorities.

After these two decisions—they were called the Sturgeon decisions—two in a row, at the U.S. Supreme Court, 9 to 0, by the way, and the U.S. Supreme Court telling the National Park Service: You are not following the Alaska National Interest Lands Conservation Act. We call it ANILCA in Alaska. You are not following the Federal Government. You need to follow it.

So the commitment I got from Mr. Sams was there was a recent regulation from the Federal Government in November of 2020 providing specifics of how the National Park Service was going to implement these two U.S. Supreme Court cases—the Sturgeon case. And he committed to me to be true to these regulations and to faithfully execute these regulations in the National Park Service on implementing Sturgeon. That is a very big deal in Alaska.

He also committed to have all of his senior Alaska staff and senior staff here in Washington, DC, take ANILCA training. This is a giant statute. The Federal Government often screws it up, and it has a negative impact on my State. So he committed to me that he will have his top leadership at the National Park Service take training to understand this complicated law. That will also help my constituents and the country very much.

So I want to, again, thank Senator WYDEN for working with me on these issues. These are important commitments that Mr. Sams has made, and I have no further objection to this nominee's confirmation.

The PRESIDING OFFICER. If there is no objection, the clerk will report the nomination.

The senior assistant legislative clerk read the nomination of Charles F. Sams III, of Oregon, to be Director of the National Park Service.

There being no objection, the Senate proceeded to consider the nomination.

The PRESIDING OFFICER. The question is, Will the Senate advise and consent to the Sams nomination?

The nomination was confirmed.

The PRESIDING OFFICER. The senior Senator from Oregon.

Mr. WYDEN. Madam President, I ask unanimous consent that the motion to reconsider be considered made and laid upon the table, all without intervening action or debate; that no further motions be made in order to the nomination; that any statements related to the nomination be printed in the Record; that the President be immediately notified of the Senate's action, and the Senate resume legislative session.

The PRESIDING OFFICER. Without objection, it is so ordered.

LEGISLATIVE SESSION

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2022—MOTION TO PROCEED—Continued

The PRESIDING OFFICER. The Senate will now resume legislative session.

MORNING BUSINESS

NOTICE OF A TIE VOTE UNDER S. RES. 27

Mr. MANCHIN. Madam President, I ask unanimous consent to print the follwing letter in the CONGRESSIONAL RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

UNITED STATES SENATE, COMMITTEE ON ENERGY AND NATURAL RESOURCES,

November 18, 2021.

TO THE SECRETARY OF THE SENATE: The nomination of Laura Daniel-Davis, of Virginia, to be an Assistant Secretary of the Interior, vice Joseph Balash, resigned, PN 761,

having been referred to the Committee on Energy and Natural Resources, the Committee, with a quorum present, has voted on the nomination as follows—

On the question of reporting the nomination favorably with the recommendation that the nomination be confirmed, 10 ayes to 10 nays.

In accordance with section 3, paragraph (l)(A) of S. Res. 27 of the 117th Congress, I hereby give notice that the Committee has not reported the nomination because of a tie vote and ask that this notice be printed in the RECORD pursuant to the resolution.

JOE MANCHIN III,
Chairman.

VOTE EXPLANATION

Ms. CANTWELL. Madam President, on November 15, 2021, I was unable to be present for the rollcall vote No. 466 on the Motion to invoke cloture on Executive Calendar No. 401, the nomination of Graham Steele to be an Assistant Secretary of the Treasury.

However, had I been present, I would have voted in favor of the motion to invoke cloture. I supported Mr. Steele's nomination based on his strong track record as a respected expert on financial policy and consumer protection and his years of service in senior level positions here in the Senate.

WORLD DAY OF REMEMBRANCE FOR ROAD TRAFFIC VICTIMS

Mr. VAN HOLLEN. Madam President, November 21, 2021, will mark the 26th World Day of Remembrance—WDoR—for Road Traffic Victims, commemorating the millions of people killed and injured on the world's road. It is also a day to thank emergency responders for their role in saving lives, to reflect on the impact of road traffic deaths and injuries on families and communities, and to draw attention to the need for improved legislation, awareness, infrastructure, and technology to save more families from the tragedy of losing a loved one.

More than I million people die from road crashes every year, and tens of millions are seriously injured. Road traffic crashes are the No. 1 killer of young people aged 15–29 and the eighth leading cause of death among all people worldwide. Rochelle Sobel, president of the Association for Safe International Road Travel, highlighted the gravity of this issue and the imperative to fix it: ''Every 27 seconds, somewhere in the world, a person dies in a road crash.''

On this 26th anniversary of World Day of Remembrance for Road Traffic Victims, it is important to remember the history and recommit to the goals of this day. It was initiated in 1995 as the European Day of Remembrance and quickly spread around the globe to countries in Africa, South America, and Asia. In 2005, the United Nations General Assembly adopted resolution 60/2, recognizing November 15 as the World Day of Remembrance for Road Traffic Victims. Since that time, the observance of this day has continued to spread to a growing number of countries on every continent.

This year marks the start of the new Decade of Action for Road Safety 2021–2030, during which the WDoR will highlight the reasons for all of the necessary actions to be taken during this coming decade. Indeed, the day has become an important moment to focus international attention on this preventable epidemic and as an advocacy tool in global efforts to reduce road casualties. As a result of the growing awareness and global call to action that World Day of Remembrance for Road Traffic Victims has generated, in September 2020, the United Nations passed a resolution declaring the years 2021 to 2030 a new Decade of Action for Road Safety. The declaration affirms the UN's commitment to work vigorously to implement a new, ambitious agenda to halve road crash deaths by 2030.

Additionally, the United Nations Sustainable Development Goal 3.6 calls on governments and their stakeholders, including NGOs and private citizens, to address the personal, medical, and financial burdens associated with road traffic deaths and injuries.

The devastation of losing a child, parent, sibling, partner, friend, caregiver, or caretaker is immeasurable, as are the challenges of caring for a permanently disabled loved. Road traffic crashes are preventable, and so we owe it to our communities to work together so that the hopes and dreams of our loved ones are not shattered on the roads of the United States and the world. We must all take action to prevent these avoidable tragedies and save lives.

TRIBUTE TO JANET COIT

Mr. WHITEHOUSE. Madam President, I rise today to honor Janet Coit, one of Rhode Island's most respected environmental advocates. Ms. Coit is the newly appointed Assistant Administrator for the National Oceanic and Atmospheric Administration's National Marine Fisheries Service. She joined NOAA after a decade of committed service leading the Rhode Island Department of Environmental Management under three Governors.

After graduating from Dartmouth College and Stanford Law School, where Ms. Coit was a member of the Environmental Law Journal, she served as counsel to the U.S. Senate Committee on the Environment and Public Works. She went on to serve as counsel and environmental coordinator for the late Senator John Chafee and, subsequently, his son Senator Lincoln Chafee.

Ms. Coit then returned to Rhode Island and began a decade of work as the State director for the Nature Conservancy, where she oversaw some of the State's largest land conservation projects.

Ms. Coit went on to be appointed by Governor Lincoln Chafee to serve as director of the Rhode Island Department of Environmental Management. Governors Raimondo and McKee wisely kept her in that position. Her legacy at DEM includes streamlined permitting processes, new opportunities for families to connect with nature, and improved customer service. As the longest serving chief executive in DEM's history, she focused on public parks, promoting local food systems, Rhode Island's fishing and shellfish industries, and climate solutions. She seized opportunities to coordinate regional efforts, including addressing equity and justice issues, improving water quality, managing PFAS contamination, and fighting the climate crisis. In this capacity, she also served as chair of the Rhode Island Executive Climate Change Coordinating Council and on the board of directors for the Regional Greenhouse Gas Initiative. She has received numerous awards for her outstanding contributions at DEM.

In June, the Biden-Harris administration appointed Ms. Coit to lead NOAA Fisheries, where she oversees fisheries management, protected species, and fisheries habitat conservation. She also serves as the Acting Assistant Secretary of Commerce for Oceans and Atmosphere and Deputy Administrator, supporting and managing NOAA's coastal and marine programs.

We are fortunate that exceptional people like Ms. Coit choose to dedicate their careers to public service. I am proud to recognize her today and thank her for her many contributions to the State of Rhode Island and the Nation.

TRIBUTE TO DEBORAH SUE MAYER

Mr. COONS. Madam President, I rise as chairman of the Select Committee on Ethics, and on behalf of the vice chairman, members of the committee, and its staff, to pay tribute to Deborah Sue Mayer as she retires after 23 years of Federal service including the last 6 as chief counsel and staff director of the Select Committee on Ethics. As a paramedic, a naval officer, and attorney, Deb's career tells the story of a life dedicated to public service. She joined the Senate in January 2015 after 4 years as director of investigations for the House Committee on Ethics. From 2002 to 2011, Deb was a prosecutor with the U.S. Department of Justice; beginning as an Assistant U.S. Attorney in the Eastern District of New York's Organized Crime and Racketeering Section. Deb went on to serve in the Department of Justice Public Integrity Section of the Criminal Division, where she investigated and prosecuted corruption at all levels of government throughout the United States. Since 1998, Deb has served as a Judge Advocate in the U.S. Navy, first on Active Duty and continuing her career in the Reserve Force.

In her time as chief counsel and staff director, Deb personally advised members of the Committee and Senate,

oversaw the nonpartisan staff in providing ethics advice and education, administered the Senate's financial disclosure program, modernized and redesigned the committee's website, and conducted investigations and enforcement of ethics rules, laws and standards of conduct. Beyond the Senate, Deb represented the committee at conferences and on councils around the country and abroad. In all these efforts, Deb brought her trademark dedication to rigorous accuracy and precision. On behalf of the members and staff of the Select Committee on Ethics, I thank Deb for her decades of service to our country and commitment to the U.S. Senate. I offer my sincere best wishes and gratitude to Deb and her family as she begins her retirement.

Thank you, Deb.

TRIBUTE TO GENERAL JOHN E. HYTEN

Mrs. FISCHER. Madam President, I rise today to congratulate Gen. John E. Hyten on his retirement from the U.S. Air Force. I also want to extend my congratulations to his wife, Laura, and note the remarkable bond they share. Their partnership in life has enabled his success in uniform, and his achievements are truly theirs.

Across four decades of service, General Hyten has risen through the ranks to become one of the most respected voices in our military, and many in this Chamber rely on his deep knowledge and expertise. This is especially true on matters relating to space and nuclear deterrence.

I got to know General Hyten when he became a Nebraska constituent following his appointment to be the commander of U.S. Strategic Command in 2016. This was actually General Hyten's second tour of duty at Offutt Air Force Base, having previously commanded the 6th Space Operations Squadron there in the late nineties.

During his 3 years as the commander of STRATCOM, I was privileged to work closely with him, not just as the senior Senator from Nebraska, but also the chair of the Senate Armed Services Committee's Strategic Forces subcommittee, which directly oversees STRATCOM's mission areas.

During this span, we witnessed a marked shift in the strategic landscape, with worrying trends with respect to adversary behavior in space and investment in nuclear arms greatly accelerating. This elevated the importance of STRATCOM's mission and meant that, as its commander, General Hyten was on the front line of some of the most daunting security challenges facing our Nation.

During his tenure, he played a key role in the Department of Defense's response to these evolving threats. As space transformed into a warfighting domain, his candid advice was invaluable in Congress reorganization of the Department of Defense's space enterprise, including the creation of the Space Force and elevation of Space Command to a full-fledged unified combatant command.

He was also an extremely effective advocate for our Nation's nuclear forces, which continue to be the bedrock of our national security. As a vocal champion of nuclear modernization, he helped make the case for renewing the triad and broadening the modernization conversation to increase focus on nuclear command, control and communications—or NC3—systems, as well as National Nuclear Security Administration's nuclear complex.

He played an important part in drafting the 2018 Nuclear Posture Review, which marked the first time since the end of the Cold War that an NPR occurred against a backdrop of growing nuclear threats and therefore had to confront the uncomfortable reality that Russia and China had not followed our lead in reducing nuclear stockpiles.

He explained the problem with his customary candor: ''When we started de-emphasizing nuclear weapons, what did the rest of the world do? The rest of the world did exactly the opposite. So if we de-emphasize nuclear weapons, we're putting the country at jeopardy and we can never allow that to happen.''

Those sage words are still true today and should continue to guide U.S. nuclear policy. They also reflect another of General Hyten's characteristics that I value greatly: his unwavering focus on the threats facing our Nation. A tireless advocate for a return of threat-based planning, he always endeavored to base his approach on the changing threat picture and to educate those around him about the activities of our adversaries.

When he was nominated to be the next Vice Chairman of the Joint Chiefs of Staff, I felt very strongly that he was the right leader, with the right expertise, at the right time. I knew he would bring all of the qualities that distinguished him as a STRATCOM commander to bear in his new role, and he did not disappoint.

As Vice Chairman, he continued to discharge his responsibilities with great professionalism and dedication, and his confirmation to the position also meant that the Nation could benefit from his leadership for 2 more years.

Sadly, that time is at an end. And while the 40 years of exemplary service Gen. John Hyten has rendered make this retirement well-earned, I hope he will continue to share his wisdom and counsel. I wish General Hyten and his wife, Laura, a wonderful retirement together and all the best in their future.

AFGHANISTAN

Mrs. BLACKBURN. Madam President, the Biden administration's disastrous withdrawal from Afghanistan jeopardized our national security, empowered our enemies, and put thousands of innocent lives in jeopardy. But as the situation devolved, stories emerged of heroic efforts to push back the Taliban's advance and save stranded Americans, allies, and Afghan partners from the clutches of one of the world's most dangerous terror organizations.

Today, I want to honor a group of unsung heroes who joined this effort from the home front. Team Blackburn is blessed to include a dedicated and tenacious group of caseworkers and personal staff who treat the needs of Tennesseans like those of their own families. During those chaotic weeks, these people fielded hundreds of panicked calls for help from and on behalf of Tennesseans who were trapped behind enemy lines. They used every resource at their disposal, leveraged every connection they could think of and worked more than a few miracles to bring those Tennesseans closer to home.

On behalf of the Volunteer State, I thank the following members of my staff who went above and beyond on behalf of the common cause of freedom: Elizabeth Kelly, Payton Scott, Kayley Russell, Heather Hatcher, Josh Knell, Jeri Wheeler, Dana Magneson, Caroline Diaz-Barriga, Kim Cordell, Mac McCullough, Alexander Gonzalez, Grace Burch, Jay Strobino, John Clement, Edward Pritchard, and Emily Manning.

TRUMP ADMINISTRATION

Mrs. HYDE-SMITH. Madam President, the U.S. Supreme Court is set to hear the most anticipated abortion case in nearly 30 years when it considers Dobbs v. Jackson Women's Health Organization in oral argument on December 1, 2021. This development allows us to consider the many people whose dedication to the pro-life cause has led us to this point. One of those people is former President Donald J. Trump. The pro-life movement would not be where it is today absent his advocacy for pro-life policies and for conservative judges.

In January 2016, Presidential candidate Trump said, ''America, when it is at its best, follows a set of rules that have worked since our Founding. One of those rules is that we, as Americans, revere life and have done so since our Founders made it the first, and most important, of our 'unalienable' rights.''

He continued, ''Over time, our culture of life in this country has started sliding toward a culture of death. Perhaps the most significant piece of evidence to support this assertion is that since Roe v. Wade was decided by the Supreme Count 43 years ago, over 50 million Americans never had the chance to enjoy the opportunities offered by this country. They never had the chance to become doctors, musicians, farmers, teachers, husbands, fathers, sons or daughters. They never had the chance to enrich the culture of this nation or to bring their skills, lives, loves or passions into the fabric of this country. They are missing, and they are missed.''

These words helped guide President Trump's actions in office as he advocated for pro-life policies both domestically and abroad. Domestically, President Trump fought to defund Planned Parenthood and other abortion providers from receiving Federal funding. He prohibited such entities from receiving title X funding and permitted States to prohibit them from participating in Medicaid as well. In 2018, President Trump issued a rule requiring health insurers to specify whether plans cover abortion. He also issued rules to protect religious objectors and moral objectors from the Department of Health and Human Services contraceptive mandate. In addition, the President established a new Conscience and Religious Freedom division of the Office for Civil Rights to protect healthcare providers who object to participating in abortions.

President Trump's commitment to the unborn was just as strong abroad. Just days after his inauguration, President Trump ended Federal funding of abortion overseas by reinstating the Mexico City Policy, which prohibits nongovernment organizations receiving U.S. aid grants from performing and promoting abortions overseas. He directed the Secretary of State to implement the ban on taxpayer funds for overseas abortions across most U.S. global health programs through his Protecting Life in Global Health Assistance policy.

In addition, President Trump also defunded the United Nations Population Fund, a program long tied to China's forced abortion one-child policy. To further underline this, the Trump administration in 2020 declared to the United Nations that abortion is not a human right and signed the Geneva Consensus Declaration, where 33 nations joined together to reaffirm the value of unborn life. Finally, in January 2021, the Trump administration and called for the Chinese Communist Party to immediately end its system of forced abortions.

In addition to his work within the executive branch, President Trump also showed his commitment to the pro-life cause by nominating constitutional conservative and originalist judges to the Federal judiciary. He nominated three originalist Justices to the U.S. Supreme Court: Justice Neil Gorsuch in 2017, Justice Brett Kavanaugh in 2018, and Justice Amy Coney Barrett in 2020. More broadly, President Trump nominated 234 new article III judges who share this commitment to upholding our Constitution as written.

As the pro-life movement advances, it is important for us to recognize how we got here. Former President Trump deserves praise for all his administration did over the past 4 years to advance the cause of the unborn. I am gratitude for that work and recognize the tireless advocacy of the Trump administration to protect both women and their babies.

RECOGNIZING THE INTERCESSORS FOR AMERICA

Mrs. HYDE-SMITH. Madam President, for many years, thousands of members of the Intercessors for America—IFA—have been devoted to prayer and fasting in the name of protecting the unborn and of ending abortion. The IFA was founded in 1973 in an era when our Nation experienced turmoil within the political, moral, and traditional values that are the cornerstone of our Nation.

In 1973, the U.S. Supreme Court issued its divisive landmark decision in Roe v. Wade, legalizing abortion and shocking the majority of Americans. IFA has worked since then to mobilize our Nation to pray for the protection of innocent life and to find unity among the cultural conflicts in our country. Today, IFA is a national organization of millions of like-minded people who are steadfast in praying for God's support and guidance for our Nation's executive, legislative, and judicial branches of government.

I thank the members of IFA for their dedication, prayers, and fasting in support of the sanctity of life. Their work has helped increase awareness for the pro-life movement and its overarching goal to defend the unborn. It is the decades of prayer and hard work of so many pro-life advocates that has led us to this moment in history in which the Supreme Court will be hearing oral arguments in Dobbs v. Jackson Women's Health Organization. This case, which focuses on the constitutionality of a Mississippi law that bars abortion after 15 weeks, could reset the abortion issue and return it to elected leaders, who are more directly accountable to the people than Federal judges.

Today, I recognize and pay tribute to the role of the IFA in the nearly 50-year fight to protect innocent life in the womb. I also join with the IFA in praying for the members of our Supreme Court, who are now preparing to hear the Dobbs case. May God grant each Justice wisdom for the task and mercy for the unborn.

TRIBUTE TO SAM BROWNBACK

Mrs. HYDE-SMITH. Madam President, it is an honor to pay tribute to my fellow public servant Sam Brownback of Kansas. During his service both as Governor of Kansas and as a U.S. Senator, he advocated tirelessly for the right to life. More recently, during the last administration, he served as the U.S. Ambassador at Large for International Religious Freedom, fighting for the free exercise of religion abroad.

After a couple years in the House of Representatives, Ambassador Brownback represented Kansas in the Senate from 1996 to 2011. He came to the Capitol with a background similar to mine. I served as the Mississippi Commissioner of Agriculture and Commerce prior to coming to the Senate, and Ambassador Brownback served as Kansas's Secretary of Agriculture before coming to DC.

Upon joining the Senate, Ambassador Brownback consistently supported pro-life legislation and voted in defense of the sanctity of life. Through his 15 years in the Senate, he supported pro-life legislation including the Unborn Child Pain Awareness Act, the Born Alive Infants Protection Act, the Unborn Victims of Violence Act, the Partial Birth Abortion Ban Act, and the Hyde amendment.

This support for unborn life continued when the people of Kansas elected Sam Brownback to be their Governor, a position in which he served from 2011 to 2018. As Governor, he signed numerous laws protecting unborn human life, including a measure that made Kansas the first State to ban dismemberment abortions. Furthermore, during his tenure, Kansas passed laws restricting funding to abortion providers and banning sex-selective abortions, among many others.

Sam Brownback's steadfast efforts paid off. By the time he became an Ambassador in 2018, Kansas had become the second most pro-life State in the Nation, as ranked by the Americans United for Life. In fact, the number of abortions in Kansas dropped by nearly 30 percent, a testimony to the success of his policies promoting a culture of life.

But his efforts did not stop there. Upon his confirmation in 2018 as the U.S. Ambassador at Large for International Religious Freedom, he continued the fight to protect life and stand up against injustice abroad. He worked hand-in-hand with Secretary of State Mike Pompeo in condemning the Chinese Communist Party for its regime of forced abortions and sterilizations.

Throughout his long and commendable career in public service, Ambassador Brownback has shown a remarkable commitment to the sanctity of life. As the Supreme Court prepares to hear the Dobbs v. Jackson Women's Health Organization case, I am pleased to rise to recognize leaders in the pro-life movement who have advanced the cause to this point. Ambassador Brownback is definitely among those leaders for his many years as a champion for life.

TRIBUTE TO SEAN DUFFY

Mrs. HYDE-SMITH. Madam President, as the U.S. Supreme Court prepares to hear oral arguments in Dobbs v. Jackson Women's Health Organization case, I am taking time to recognize leaders in the pro-life movement who have helped bring us to this point. Today, I pay tribute to former Congressman Sean Duffy, who represented the pro-life values of the Seventh District of Wisconsin for five terms from 2011–2019.

Throughout his time in the House, Representative Duffy remained unwavering in his commitment to the sanctity of life. Whatever pro-life issue

arose, Representative Duffy was there to defend the unborn and the value of all life.

As religious liberty issues entered in the debate over the Affordable Care Act—ACA—Representative Duffy fought to keep taxpayer funding from covering abortions in ACA health plans. His opposition was part of his larger effort to oppose taxpayer funding for abortion in any arena, a fight embodied in his support of the No Taxpayer Funding for Abortion Act.

As our Nation a few years later learned of the horrors perpetrated by notorious abortionist Kermit Gosnell, Representative Duffy took to the House floor to highlight the evil of abortion as shown in Gosnell's case.

When videos revealed that Planned Parenthood was illegally selling fetal tissue from aborted babies, Representative Duffy joined his colleagues in calling for an investigation into this travesty. His pro-life leadership role led to an appointment to the House Energy and Commerce Committee's Select Investigative Panel on Planned Parenthood that investigated that organization's illegal fetal tissue sales.

A true pro-life hero, Representative Duffy leads by example in living out his pro-life values. On August 2019, Representative Duffy announced his resignation to focus on his ninth child who was born with heart defects and Down's syndrome.

Representative Duffy, along with his wife Rachel Campos-Duffy, stands as an inspirational example of how to champion pro-life and pro-family values in both public roles and in private lives.

TRIBUTE TO BETHANY KOZMA

Mrs. HYDE-SMITH. Madam President, I rise to recognize Bethany Kozma, former Deputy Chief of Staff at the United States Agency for International Development—USAID. She deserves to be honored for her tireless work during the last administration to execute pro-life, pro-family, and pro-religious freedom policies across USAID.

While her efforts in this regard garnered criticism, Mrs. Kozma remained resolute in advancing the Agency's firm pro-life positions. Her courage is an example to us all to cling tightly to our strongly held values, even in face of criticism.

Standing strong, Mrs. Kozma played an integral role in helping the U.S. Department of State, USAID, and the U.S. Department of Health and Human Services better synchronize their efforts in countless multilateral negotiations. This synergy helped ensure that the agreements formed by those negotiations did not promote or permit abortion.

In my own work here in the Senate, I know staff members toiling behind the scenes do important work that allows me to do my job successfully. No doubt, that is also true in the executive branch.

The work of dedicated agency staff like Mrs. Kozma was integral to the many pro-life successes of the past administration. Her tireless work helped ensure the United States could lead in pro-life policies abroad. Mrs. Kozma and others like her deserve recognition and our gratitude.

TRIBUTE TO MIKE POMPEO

Mrs. HYDE-SMITH. Madam President, I rise to pay tribute to former Secretary of State Mike Pompeo. During Mr. Pompeo's time at the State Department, he worked tirelessly to defend unborn children around the world. Under then-Secretary Pompeo's leadership, the United States stood as a nation that values all human rights, including the right to life. His bold leadership encouraged other world leaders to join the United States in standing against efforts by some within the United Nations to make abortion on demand an international right.

Mr. Pompeo established his pro-life bona fides during his four terms in the U.S. House of Representatives. During that time, he supported numerous pieces of pro-life legislation, such as the No Taxpayer Funding for Abortion Act and the Pain Capable Unborn Child Protection Act.

His commitment to the pro-life cause continued in his role as our Nation's top diplomat. A few particular successes stand out.

First, Secretary Pompeo initiated a new compliance mechanism to ensure enforcement of the Mexico City Policy, which prohibits taxpayer dollars from being used for abortion overseas. Under the Protecting Life in Global Health Assistance policy, the State Department would refuse to partner with any foreign organizations involved in supporting abortions. Additionally, these nongovernment organizations will also have to provide certification to the State Department that they are not involved with abortions. This highly successful policy closed an overwhelming proportion of the loopholes that had previously allowed organizations to skirt compliance with the Mexico City Policy.

Second, Secretary Pompeo ensured full enforcement of the Siljander amendment, an annual rider in the State and foreign operations appropriations bill to prohibit the use of U.S. funds, including foreign assistance, to lobby for or against abortion abroad.

Third, the Department of State led the United States to sign the Geneva Consensus Declaration in 2020, which reaffirmed ''that there is no international right to abortion.'' Thirty-three other nations, representing more than 1.6 billion people, also signed the declaration, an achievement that would not have been possible without American leadership on the issue.

Finally, Pompeo's Department of State in 2020 also sanctioned China for its many human rights abuses, including forced abortions and forced sterilizations.

These accomplishments make clear that former Secretary of State Mike Pompeo made true strides in vigorously defending the right to life of the unborn babies around the globe. His endeavors deserve our applause and gratitude.

TRIBUTE TO MORSE TAN

Mrs. HYDE-SMITH. Madam President, I rise to pay tribute to Morse Tan, former Ambassador at Large for Global Criminal Justice, whose dedication to the legal defense of human rights and the rights of the unborn is commendable.

Morse Tan's work to promote these values has spanned the globe. As an expert on North Korea, he has written extensively about the human rights abuses occurring in that country and how those responsible can be held accountable. In his book, ''North Korea, International Law and the Dual Crises: Narrative and Constructive Engagement,'' Tan sheds light on the genocide of Christians in North Korea, focusing specifically on the forced abortions imposed on many North Korean women.

As Ambassador at Large for Global Criminal Justice during the last administration, Ambassador Tan worked to gather evidence of China's repressive treatment of the Uyghurs and other ethnic minorities, including forced abortions and forced sterilizations. Based in part on the Ambassador's work, Secretary of State Mike Pompeo in July 2020 imposed sanctions on Chinese officials because of human rights abuses. Furthermore, Secretary Pompeo determined that China had committed crimes against humanity and genocide against the Uyghurs and other ethnic minority groups, based on the findings of an internal review led by Ambassador Tan.

Ambassador Tan has also undertaken significant work on behalf of the sanctity of life in the United States as well. He has filed amicus briefs in two Supreme Court cases regarding pro-life issues. In McCorvey v. Hill, Ambassador Tan coordinated, researched, and edited some 24 amicus briefs on behalf of Norma McCorvey, who was the plaintiff ''Jane Roe'' in Roe v. Wade. In Cano v. Baker, he coordinated, researched, and edited 22 amicus briefs on behalf of Sandra Cano, who was the plaintiff ''Mary Doe'' in Doe v. Bolton.

Finally, I hope that Ambassador Tan's work as a law professor in courses such as bioethics, international human rights, and constitutional law will inspire a new generation to take up the legal fight to protect the sanctity of life.

It is an honor to recognize Ambassador Morse Tan for his uncompromising work to defend the right of the unborn babies in courts and to bring justice and accountability for perpetrators of forced abortions around the world.

TRIBUTE TO ANN WAGNER

Mrs. HYDE-SMITH. Madam President, I rise to recognize Congresswoman ANN WAGNER, who represents the Second Congressional District of Missouri in the U.S. House of Representatives. Throughout her tenure in the House; Representative WAGNER has remained an outspoken champion for life. Representative WAGNER has worked to protect unborn life, through her vocal support of the Pain-Capable Unborn Child Protection Act and so many other pieces of pro-life legisltaion. Additionally, she has helped lead the charge to prevent taxpayer funding of abortion on-demand.

This public servant's efforts to protect vulnerable children from sexual exploitation and trafficking are particularly inspirational. She has fought hard for legislation that would increase the penalties for criminals who profit from sexual exploitation of innocent children.

Representative WAGNER's commitment to children both inside and outside the womb is commendable. I know I take inspiration from her years of work on behalf of vulnerable children. Therefore, I offer my praise and gratitude for that work as the U.S. Supreme Court takes up Dobbs v. Jackson Women's Health Organization, a case that could significantly change the landscape in terms of protecting young lives.

ADDITIONAL STATEMENTS

TRIBUTE TO BRANDON BOUCHARD

• Mr. BARRASSO. Madam President, I would like to take the opportunity to express my appreciation to Brandon for his hard work as an intern in the Senate Republican conference. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

Brandon is a native of Maryland. He is a graduate of the University of Maryland, College Park, where he studied philosophy, politics, and economics. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank Brandon for the dedication he has shown while working for me and my staff. It is a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his journey.•

TRIBUTE TO GARTH OWEN COSSAIRT

• Mr. BARRASSO. Madam President, I would like to take the opportunity to express my appreciation to Owen for his hard work as an intern in the Energy and Natural Resources Committee. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

Owen is a native of Laramie. He is a graduate of the University of Wyoming, where he studied mathematics. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank Owen for the dedication he has shown while working for me and my staff. It is a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his journey.•

TRIBUTE TO DAVID GIRALT

• Mr. BARRASSO. Madam President, I would like to take the opportunity to express my appreciation to David for his hard work as an intern in my Washington, DC, office. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

David is a native of Casper. He is a graduate student at George Washington University, where he is studying legislative affairs. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank David for the dedication he has shown while working for me and my staff. It is a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his journey.•

TRIBUTE TO STEPHEN HANK HOVERSLAND

• Mr. BARRASSO. Madam President, I would like to take the opportunity to express my appreciation to Hank for his hard work as an intern in the Energy and Natural Resources Committee. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

Hank is a native of Casper. He is a student at the University of Wyoming, where he is studying political science and economics. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank Hank for the dedication he has shown while working for me and my staff. It is a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his journey.•

TRIBUTE TO MATTHEW LOWE

• Mr. BARRASSO. Madam President, I would like to take the opportunity to express my appreciation to Matthew for his hard work as an intern in the Senate Republican conference. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

Matthew is a native of Oklahoma. He is a graduate of the Bush School of Government and Public Service at Texas A&M University, where he studied international affairs. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank Matthew for the dedication he has shown while working for me and my staff. It is a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his journey.•

TRIBUTE TO WILLIAM TORGERSON

• Mr. BARRASSO. Madam President, I would like to take the opportunity to express my appreciation to Billy for his hard work as an intern in my Washington, DC, office. I recognize his efforts and contributions to my office as well as to the State of Wyoming.

Billy is a native of Riverton. He is a student at Georgetown University, where he is studying government and English. He has demonstrated a strong work ethic, which has made him an invaluable asset to our office. The quality of his work is reflected in his great efforts over the last several months.

I want to thank Billy for the dedication he has shown while working for me and my staff. It is a pleasure to have him as part of our team. I know he will have continued success with all of his future endeavors. I wish him all my best on his journey.•

ADAMS STATE UNIVERSITY CENTENNIAL

• Mr. BENNET. Madam President, it is my honor to congratulate Adams State University on 100 years of educating students in Alamosa, CO. The school was established on May 4, 1921, as Adams State Normal School by the Colorado Legislature following the tireless advocacy of Colorado State Representative William ''Billy'' H. Adams. Founded as a teacher's college, Adams State now has more than 3,000 students enrolled in 27 bachelor's degree programs, nine master's degree programs, and one Ph.D. degree program.

Located in the San Luis Valley with deep Hispano roots, Adams State was the first federally designated Hispanic serving institution in Colorado. The school has also fostered an elite distance-running culture over decades after hosting the U.S. Olympic Marathon Trials in August 1968.

Over the past 100 years, Adams State has educated thousands of community leaders, businessowners, doctors, attorneys, farmers and ranchers, and, most

important, teachers and has been a key economic and cultural educational institution for Alamosa and the entire San Luis Valley.●

RECOGNIZING THE 2020–2021 NATIONAL FFA OFFICER TEAM

● Mr. BOOZMAN. Madam President, I rise today to recognize the 2020–2021 National FFA officer team who recently retired at the 94th National FFA Convention and Expo in Indianapolis, IN. Team members include president Doster Harper of Georgia, central region vice president Paxton Dahmer of Missouri, eastern region vice president Miriam Hoffman of Illinois, western region vice president David Lopez of California, southern region vice president Artha Jonassaint of Florida, and from my home State of Arkansas, National FFA secretary Anna Mathis.

The Future Farmers of America was founded in 1928 by a group of young farmers with dreams of developing an organization to address the challenges of feeding a growing population. Their leadership was founded on their experience and passion for agricultural pursuits. Now known as the National FFA Organization to represent its diverse membership, FFA grows the next generation of leaders, builds communities, and strengthens agriculture. There are 735,038 middle and high school FFA members in 8,817 chapters in all 50 States and Puerto Rico.

Each year, six student members are elected to represent FFA as a national officer. They serve the organization at the highest level, promoting FFA and inspiring members, advisers, staff, teachers, alumni, and supporters. These individuals pause their educational pursuits and other commitments for an entire year in order to fully dedicate themselves to bettering the organization and the agricultural industry. National FFA officers spend time attending, speaking at, and facilitating FFA camps, conferences, and conventions and often meet with donors, stakeholders, and alumni. Additionally, national officers serve as members of the National FFA board of directors, a testament to FFA being a student-led organization. It is no secret that these young leaders have a profound impact on the future of the organization and agriculture.

The 2020–2021 National FFA officer team led the organization with character, determination, and grit in the midst of a global pandemic. During this year and a half when many schools moved online and extracurricular activities at school, such as FFA, were unable to meet and continue normally, it is remarkable that, under this team's leadership, the number of FFA chapters in the organization increased despite the hardships faced. Their tenure as a national officer concluded after planning and leading the 94th National FFA Convention and Expo. The largest youth convention in the country, this year's convention drew over 60,000 registered attendees.

Behind every great team are hosts of people who support them. I commend the families, staff, advisers, teachers, mentors, students, alumni, and others who supported these leaders and FFA. Their tenacity and leadership is encouraging to those they serve and to myself. I had the opportunity to visit with these national officers during their year of service. It has been an honor to meet and interact with this team. I am ever-increasingly optimistic about the future of agriculture, especially with passionate, dedicated leaders like themselves at the helm. Doster, Anna, Paxton, Miriam, David, and Artha, I wish you the best in your future endeavors and congratulate you for your year of service as the 2020–2021 National FFA officer team.●

CONGRATULATING THE KINDRED HIGH SCHOOL VIKINGS

● Mr. CRAMER. Madam President, for the second time this year, I have the privilege of congratulating my alma mater, Kindred High School, on a State championship.

In March, my hometown school celebrated the boys basketball team's first-ever State championship. Eight months later, on November 12, the Kindred Vikings football team won the State 11B title at the Dakota Bowl State Football Tournament. The Vikings defeated longtime rivals, the No. 1-ranked Hillsboro-Central Valley Burros, by a score of 37 to 14, for the championship. They had earlier won their first three games, defeating Lisbon, Central Cass, and Bishop Ryan teams.

This was the first State championship for the Vikings since State playoffs sponsored by the North Dakota High School Activities Association began in 1975. They had made only one other Dakota Bowl appearance in 2016. To advance to the tournament this year, the Vikings defeated the Langdon-Edmore-Munich Cardinals, which had played in every Dakota Bowl since 2016.

Graduating from Kindred High School in 1979, I lettered for 4 years in football, basketball and track. I was the starting quarterback my junior and senior years, and our team was bad, me especially.

Knowing firsthand what it is like to persevere on a losing team, watching these Kindred Vikings, who ended the season with a 12–1 record, was thrilling. I saw very talented athletes excel by tapping into the strength of each player. Notably, the impressive skills of running back Trey Heinrich did not go unnoticed when he was named the MaxPreps North Dakota Player of the Year.

I want to recognize this year's team members Charles Biewer, Masen Allmaras, Lukas Klabunde, Izaak Spelhaug, Maxwell McQuillan, Andrew Trom, Taylor Stefonowicz, Carter Schmitz, Caleb Klabunde, Connor Rolland, Jack McDonald, Wyatt Briscoe, Graham Glasoe, Jordyn Sunram, Hayden Cichy, Owen Hoyme, Kylan Swenson, Jorgen Swenson, Camron Schwartzwalter, Trey Heinrich, Ty Roesler, Tyson Johnson, Chase Miller, Jeremiah Dockter, Alex Moffet, Jacob Hiatt, Samuel Jenness, Jacob Lund, Jack Huesman, Blake Houska, Tate Miller, Landon Kottsick, Grant Spelhaug, Andrew Haley, Colin Lunde, Ethan Fornshell, Mason Nipstad, Kelby Erdmann, Dilon Filler, Riley Sunram, Jack Packer, Jack Olson, Hunter Bindas, Maxwell Opgrand, and Ryker Lachowitzer.

I congratulate the team, as well as Coach Matt Crane, his assistants Brad Ambrosius, Eric Burgad, Joe Harder, Nate Safe, and Ryan Sunram and all the hometown fans on winning this championship.

I join the rest of North Dakota in thanking the Kindred Vikings for inspiring all of us to achieve excellence. For the second time this year, they have demonstrated what can be achieved by combining faith and passion with determination and teamwork.●

TRIBUTE TO JOHN D. BECKETT

● Mrs. HYDE-SMITH. Madam President, with the U.S. Supreme Court set to consider Dobbs v. Jackson Women's Health Organization in oral arguments on December 1, 2021, I am taking time to recognize individuals whose dedication to the pro-life cause has led us to this point. In this case, I pay tribute to Mr. John D. Beckett from Elyria, OH. His activities have been intertwined with championing pro-life and religious freedom.

Mr. Beckett graduated from the Massachusetts Institute of Technology in 1960, after which he initially worked as an engineer in the aerospace industry. In 1963, he joined his father's small manufacturing business, R.W. Beckett Corporation, and 2 years later became president following his father's death. Under Mr. Beckett's leadership, this small company grew over time to become a worldwide leader in producing engineered components for residential and commercial heating. With its affiliates, the company employs nearly 1,000 people.

In addition to his business endeavors, Mr. Beckett has long been active in both church and community-related activities. This is where he has established himself as a champion of the pro-life movement.

In 1973, Mr. Beckett became a founding member of the Intercessors for America, a national prayer organization, and he continues to serve on the board today. The Intercessors for America has helped lead grassroots efforts for people of faith to unite in prayer for the pro-life movement and for the unborn. In addition, he also became a founding board member of King's College in New York City, a Christian university, and he also serves on the board of Cru—Campus Crusade for Christ International. Alongside

these community activities, Mr. Beckett also found time to become a published author, writing two books about faith in the workplace.

For these business and community activities, Mr. Beckett has received numerous accolades. He received an honorary doctor of law degree from both Spring Arbor University in 2002 and also from King's College in 2008. He was also named Christian Businessman of the Year by the Christian Broadcasting Network in 1999 and the Entrepreneur of the Year by Ernst & Young in 2003.

Today, he resides in Elyria, OH, with his wife, Wendy, to whom he has been married since 1961.

I am thankful to John D. Beckett for his support of many nonprofit organizations that defend the rights of the unborn and religious freedom. His work in helping establish the Intercessors for America has led to untold numbers of prayers being raised for the pro-life movement. I am pleased to honor his work through that organization as well as his lifetime of service to so many worthy causes.●

TRIBUTE TO PHIL BRYANT

● Mrs. HYDE-SMITH. Madam President, I am honored to pay tribute to former Governor Phil Bryant of Mississippi. While there are many things for which the Governor deserves praise, today I specifically want to speak about Governor Bryant's stalwart work during his term of office from 2012–2020 to protect and defend the most vulnerable of our society: unborn children.

While running for office, Phil Bryant promised Mississippians that he would work tirelessly as Governor to protect the rights of the unborn. He fulfilled that promise. Throughout two terms in office, Governor Bryant was a driving force behind legislative efforts to protect life in Mississippi.

In April 2012, Governor Bryant signed Mississippi House Bill 1390. This bill required abortion practitioners to be certified as obstetrician-gynecologists and to maintain admitting privileges at a local hospital. Through these requirements, this legislation sought to strengthen abortion regulations and ensure that women receive quality care for any complications following an abortion.

In April 2014, Governor Bryant signed Mississippi House Bill 1400, banning abortions performed after 20 weeks. This legislation cited a plethora of medical evidence, showing that a baby can feel pain at this stage, and that pregnant women are at increased health risks, even death, when undergoing later-term abortion procedures.

Additionally, Governor Bryant signed into law the Unborn Child Protection from Dismemberment Abortion Act in 2016, banning dismemberment abortions or those involving the practice known as D&E or ''dilation and evacuation.'' Dismemberment is the most prevalent method of second trimester abortion, accounting for 96 percent of all second trimester abortions. With the enactment of this law, Governor Bryant not only banned these violent dismemberment procedures from taking place in the Mississippi, he also prohibited the illegal trafficking of the bodies of aborted babies in Mississippi.

Governor Bryant did not stop there and continued working to keep his promise to make Mississippi ''the safest place in America'' for unborn babies. In 2018, he signed the Gestational Age Act, which banned abortions after 15 weeks in most cases. It is this law being challenged at the U.S. Supreme Court in Dobbs v. Jackson Women's Health.

Throughout all of these laws, Governor Bryant maintained steadfast courage and held tightly to his promise to the people of Mississippi to fight continuously to protect the unborn. I love what he once said when groups threatened legal action against our State's pro-life legislation. He said, ''We will all answer to the good Lord one day. I will say in this instance, 'I fought for the lives of innocent babies, even under threat of legal action.' ''

That is indeed true. When his time comes, Governor Bryant can stand tall before the Lord, having fought the good fight to protect the unborn. And indeed, when the Supreme Court hears oral arguments in the Dobbs case on December 1, Governor Bryant can smile in the knowledge that his work was not in vain.

For all these reasons, I call attention to Governor Phil Bryant. He deserves laudable recognition for his 8-year fight to protect and defend the right to life for the unborn babies in the womb, reflecting the character and values of the people of our State, Mississippi.●

TRIBUTE TO BECKY CURRIE

● Mrs. HYDE-SMITH. Madam President, it is an honor to pay tribute to Representative Becky Currie, a member of the Mississippi House of Representatives, who authored the Gestational Age Act. It is this State law that underlies the U.S. Supreme Court's consideration of Dobbs v. Jackson Women's Health Organization this term.

When the Supreme Court hears oral arguments on Dobbs on December 1, 2021, it will hear a defense of the pro-life cause generating from the work of Becky Currie, my friend and my representative. In the Mississippi House, she represents district 92, which covers my hometown of Brookhaven.

Becky's forethought in introducing this bill and shepherding it through the State legislature has led us to the point where the Supreme Court is considering a direct challenge to Roe v. Wade. By prohibiting most abortions after 15 weeks, the Gestational Age Act presents directly the question of whether Roe's viability standard remains good law.

Becky's background as a nurse, her tenacious personality, and her heart for the unborn made her the perfect person to sponsor this important bill. She knows how to fight and isn't afraid of criticism. Her stubborn persistence in promoting policies to protect the unborn has made Mississippi a safer place for women and their babies. Through the Supreme Court's consideration of her bill, Becky Currie has the potential to do that for our entire Nation.

As the Supreme Court prepares to hear oral arguments in the Dobbs case, we are all indebted to Representative Currie's her courage and tenacity in sponsoring the Gestational Age Act. Praise God for bringing us this far. I also pray that He will continue to work through Representative Currie, using her law to overrule Roe v. Wade and make our Nation a safer place for the unborn and their mothers.●

TRIBUTE TO MARK LEE DICKSON

● Mrs. HYDE-SMITH. Madam President, I rise to pay tribute to Pastor Mark Lee Dickson of Longview, TX, who founded the Sanctuary Cities for the Unborn Initiative in 2019. This innovative organization works to encourage cities and towns to adopt ordinances declaring themselves as Sanctuary Cities for the Unborn.

Under Pastor Dickson's leadership, this grassroots Sanctuary Cities for the Unborn movement has saved many babies throughout the Nation in 41 towns and cities that have adopted these ordinances.

This is not the only way that Pastor Dickson has dedicated himself to championing the pro-life movement. He also serves as the director of Grassroots for Right to Life of East Texas and as the senior pastor of Sovereign Love Church in Longview.

Across our Nation, pro-life citizens of all ages and backgrounds represent the backbone of the grassroots movement to protect the unborn. Individuals like Pastor Dickson who take it on themselves to help promote life and prevent abortion in their own communities drive the passion in this movement.

The Pastor Dickson and millions of other Americans have kept this issue salient for our political discourse and has led us to the place where the U.S. Supreme Court will be reconsidering its misguided abortion jurisprudence established by Roe v. Wade when it takes up a challenge to a Mississippi law banning most abortions after 15 weeks gestation. In Dobbs v. Jackson Women's Health Organization, the stage is set for the potential overturning of Roe and returning the issue of abortion to the States.

I pray for Pastor Dickson and that God would raise up more like him. Pastor Dickson's example shows that the courage of one person can make a difference.●

TRIBUTE TO LYNN FITCH

• Mrs. HYDE-SMITH. Madam President, I rise to pay tribute to Mississippi Attorney General Lynn Fitch.

My State has much to be proud of in Attorney General Fitch as the first Republican to hold this office in almost 150 years and as Mississippi's first female attorney general ever.

Specifically today, I rise to honor her for her unwavering fight to defend Mississippi's pro-life laws. Attorney General Fitch is representing the State of Mississippi in Dobbs v. Jackson Women's Health Organization at the U.S. Supreme Court this term. This case is the most anticipated abortion case to reach the Court since Casey v. Planned Parenthood in 1992, nearly 30 years ago.

In the Dobbs case, Attorney General Fitch is defending a challenge to Mississippi House bill 1510, the Gestational Age Act Enacted in 2018, this legislation bans most abortions after 15 weeks gestation. By consistently defending this law all the way up to the Supreme Court, Attorney General Fitch has set the stage for the Court to consider overturning Roe v. Wade and return the issue of abortion to the States.

The Dobbs case presents the strongest challenge to Roe in our lifetime. It is encouraging that the Supreme Court, with its first conservative majority in many years, will hear arguments on the merits of this Mississippi law. I am so proud that our female Mississippi Attorney General will be in the courtroom to defend our law in this case.

In arguing for the Court to reconsider Roe in the State's brief in the case, Attorney General Fitch said, ''There are those who would like to believe that Roe v. Wade settled the issue of abortion once and for all. But all it did was establish a special-rules regime for abortion jurisprudence that has left these cases out of step with other Court decisions and neutral principles of law applied by the Court. As a result, state legislatures, and the people they represent, have lacked clarity in passing laws to protect legitimate public interests, and artificial guideposts have stunted important public debate on how we, as a society, care for the dignity of women and their children.''

I wholeheartedly agree. The unlimited-abortion regime created by the Roe decision was wrong when it was handed down, and it is wrong now. It is bad for the unborn, and it is bad for women. I hope the Supreme Court recognizes that when it hears oral arguments in the Dobbs case on December 1.

I am confident Attorney General Fitch will make our State proud by steadfastly defending Mississippi's law to protect unborn. Mississippians are proud to have this champion for life representing our State in this landmark case. I am praying for General Fitch and for her staff as they prepare to continue the fight to defend life before the highest court in the land.•

RECOGNIZING INTERNS

• Ms. ROSEN. Madam President, I am proud to host a number of interns from Nevada in my office, all of whom have contributed greatly to my work in the U.S. Senate. I know I speak for my colleagues as well when I say that many of our interns have enjoyed and benefited from a wonderful program operated by the Stennis Center for Public Service. This program is designed to enhance the internship experience for exceptional future leaders, giving young Americans an inside look at how Congress works and an opportunity to learn from bipartisan senior staffers and foster bipartisan relationships that will carry some of them through their career supporting Congress.

Stennis interns are selected based on their employment experience, college course load, and future service to Congress. This fall, 32 interns were chosen to be a part of this prestigious experience. These interns serve us on both sides of the aisle, working for Democrats and Republicans in the House and Senate, including one exceptional intern in my office who was awarded this opportunity: Natalie Gilbert of Las Vegas, NV.

Natalie is an impressive young Nevadan, having earned the distinguished honors of State of Nevada Mock Trial Outstanding Attorney and National Merit Commended Scholar in 2020. Before interning with my office, she interned with the Clark County District Attorney's Office in the homicide and domestic violence departments and worked directly with their victim advocacy program. Surpassing over 100 hours of volunteer service, Natalie has been an invaluable member of our Las Vegas community. I am proud to recognize Natalie and her incredible efforts. I wish her only the best as she continues to pursue her studies in political economy and justice and peace studies at Georgetown University.

In addition to Natalie, I would like to congratulate all of the Stennis interns on their completion of this exceptional program. I also thank the Stennis Center and their senior Fellows for providing a meaningful experience and fostering bipartisan work.

I ask that the names of the 2021 Fall Stennis congressional interns and the offices in which they work be printed in the RECORD.

The material follows:

Delanie Blubaugh, LaVale, MD, U.S. Representative David Trone; Sameer Chhetri, Philadelphia, PA, U.S. Representative Lois Frankel; Alexandra Dorotinsky, Damascus, MD, U.S. Senator Chris Van Hollen; Adam Duffy, Washington, DC, House Committee on Rules; Drew Ficociello, Washington, DC, U.S. Representative Cindy Axne; Rukmini Ganesh, Bowling Green, KY, House Committee on Education and Labor.

Natalie Gilbert, Las Vegas, NV, U.S. Senator Jacky Rosen; Ava Goble, Hilo, HI, U.S. Representative Kaiali'i Kahele; Diana Grechukhina, Ocean City, MD, U.S. Senator Chris Van Hollen; Kathleen Griffith, Washington, DC, Senate Special Committee on Aging; Kendall Groza, Washington, DC, U.S. Representative Billy Long; Amanda Guilardi, Washington, DC, House Committee on the Judiciary.

Kylie Harlan, Bells, TX, U.S. Representative Kevin Brady; Victoria Izaguirre, Spring Branch, TX, U.S. Representative Randy Weber; Niklas Kleinworth, Washington, DC, U.S. Senator James Risch; Catherine Lawson, Arlington, VA, U.S. Representative Kevin Brady; Haley Ledford, Fort Dodge, IA, U.S. Representative Randy Feenstra; Laura Ludwig, Washington, DC, U.S. Representative Jimmy Panetta.

Sophie Mittelstaedt, Washington, DC, U.S. Representative Marilyn Strickland; Jennifer Rivera-Galindo, Miami, FL, Senate Foreign Relations Committee; Jeremy Rodriguez-Melendez, Hormigueros, PR, U.S. Representative Don Young; Owen Rosenberg, Washington, DC, U.S. Representative Andrew Garbarino; Caroline Rykard, Midway, GA, U.S. Representative Buddy Carter; Natalie Salazar, Houston, TX, U.S. Representative Sylvia Garcia.

Ethan Sanders, Bartlesville, OK, U.S. Representative Lizzie Fletcher; Ben Savercool, Washington, DC, House Committee on Appropriations; Alexandra Schindewolf, Woodbine, NJ, U.S. Representative Ken Buck; Alexander Siegal, Longboat Key, FL, U.S. Representative Charlie Crist; Jaydn Smith, Washington, DC, U.S. Senator Deb Fischer; Sydney Smith, Washington, DC, U.S. Representative Mondaire Jones.

McKayla Steineke, Boston, MA, Senate Foreign Relations Committee; Jessie Xu, West Hartford, CT, Senate Committee on Banking, Housing and Urban Affairs.•

TRIBUTE TO MAHAM SHAH

• Mr. THUNE. Madam President, today I recognize Maham Shah, an intern in my Washington, DC, office, for all of the hard work she has done for me, my staff, and the State of South Dakota over the past several months.

Maham is a recent graduate of Baylor University in Waco, TX, having earned degrees in psychology and political science. This spring, Maham plans to continue serving the American people by working on Capitol Hill. She is a hard worker who has been dedicated to getting the most out of her internship experience.

I extend my sincere thanks and appreciation to Maham for all of the fine work she has done and wish her continued success in the years to come.•

TRIBUTE TO DESTINY WENGER

• Mr. THUNE. Madam President, today I recognize Destiny Wenger, an intern in my Aberdeen, SD, office, for all of the hard work she has done for me, my staff, and the State of South Dakota over the past several months.

Destiny is a graduate of Hazelton-Moffit-Braddock High School in Hazelton, ND. Currently, she is attending Northern State University in Aberdeen, SD, where she is majoring in political science. She is a hard worker who has been dedicated to getting the most out of her internship experience.

I extend my sincere thanks and appreciation to Destiny for all of the fine work she has done and wish her continued success in the years to come.•

TRIBUTE TO LAUREN CARSON

• Mr. WHITEHOUSE. Madam President, I rise today to honor an accomplished policymaker, a protector of environmental and public health, and my State representative: Lauren Carson. Representative Carson represents Rhode Island's 75th district and has a long history of working on issues related to sea level rise, reducing waste, and protecting the health and safety of Rhode Islanders.

Representative Carson holds a bachelor's degree from Ramapo College and two master's degrees from the University of Rhode Island. She is a businessowner and an environmental advocate who worked for several years with Clean Water Action.

Representative Carson also served her community through several organizations, including the advisory board of the Alliance for a Livable Newport, the Newport Energy and Environment Commission, the Rhode Island Green Infrastructure Coalition, and the Environmental Council of Rhode Island.

In 2014, Representative Carson successfully ran for a seat in the State legislature. At the statehouse, she has moved policy forward to protect Rhode Island's environment. Among many other accomplishments, Ms. Carson created and led a commission on the effects of rising seas. She introduced a bill that created a uniform statewide process for permitting solar panel installations. She cosponsored legislation to phase out polluting cesspools. Earlier this year, she was appointed as, deputy majority leader, a role which she used to steward the 2021 Act on Climate into law, setting statewide net-zero goals for 2050 across all sectors. She coleads the Aquidneck Island Climate Caucus to give voice to the importance of preventing and preparing for a warmer world and focus the island's efforts on sea level rise.

I am glad to recognize Representative Carson's dedicated service and to share my appreciation for all of her contributions to our State and our environment.•

TRIBUTE TO DAWN EUER

• Mr. WHITEHOUSE. Madam President, I rise today to honor one of Rhode Island's most respected oceans and environmental policymakers, who happens to also be my State Senator, Dawn Euer. All of us whom have worked with Senator Euer recognize her deep commitment to Rhode Island and to safeguarding the future of the planet by fighting the climate crisis.

Senator Euer earned a law degree from Roger Williams University. While in law school, she served as a legal intern in my office, where I saw firsthand her dedication to public service and to using the law to better the lives of others.

Senator Euer began her political career as an activist and organizer. She was instrumental in the fight to make gay marriage the law of the land in Rhode Island.

Senator Euer has served on the boards of the Environmental Justice League of Rhode Island and Bike Newport. She has also advised the Newport City Council on energy efficiency, renewables, sustainable planning, and other environmental matters.

In 2017, Senator Euer successfully ran to represent parts of Newport and Jamestown in the Rhode Island State Senate. Running in a district on the front lines of climate change and sea level rise, Senator Euer advocated for substantial investments in renewable energy and resiliency. In the last legislative session, Senator Euer delivered on that promise in a big way. She succeeded in passing the Act on Climate bill, the most comprehensive climate legislation in State history. As the lead sponsor, Senator Euer developed an actionable plan to create mandatory and enforceable emissions reduction goals that chart a course to a safer future. With that legislative victory in hand, Senator Euer recently traveled to COP26 in Glasgow to help show the world that American climate leadership is back.

For my friend Senator Euer's tireless efforts in championing the 2021 Act on Climate and for all of her hard work on behalf of the people of Newport and Jamestown, I stand today to recognize her.•

TRIBUTE TO MEG KERR

• Mr. WHITEHOUSE. Madam President, I rise today to honor Meg Kerr, a staunch advocate for the environmental movement. Ms. Kerr retired earlier this year after a successful career of climate leadership and service to the State of Rhode Island.

After graduating from Brown University and the University of North Carolina, Ms. Kerr began the early part of her career as a scientist. She worked for the Environmental Protection Agency across North Carolina, Virginia, and Washington, D.C., where she partnered with States to standardize water quality reporting aligned with the Clean Water Act.

Ms. Kerr then moved back to Rhode Island and quickly established herself as a prominent advocate for the environment, taking on roles at the Rhode Island Rivers Council, the Narragansett Bay Estuary Program, and Clean Water Action. Ms. Kerr closed out her impressive career as the Audubon Society of Rhode Island's Senior Director of Policy.

To add to the list of her accomplishments, Ms. Kerr was a founder of the Rhode Island Green Infrastructure Coalition and helped launch the Providence Stormwater Innovation Center. She also helped found the annual Land and Water Conservation Summit that brought together hundreds of environmentalists from the State and region for over a decade. Ms. Kerr is passionate about pollinators, as demonstrated by her work organizing the Bee Rally to bring attention to the threats faced by our beloved bugs.

Ms. Kerr is a fierce and respected leader for the environment and a familiar face at the Rhode Island statehouse. Her expertise, mentorship of others, and ability to get things done for Rhode Island's environmental community has made a real mark on our State. I am proud to recognize her service and thank her for all she has done to protect our environment.•

MESSAGES FROM THE PRESIDENT

Messages from the President of the United States were communicated to the Senate by Mr. Swann, one of his secretaries.

EXECUTIVE MESSAGES REFERRED

As in executive session the Presiding Officer laid before the Senate messages from the President of the United States submitting sundry nominations which were referred to the Committee on the Judiciary.

(The messages received today are printed at the end of the Senate proceedings.)

PRESIDENTIAL MESSAGE

REPORT ON THE ISSUANCE OF AN EXECUTIVE ORDER THAT TERMINATES THE NATIONAL EMERGENCY DECLARED IN EXECUTIVE ORDER 13712 OF NOVEMBER 22, 2015, WITH RESPECT TO BURUNDI, AND REVOKES THAT EXECUTIVE ORDER—PM 18

The PRESIDING OFFICER laid before the Senate the following message from the President of the United States, together with an accompanying report; which was referred to the Committee on Banking, Housing, and Urban Affairs:

To the Congress of the United States:

Consistent with subsection 204(b) of the International Emergency Economic Powers Act, 50 U.S.C. 1703(b), I hereby report that I have issued an Executive Order that terminates the national emergency declared in Executive Order 13712 of November 22, 2015, and revokes that Executive Order.

The President issued Executive Order 13712 to deal with the unusual and extraordinary threat to the national security and foreign policy of the United States constituted by the situation in Burundi, which had been marked by the killing of and violence against civilians, unrest, incitement of imminent violence, and significant political repression. In Executive Order 13712, the President addressed the threat by blocking the property and interests in property of, among others, persons determined by the Secretary of the Treasury, in consultation with the Secretary of State, to be responsible for or

complicit in actions or policies that threaten the peace, security, and stability of Burundi or undermine democratic processes or institutions in Burundi, or to have engaged in human rights abuses.

I have determined that the situation in Burundi that gave rise to the national emergency declared in Executive Order 13712 has been significantly altered by events of the past year, including the transfer of power following elections in 2020, significantly decreased violence, and President Ndayishimiye's pursuit of reforms across multiple sectors. For these reasons I have determined that it is necessary to terminate the national emergency declared in Executive Order 13712 and revoke that order.

I am enclosing a copy of the Executive Order I have issued.

JOSEPH R. BIDEN,Jr.,

THE WHITE HOUSE, *November 18, 2021*.

MESSAGE FROM THE HOUSE

At 11:15 a.m., a message from the House of Representatives, delivered by Mrs. Alli, one of its reading clerks, announced that the House has passed the following bill, in which it requests the concurrence of the Senate:

H.R. 5652. An act to amend the Homeland Security Act of 2002 to establish the Acquisition Review Board in the Department of Homeland Security, and for other purposes.

MEASURES REFERRED

The following bill was read the first and the second times by unanimous consent, and referred as indicated:

H.R. 5652. An act to amend the Homeland Security Act of 2002 to establish the Acquisition Review Board in the Department of Homeland Security, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

PRIVILEGED NOMINATIONS REFERRED TO COMMITTEE

On request by Senator TOMMY TUBERVILLE, under the authority of S. Res. 116, 112th Congress, the following nomination was referred to the Committee on Homeland Security and Governmental Affairs: Michael F. Gerber, of Pennsylvania, to be a Member of the Federal Retirement Thrift Investment Board for a term expiring September 25, 2022, vice Michael D. Kennedy, term expired.

On request by Senator TOMMY TUBERVILLE, under the authority of S. Res. 116, 112th Congress, the following nomination was referred to the Committee on Homeland Security and Governmental Affairs: Michael F. Gerber, of Pennsylvania, to be a Member of the Federal Retirement Thrift Investment Board for a reappointment term expiring September 25, 2026.

EXECUTIVE AND OTHER COMMUNICATIONS

The following communications were laid before the Senate, together with accompanying papers, reports, and documents, and were referred as indicated:

EC–2626. A communication from the Treasurer of the National Gallery of Art, transmitting, pursuant to law, the Gallery's Inspector General Report for fiscal year 2021; to the Committee on Homeland Security and Governmental Affairs.

EC–2627. A communication from the Director, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Federal Acquisition Circular 2022–01, Small Entity Compliance Guide'' (FAC 2022–01) received in the Office of the President of the Senate on November 15, 2021; to the Committee on Homeland Security and Governmental Affairs.

EC–2628. A communication from the Director, Office of Acquisition Policy, General Services Administration, transmitting, pursuant to law, the report of a rule entitled ''Federal Acquisition Regulation; Federal Acquisition Circular 2022–01, Introduction'' (FAC 2022–01) received in the Office of the President of the Senate on November 15, 2021; to the Committee on Homeland Security and Governmental Affairs.

EC–2629. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 24–198, ''Wilkinson School Disposition Authorization Temporary Act of 2021''; to the Committee on Homeland Security and Governmental Affairs.

EC–2630. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 24–199, ''Advisory Neighborhood Commissions Humanitarian Relief Extension Temporary Amendment Act of 2021''; to the Committee on Homeland Security and Governmental Affairs.

EC–2631. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 24–200, ''Coronavirus Unemployment Compensation Provisions Sunset Temporary Amendment Act of 2021''; to the Committee on Homeland Security and Governmental Affairs.

EC–2632. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 24–201, ''Office of Administrative Hearings Unemployment Appeals Extension Temporary Amendment Act of 2021''; to the Committee on Homeland Security and Governmental Affairs.

EC–2633. A communication from the Chairman of the Council of the District of Columbia, transmitting, pursuant to law, a report on D.C. Act 24–202, ''Certified Midwife Credential Amendment Act of 2021''; to the Committee on Homeland Security and Governmental Affairs.

EC–2634. A communication from the Secretary of the Board of Governors, United States Postal Service, transmitting, pursuant to law, the Board's annual report relative to its compliance with Section 3686(c) of the Postal Accountability and Enhancement Act of 2006; to the Committee on Homeland Security and Governmental Affairs.

EC–2635. A communication from the Chairman of the Board, Farm Credit System Insurance Corporation, transmitting, pursuant to law, the Corporation's consolidated report addressing the Federal Managers Financial Integrity Act (FMFIA or Integrity Act); to the Committee on Homeland Security and Governmental Affairs.

EC–2636. A communication from the Board Chairman and Chief Executive Officer, Farm Credit Administration, transmitting, pursuant to law, the Administration's Semiannual Report of the Inspector General and the Semiannual Management Report on the Status of Audits for the period from April 1, 2021 through September 30, 2021; to the Committee on Homeland Security and Governmental Affairs.

EC–2637. A communication from the Board Chairman and Chief Executive Officer, Farm Credit Administration, transmitting, pursuant to law, the Administration's Performance and Accountability Report for fiscal year 2021; to the Committee on Homeland Security and Governmental Affairs.

EC–2638. A communication from the Senior Advisor, Department of Health and Human Services, transmitting, pursuant to law, a report relative to two (2) vacancies in the Department of Health and Human Services, received in the Office of the President of the Senate on November 15, 2021; to the Committee on Indian Affairs.

EC–2639. A communication from the Director of the Office of Regulatory Affairs and Collaborative Action, Bureau of Indian Affairs, Department of the Interior, transmitting, pursuant to law, the report of a rule entitled ''Election of Officers of the Osage Minerals Council'' (RIN1076–AF58) received in the Office of the President of the Senate on November 2, 2021; to the Committee on Indian Affairs.

EXECUTIVE REPORTS OF COMMITTEES

The following executive reports of nominations were submitted:

By Mr. MANCHIN for the Committee on Energy and Natural Resources.

*Sara C. Bronin, of Connecticut, to be Chairman of the Advisory Council on Historic Preservation for a term expiring January 19, 2025.

By Mr. DURBIN for the Committee on the Judiciary.

Cindy K. Chung, of Pennsylvania, to be United States Attorney for the Western District of Pennsylvania for the term of four years.

Gary M. Restaino, of Arizona, to be United States Attorney for the District of Arizona for the term of four years.

*Nomination was reported with recommendation that it be confirmed subject to the nominee's commitment to respond to requests to appear and testify before any duly constituted committee of the Senate.

(Nominations without an asterisk were reported with the recommendation that they be confirmed.)

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

The following bills and joint resolutions were introduced, read the first and second times by unanimous consent, and referred as indicated:

By Mr. WYDEN (for himself and Ms. LUMMIS):

S. 3231. A bill to amend title 18, United States Code, to require law enforcement officials to obtain a warrant before accessing data stored in cars, and for other purposes; to the Committee on the Judiciary.

By Mr. CASEY (for himself, Ms. KLOBUCHAR, Mr. BLUMENTHAL, Mr. COTTON, Mr. MARKEY, Ms. CORTEZ MASTO, Ms. SMITH, Ms. WARREN, Mr. COONS, Mrs. FEINSTEIN, Ms. BALDWIN, Mr. CARDIN, and Mr. DURBIN):

S. 3232. A bill to require the Consumer Product Safety Commission to promulgate a

consumer product safety rule for free-standing clothing storage units to protect children from tip-over related death or injury, and for other purposes; to the Committee on Commerce, Science, and Transportation.

By Ms. COLLINS (for herself and Mr. DURBIN):

S. 3233. A bill to help increase the development, distribution, and use of clean cookstoves and fuels to improve health, protect the climate and environment, empower women, create jobs, and help consumers save time and money; to the Committee on Foreign Relations.

By Mr. OSSOFF (for himself and Mr. SCOTT of South Carolina):

S. 3234. A bill to provide for outreach and assistance to historically Black colleges and universities regarding Defense Innovation Unit programs; to the Committee on Armed Services.

By Mr. MENENDEZ (for himself, Mr. BROWN, and Mr. CARDIN):

S. 3235. A bill to apply the Truth in Lending Act to small business financing, and for other purposes; to the Committee on Banking, Housing, and Urban Affairs.

By Ms. KLOBUCHAR (for herself, Mr. THUNE, Mr. HICKENLOOPER, and Mr. MORAN):

S. 3236. A bill to require the Federal Communications Commission to reform the contribution system of the Universal Service Fund, and for other purposes; to the Committee on Commerce, Science, and Transportation.

By Mr. SCHATZ (for himself and Mr. BRAUN):

S. 3237. A bill to amend title 49, United States Code, to include affordable housing incentives in certain capital investment grants, and for other purposes; to the Committee on Banking, Housing, and Urban Affairs.

By Mr. CASEY (for himself and Mr. DAINES):

S. 3238. A bill to assist employers providing employment under special certificates issued under section 14(c) of the Fair Labor Standards Act of 1938 in transforming their business and program models to models that support people with disabilities through competitive integrated employment, to phase out the use of such special certificates, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

By Mr. BROWN (for himself, Mr. KING, Ms. BALDWIN, Mr. CASEY, Ms. SMITH, Mr. BLUMENTHAL, Mr. VAN HOLLEN, Mr. MERKLEY, Mr. WHITEHOUSE, Ms. CORTEZ MASTO, Mr. MARKEY, Mr. KAINE, Ms. KLOBUCHAR, Mr. BOOKER, and Ms. ROSEN):

S. 3239. A bill to amend title XXVII of the Public Health Service Act to provide for a special enrollment period for pregnant persons, and for other purposes; to the Committee on Finance.

By Mr. RUBIO (for himself, Mrs. GILLIBRAND, Mr. COTTON, Mr. SCOTT of Florida, Mr. BRAUN, Mr. RISCH, and Mrs. BLACKBURN):

S. 3240. A bill to waive the application fee for applications for special use permits for veterans' special events at war memorials on land administered by the National Park Service in the District of Columbia and its environs, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. KENNEDY:

S. 3241. A bill to amend title 28, United States Code, to allow claims against foreign states for unlawful computer intrusion, and for other purposes; to the Committee on the Judiciary.

By Mr. MORAN:

S. 3242. A bill to provide for the settlement of claims relating to the Shab-eh-nay Band Reservation in Illinois, and for other purposes; to the Committee on Indian Affairs.

By Mr. LEE:

S. 3243. A bill to prohibit certain Federal agencies from requiring that any employee of such an agency receive a COVID–19 vaccine, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

By Ms. BALDWIN (for herself, Ms. COLLINS, Ms. ROSEN, Ms. MURKOWSKI, Mrs. GILLIBRAND, and Mr. CARDIN):

S. 3244. A bill to amend the Public Health Service Act to establish a Bio-Preparedness and Infectious Diseases Workforce Loan Repayment Program; to the Committee on Health, Education, Labor, and Pensions.

By Ms. MURKOWSKI (for herself and Mr. WHITEHOUSE):

S. 3245. A bill to establish the Interagency Working Group on Coastal Blue Carbon, and for other purposes; to the Committee on Commerce, Science, and Transportation.

By Mr. PETERS (for himself and Mrs. CAPITO):

S. 3246. A bill to amend title XVIII of the Social Security Act to reduce the occurrence of diabetes in Medicare beneficiaries by extending coverage under Medicare for medical nutrition therapy services to such beneficiaries with pre-diabetes or with risk factors for developing type 2 diabetes; to the Committee on Finance.

By Ms. CORTEZ MASTO (for herself, Mr. TESTER, Mr. BLUMENTHAL, Ms. ROSEN, Ms. HIRONO, Mr. BROWN, and Mr. KELLY):

S. 3247. A bill to extend certain expiring provisions of law relating to benefits provided under Department of Veterans Affairs educational assistance programs during COVID–19 pandemic, and for other purposes; to the Committee on Veterans' Affairs.

By Mr. RUBIO (for himself, Mr. BRAUN, Mr. CRAMER, and Mr. SCOTT of Florida):

S. 3248. A bill to allow States and Tribal entities to use unexpended COVID–19 relief funds to pay fines on behalf of employers for violating the emergency temporary standard issued by the Department of Labor relating to COVID–19 Vaccination and Testing and any final rule issued with respect to such emergency temporary standard, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

By Mr. WYDEN (for himself and Ms. LUMMIS):

S. 3249. A bill to revise the rules of construction applicable to information reporting requirements imposed on brokers with respect to digital assets, and for other purposes; to the Committee on Finance.

By Mr. CASEY:

S. 3250. A bill to increase access to higher education by providing public transit grants; to the Committee on Commerce, Science, and Transportation.

By Mr. DURBIN (for himself, Mr. WHITEHOUSE, Ms. WARREN, Mr. BROWN, Mr. BLUMENTHAL, Ms. HIRONO, Mr. MARKEY, and Mr. REED):

S. 3251. A bill to provide that chapter 1 of title 9 of the United States Code, relating to the enforcement of arbitration agreements, shall not apply to enrollment agreements made between students and certain institutions of higher education, and to prohibit limitations on the ability of students to pursue claims against certain institutions of higher education; to the Committee on Health, Education, Labor, and Pensions.

By Mr. LEE (for himself and Ms. LUMMIS):

S. 3252. A bill to address the supply chain backlog in the freight network at United States ports, and for other purposes; to the Committee on Commerce, Science, and Transportation.

By Mr. COTTON:

S. 3253. A bill to amend the Family and Medical Leave Act of 1993 to provide leave for the spontaneous loss of an unborn child, and for other purposes; to the Committee on Finance.

By Mr. MERKLEY (for himself, Mr. BLUMENTHAL, and Ms. WARREN):

S. 3254. A bill to provide grants to local educational agencies to help public schools reduce class size in the early elementary grades, and for other purposes; to the Committee on Health, Education, Labor, and Pensions.

By Mr. BOOKER:

S. 3255. A bill to direct the Secretary of Veterans Affairs to increase the number of Vet Centers in certain States based on population metrics, and for other purposes; to the Committee on Veterans' Affairs.

By Mr. SCOTT of Florida (for himself and Mr. LANKFORD):

S. 3256. A bill to amend the Robert T. Stafford Disaster Relief and Emergency Assistance Act to improve accountability of disaster contracts, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

By Mrs. SHAHEEN (for herself and Mrs. CAPITO):

S. 3257. A bill to amend the Controlled Substances Act to lengthen the period of time during which certain controlled substances must be administered to a patient after being delivered by a pharmacy to the administering practitioner; to the Committee on the Judiciary.

By Mr. MARKEY (for himself, Mr. VAN HOLLEN, Ms. KLOBUCHAR, Mr. BLUMENTHAL, and Ms. SMITH):

S. 3258. A bill to conduct or support further comprehensive research for the creation of a universal influenza vaccine or preventative; to the Committee on Health, Education, Labor, and Pensions.

By Ms. KLOBUCHAR (for herself and Mr. HOEVEN):

S. 3259. A bill to amend the Internal Revenue Code of 1986 to recognize Indian tribal governments for purposes of determining under the adoption credit whether a child has special needs; to the Committee on Finance.

By Mr. WICKER:

S. 3260. A bill to require a 20th anniversary review of the missions, capabilities, and performance of the Transportation Security Administration; to the Committee on Commerce, Science, and Transportation.

By Mr. BRAUN:

S. 3261. A bill to amend title 38, United States Code, to provide for the inclusion of certain emblems on headstones and markers furnished for veterans by the Secretary of Veterans Affairs, and for other purposes; to the Committee on Veterans' Affairs.

By Mr. WICKER (for himself, Mrs. CAPITO, Mr. MORAN, Mr. YOUNG, and Mrs. BLACKBURN):

S. 3262. A bill to improve the efficient movement of freight at ports in the United States, and for other purposes; to the Committee on Commerce, Science, and Transportation.

By Mr. SCOTT of Florida (for himself, Mr. TUBERVILLE, Mrs. BLACKBURN, Mr. JOHNSON, Mr. PORTMAN, Mr. LANKFORD, and Mr. LEE):

S. 3263. A bill to require the Inspector General of the Department of Homeland Security to investigate the vetting and processing of illegal aliens apprehended along the southwest border and to ensure that all laws are being upheld; to the Committee on the Judiciary.

By Mr. LUJÁN (for himself, Mr. CRAMER, Mr. HEINRICH, and Mr. MANCHIN):

S. 3264. A bill to require the Secretary of the Interior and the Secretary of Agriculture to develop long-distance bike trails on Federal land, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. PORTMAN (for himself and Mr. BROWN):

S. 3265. A bill to require the National Nuclear Security Administration to release all of its reversionary rights to the building located at 4170 Allium Court, Springfield, Ohio; to the Committee on Armed Services.

By Mr. MANCHIN (for himself and Mr. BARRASSO):

S. 3266. A bill to improve recreation opportunities on, and facilitate greater access to, Federal public land, and for other purposes; to the Committee on Energy and Natural Resources.

By Ms. KLOBUCHAR (for herself, Mr. BLUMENTHAL, Ms. HIRONO, and Mr. BOOKER):

S. 3267. A bill to reform the antitrust laws to better protect competition in the American economy, to amend the Clayton Act to modify the standard for an unlawful acquisition; to the Committee on the Judiciary.

By Mr. PAUL (for himself, Mr. SANDERS, and Mr. LEE):

S.J. Res. 31. A joint resolution providing for congressional disapproval of the proposed foreign military sale to the Kingdom of Saudi Arabia of certain defense articles; to the Committee on Foreign Relations.

SUBMISSION OF CONCURRENT AND SENATE RESOLUTIONS

The following concurrent resolutions and Senate resolutions were read, and referred (or acted upon), as indicated:

By Mr. DURBIN (for himself, Mr. RISCH, Mr. LEAHY, Mr. COONS, Mr. ROUNDS, Mr. BOOZMAN, and Mr. CARDIN):

S. Res. 456. A resolution expressing support for a free, fair, and peaceful December 4, 2021, election in The Gambia; to the Committee on Foreign Relations.

By Ms. WARREN (for herself, Mrs. CAPITO, and Mr. MARKEY):

S. Res. 457. A resolution expressing support for the designation of November 9, 2021, as ''National Microtia and Atresia Awareness Day''; to the Committee on Health, Education, Labor, and Pensions.

By Mr. COONS:

S. Res. 458. A resolution recognizing the 75th anniversary of the establishment of the United Nations Children's Fund; to the Committee on Foreign Relations.

ADDITIONAL COSPONSORS

S. 327

At the request of Mr. KELLY, the name of the Senator from Minnesota (Ms. KLOBUCHAR) was added as a cosponsor of S. 327, a bill to direct the Administrator of the Small Business Administration to establish a border closure recovery loan program for small businesses located near the United States border, and for other purposes.

S. 385

At the request of Mr. BROWN, the name of the Senator from California (Mr. PADILLA) was added as a cosponsor of S. 385, a bill to improve the full-service community school program, and for other purposes.

S. 435

At the request of Mr. CRAPO, the names of the Senator from California (Mr. PADILLA) and the Senator from New Mexico (Mr. HEINRICH) were added as cosponsors of S. 435, a bill to extend the Secure Rural Schools and Community Self-Determination Act of 2000.

S. 450

At the request of Mr. BOOKER, the name of the Senator from New York (Mr. SCHUMER) was added as a cosponsor of S. 450, a bill to award posthumously the Congressional Gold Medal to Emmett Till and Mamie Till-Mobley.

S. 535

At the request of Ms. ERNST, the name of the Senator from Georgia (Mr. OSSOFF) was added as a cosponsor of S. 535, a bill to authorize the location of a memorial on the National Mall to commemorate and honor the members of the Armed Forces that served on active duty in support of the Global War on Terrorism, and for other purposes.

S. 581

At the request of Mr. BROWN, the name of the Senator from Minnesota (Ms. SMITH) was added as a cosponsor of S. 581, a bill to amend title XIX of the Social Security Act to improve access to adult vaccines under Medicaid.

S. 697

At the request of Ms. ROSEN, the name of the Senator from Mississippi (Mrs. HYDE-SMITH) was added as a cosponsor of S. 697, a bill to require the Secretary of the Treasury to mint commemorative coins in recognition of the Bicentennial of Harriet Tubman's birth.

S. 904

At the request of Mr. RISCH, the names of the Senator from Oregon (Mr. WYDEN) and the Senator from New Hampshire (Ms. HASSAN) were added as cosponsors of S. 904, a bill to require the Secretary of the Interior, the Secretary of Agriculture, and the Assistant Secretary of the Army for Civil Works to digitize and make publicly available geographic information system mapping data relating to public access to Federal land and waters for outdoor recreation, and for other purposes.

S. 910

At the request of Mr. MERKLEY, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 910, a bill to create protections for financial institutions that provide financial services to cannabis-related legitimate businesses and service providers for such businesses, and for other purposes.

S. 1098

At the request of Mr. WARNER, the name of the Senator from Minnesota (Ms. SMITH) was added as a cosponsor of S. 1098, a bill to amend the Higher Education Act of 1965 to authorize borrowers to separate joint consolidation loans.

S. 1125

At the request of Ms. STABENOW, the name of the Senator from Louisiana (Mr. CASSIDY) was added as a cosponsor of S. 1125, a bill to recommend that the Center for Medicare and Medicaid Innovation test the effect of a dementia care management model, and for other purposes.

S. 1198

At the request of Ms. HASSAN, the name of the Senator from Maine (Ms. COLLINS) was added as a cosponsor of S. 1198, a bill to amend title 38, United States Code, to improve and expand the Solid Start program of the Department of Veterans Affairs, and for other purposes.

S. 1210

At the request of Mr. BLUMENTHAL, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of S. 1210, a bill to amend the Lacey Act Amendments of 1981 to clarify provisions enacted by the Captive Wildlife Safety Act, to further the conservation of certain wildlife species, and for other purposes.

S. 1488

At the request of Ms. DUCKWORTH, the name of the Senator from Rhode Island (Mr. WHITEHOUSE) was added as a cosponsor of S. 1488, a bill to amend title 37, United States Code, to establish a basic needs allowance for low-income regular members of the Armed Forces.

S. 1625

At the request of Mr. CRAMER, the name of the Senator from Tennessee (Mrs. BLACKBURN) was added as a cosponsor of S. 1625, a bill to authorize notaries public to perform, and to establish minimum standards for, electronic notarizations and remote notarizations that occur in or affect interstate commerce, to require any Federal court to recognize notarizations performed by a notarial officer of any State, to require any State to recognize notarizations performed by a notarial officer of any other State when the notarization was performed under or relates to a public Act, record, or judicial proceeding of the notarial officer's State or when the notarization occurs in or affects interstate commerce, and for other purposes.

S. 1679

At the request of Mr. CASEY, the name of the Senator from Maryland (Mr. CARDIN) was added as a cosponsor of S. 1679, a bill to amend title VII of the Public Health Service Act to authorize assistance for increasing workforce diversity in the professions of physical therapy, occupational therapy, respiratory therapy, audiology, and speech-language pathology, and for other purposes.

S. 1725

At the request of Mr. ROUNDS, the name of the Senator from South Carolina (Mr. GRAHAM) was added as a cosponsor of S. 1725, a bill to grant a Federal charter to the National American Indian Veterans, Incorporated.

S. 1748

At the request of Mr. MENENDEZ, the name of the Senator from North Carolina (Mr. TILLIS) was added as a cosponsor of S. 1748, a bill to modify the prohibition on recognition by United States courts of certain rights relating to certain marks, trade names, or commercial names.

S. 1780

At the request of Mr. BOOKER, the name of the Senator from Hawaii (Ms. HIRONO) was added as a cosponsor of S. 1780, a bill to remove college cost as a barrier to every student having access to a well-prepared and diverse educator workforce, and for other purposes.

S. 1813

At the request of Mr. COONS, the name of the Senator from Wyoming (Mr. BARRASSO) was added as a cosponsor of S. 1813, a bill to direct the Secretary of Health and Human Services to support research on, and expanded access to, investigational drugs for amyotrophic lateral sclerosis, and for other purposes.

S. 1901

At the request of Mr. TESTER, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of S. 1901, a bill to amend the Act of June 18, 1934, to reaffirm the authority of the Secretary of the Interior to take land into trust for Indian Tribes, and for other purposes.

S. 1964

At the request of Mr. BENNET, the name of the Senator from Washington (Ms. CANTWELL) was added as a cosponsor of S. 1964, a bill to amend the Omnibus Parks and Public Lands Management Act of 1996 to provide for the establishment of a Ski Area Fee Retention Account, and for other purposes.

S. 2103

At the request of Mr. PADILLA, the name of the Senator from Rhode Island (Mr. WHITEHOUSE) was added as a cosponsor of S. 2103, a bill to amend the Revised Statutes of the United States to hold certain public employers liable in civil actions for deprivation of rights, and for other purposes.

S. 2160

At the request of Mr. MORAN, the name of the Senator from Georgia (Mr. WARNOCK) was added as a cosponsor of S. 2160, a bill to prohibit the Administrator of General Services from establishing per diem reimbursements rates for travel within the continental United States (commonly known as ''CONUS'') for certain fiscal years below a certain level, and for other purposes.

S. 2233

At the request of Mr. BLUMENTHAL, the name of the Senator from North Carolina (Mr. BURR) was added as a cosponsor of S. 2233, a bill to establish a grant program for shuttered minor league baseball clubs, and for other purposes.

S. 2266

At the request of Mr. CARDIN, the name of the Senator from Delaware (Mr. COONS) was added as a cosponsor of S. 2266, a bill to amend the Internal Revenue Code of 1986 to improve the historic rehabilitation tax credit, and for other purposes.

S. 2342

At the request of Mrs. GILLIBRAND, the name of the Senator from Maine (Ms. COLLINS) was added as a cosponsor of S. 2342, a bill to amend title 9 of the United States Code with respect to arbitration of disputes involving sexual assault and sexual harassment.

S. 2376

At the request of Mr. CRUZ, the names of the Senator from California (Mrs. FEINSTEIN) and the Senator from Georgia (Mr. WARNOCK) were added as cosponsors of S. 2376, a bill to ensure the parental guardianship rights of cadets and midshipmen consistent with individual and academic responsibilities, and for other purposes.

S. 2390

At the request of Ms. DUCKWORTH, the name of the Senator from Hawaii (Ms. HIRONO) was added as a cosponsor of S. 2390, a bill to allow Americans to receive paid leave time to process and address their own health needs and the health needs of their partners during the period following a pregnancy loss, an unsuccessful round of intrauterine insemination or of an assisted reproductive technology procedure, a failed adoption arrangement, a failed surrogacy arrangement, or a diagnosis or event that impacts pregnancy or fertility, to support related research and education, and for other purposes.

S. 2493

At the request of Mr. BENNET, the name of the Senator from Iowa (Ms. ERNST) was added as a cosponsor of S. 2493, a bill to extend the deadline for eligible health care providers to use certain funds received from the COVID–19 Provider Relief Fund, and for other purposes.

S. 2559

At the request of Mr. PORTMAN, the name of the Senator from Georgia (Mr. WARNOCK) was added as a cosponsor of S. 2559, a bill to establish the National Deepfake and Digital Provenance Task Force, and for other purposes.

S. 2562

At the request of Ms. STABENOW, the names of the Senator from Maine (Mr. KING) and the Senator from North Dakota (Mr. CRAMER) were added as cosponsors of S. 2562, a bill to amend title XVIII of the Social Security Act to improve extended care services by providing Medicare beneficiaries with an option for cost effective home-based extended care under the Medicare program, and for other purposes.

S. 2675

At the request of Mr. CARDIN, the name of the Senator from New Hampshire (Mrs. SHAHEEN) was added as a cosponsor of S. 2675, a bill to amend the American Rescue Plan Act of 2021 to increase appropriations to Restaurant Revitalization Fund, and for other purposes.

S. 2721

At the request of Mr. CRAPO, the name of the Senator from Iowa (Ms. ERNST) was added as a cosponsor of S. 2721, a bill to require the Internal Revenue Service to issue a report on the tax gap, to establish a fellowship program within the Internal Revenue Service to recruit mid-career tax professionals to create and participate in an audit task force, and for other purposes.

S. 2727

At the request of Mr. LANKFORD, the name of the Senator from Arizona (Mr. KELLY) was added as a cosponsor of S. 2727, a bill to provide for a period of continuing appropriations in the event of a lapse in appropriations under the normal appropriations process, and establish procedures and consequences in the event of a failure to enact appropriations.

S. 2780

At the request of Mr. MARSHALL, the name of the Senator from Arkansas (Mr. BOOZMAN) was added as a cosponsor of S. 2780, a bill to amend title 10, United States Code, to prohibit certain adverse personnel actions taken against members of the Armed Forces based on declining the COVID–19 vaccine.

S. 2838

At the request of Mr. PORTMAN, the names of the Senator from Nevada (Ms. ROSEN) and the Senator from Georgia (Mr. WARNOCK) were added as cosponsors of S. 2838, a bill to require the Director of the Government Publishing Office to establish and maintain an online portal accessible to the public that allows the public to obtain electronic copies of all congressionally mandated reports in one place, and for other purposes.

S. 2959

At the request of Mr. THUNE, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 2959, a bill to provide that, due to disruptions caused by COVID–19, applications for impact aid funding for fiscal year 2023 may use certain data submitted in the fiscal year 2022 application.

S. 2960

At the request of Mr. MERKLEY, the name of the Senator from Massachusetts (Ms. WARREN) was added as a cosponsor of S. 2960, a bill to encourage reduction of disposable plastic products in units of the National Park System, and for other purposes.

S. 2973

At the request of Mrs. BLACKBURN, the name of the Senator from Iowa (Ms. ERNST) was added as a cosponsor of S. 2973, a bill to establish an Inspector General of the National Institutes of Health.

S. 3018

At the request of Mr. MARSHALL, the names of the Senator from Delaware (Mr. CARPER) and the Senator from Louisiana (Mr. CASSIDY) were added as

cosponsors of S. 3018, a bill to amend title XVIII of the Social Security Act to establish requirements with respect to the use of prior authorization under Medicare Advantage plans, and for other purposes.

S. 3079

At the request of Mrs. BLACKBURN, the name of the Senator from Missouri (Mr. HAWLEY) was added as a cosponsor of S. 3079, a bill to exempt essential workers from Federal COVID–19 vaccine mandates.

S. 3108

At the request of Ms. HIRONO, the name of the Senator from Ohio (Mr. BROWN) was added as a cosponsor of S. 3108, a bill to provide counsel for unaccompanied children, and for other purposes.

S. 3111

At the request of Mr. COONS, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 3111, a bill to require the Secretary of Energy to establish a grant program to support hydrogen-fueled equipment at ports and to conduct a study with the Secretary of Transportation and the Secretary of Homeland Security on the feasibility and safety of using hydrogen-derived fuels, including ammonia, as a shipping fuel.

S. 3118

At the request of Mr. COONS, the name of the Senator from Alaska (Ms. MURKOWSKI) was added as a cosponsor of S. 3118, a bill to require the Secretary of Energy to establish a hydrogen infrastructure finance and innovation pilot program, and for other purposes.

S. 3149

At the request of Mr. MERKLEY, the name of the Senator from Virginia (Mr. KAINE) was added as a cosponsor of S. 3149, a bill to direct the Secretary of Health and Human Services to establish within the Office of the Director of the Centers for Disease Control and Prevention the Office of Rural Health, and for other purposes.

S. 3164

At the request of Mr. CARDIN, the name of the Senator from New Mexico (Mr. HEINRICH) was added as a cosponsor of S. 3164, a bill to require non-Federal prison, correctional, and detention facilities holding Federal prisoners or detainees under a contract with the Federal Government to make the same information available to the public that Federal prisons and correctional facilities are required to make available.

S. 3197

At the request of Ms. KLOBUCHAR, the names of the Senator from Connecticut (Mr. BLUMENTHAL) and the Senator from Texas (Mr. CRUZ) were added as cosponsors of S. 3197, a bill to promote competition and economic opportunity in digital markets by establishing that certain acquisitions by dominant online platforms are unlawful.

S. 3217

At the request of Mr. MENENDEZ, the name of the Senator from Louisiana (Mr. CASSIDY) was added as a cosponsor of S. 3217, a bill to amend the Internal Revenue Code of 1986 to provide special rules for purposes of determining if financial guaranty insurance companies are qualifying insurance corporations under the passive foreign investment company rules.

S. 3220

At the request of Mr. MENENDEZ, the name of the Senator from Connecticut (Mr. BLUMENTHAL) was added as a cosponsor of S. 3220, a bill to amend the Animal Welfare Act to restrict the use of exotic and wild animals in traveling performances.

S. 3229

At the request of Mrs. FISCHER, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of S. 3229, a bill to amend the Agricultural Marketing Act of 1946 to establish a cattle contract library, and for other purposes.

AMENDMENT NO. 3867

At the request of Mr. REED, the name of the Senator from Oklahoma (Mr. INHOFE) was added as a cosponsor of amendment No. 3867 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3887

At the request of Mr. DURBIN, the name of the Senator from Connecticut (Mr. BLUMENTHAL) was added as a cosponsor of amendment No. 3887 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3893

At the request of Mr. MORAN, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of amendment No. 3893 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3904

At the request of Mr. WARNOCK, the name of the Senator from Nevada (Ms. ROSEN) was added as a cosponsor of amendment No. 3904 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3914

At the request of Mr. HOEVEN, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 3914 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3948

At the request of Mr. PORTMAN, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 3948 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3959

At the request of Mr. BOOZMAN, the name of the Senator from Nevada (Ms. ROSEN) was added as a cosponsor of amendment No. 3959 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 3993

At the request of Ms. ERNST, the name of the Senator from South Carolina (Mr. SCOTT) was added as a cosponsor of amendment No. 3993 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4023

At the request of Mrs. SHAHEEN, the name of the Senator from New York (Mrs. GILLIBRAND) was added as a cosponsor of amendment No. 4023 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4075

At the request of Mr. HAWLEY, the name of the Senator from South Carolina (Mr. SCOTT) was added as a cosponsor of amendment No. 4075 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4105

At the request of Mr. LANKFORD, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 4105 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4119

At the request of Mr. WICKER, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of amendment No. 4119 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4161

At the request of Mr. WYDEN, the name of the Senator from Vermont (Mr. LEAHY) was added as a cosponsor of amendment No. 4161 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4177

At the request of Mr. MENENDEZ, the name of the Senator from Michigan (Mr. PETERS) was added as a cosponsor of amendment No. 4177 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4208

At the request of Mr. PADILLA, the name of the Senator from Nevada (Ms. ROSEN) was added as a cosponsor of amendment No. 4208 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4214

At the request of Mr. PADILLA, the names of the Senator from Nevada (Ms. ROSEN) and the Senator from Montana (Mr. DAINES) were added as cosponsors of amendment No. 4214 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4216

At the request of Mr. MARKEY, the names of the Senator from Massachusetts (Ms. WARREN) and the Senator from Oregon (Mr. MERKLEY) were added as cosponsors of amendment No. 4216 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4252

At the request of Mr. PADILLA, the names of the Senator from North Carolina (Mr. BURR), the Senator from North Carolina (Mr. TILLIS), the Senator from New York (Mrs. GILLIBRAND) and the Senator from Maine (Ms. COLLINS) were added as cosponsors of amendment No. 4252 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4255

At the request of Ms. HASSAN, the name of the Senator from Texas (Mr. CORNYN) was added as a cosponsor of amendment No. 4255 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4260

At the request of Mr. LUJÁN, the names of the Senator from New Jersey (Mr. BOOKER) and the Senator from Oregon (Mr. WYDEN) were added as cosponsors of amendment No. 4260 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4269

At the request of Mr. WICKER, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of amendment No. 4269 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4283

At the request of Mr. MENENDEZ, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of amendment No. 4283 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4284

At the request of Mr. SASSE, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 4284 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4333

At the request of Mr. RUBIO, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 4333 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4402

At the request of Mr. SULLIVAN, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of amendment No. 4402 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4405

At the request of Mr. PETERS, the name of the Senator from Ohio (Mr. PORTMAN) was added as a cosponsor of amendment No. 4405 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4422

At the request of Mr. ROUNDS, the name of the Senator from South Carolina (Mr. GRAHAM) was added as a cosponsor of amendment No. 4422 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4425

At the request of Mr. REED, the names of the Senator from Nevada (Ms.

ROSEN) and the Senator from Georgia (Mr. WARNOCK) were added as cosponsors of amendment No. 4425 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4476

At the request of Mr. ROMNEY, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 4476 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4533

At the request of Mr. SANDERS, the names of the Senator from Hawaii (Mr. SCHATZ) and the Senator from Oregon (Mr. MERKLEY) were added as cosponsors of amendment No. 4533 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4540

At the request of Mr. PORTMAN, the name of the Senator from New Hampshire (Mrs. SHAHEEN) was added as a cosponsor of amendment No. 4540 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4566

At the request of Mr. BENNET, the name of the Senator from Colorado (Mr. HICKENLOOPER) was added as a cosponsor of amendment No. 4566 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4572

At the request of Mr. CORNYN, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of amendment No. 4572 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4578

At the request of Ms. ERNST, the names of the Senator from Georgia (Mr. OSSOFF) and the Senator from Idaho (Mr. CRAPO) were added as cosponsors of amendment No. 4578 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4581

At the request of Mrs. GILLIBRAND, the name of the Senator from Nevada (Ms. ROSEN) was added as a cosponsor of amendment No. 4581 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4600

At the request of Mr. LUJÁN, the name of the Senator from New Mexico (Mr. HEINRICH) was added as a cosponsor of amendment No. 4600 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4629

At the request of Ms. DUCKWORTH, the names of the Senator from Nevada (Ms. ROSEN) and the Senator from Hawaii (Ms. HIRONO) were added as cosponsors of amendment No. 4629 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4638

At the request of Mr. RISCH, the name of the Senator from Maryland (Mr. CARDIN) was added as a cosponsor of amendment No. 4638 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4649

At the request of Mr. WICKER, the name of the Senator from South Carolina (Mr. SCOTT) was added as a cosponsor of amendment No. 4649 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4654

At the request of Mr. SANDERS, the name of the Senator from New Jersey (Mr. BOOKER) was added as a cosponsor of amendment No. 4654 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4666

At the request of Mr. SULLIVAN, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of amendment No. 4666 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4671

At the request of Mr. TOOMEY, the name of the Senator from Montana (Mr. DAINES) was added as a cosponsor of amendment No. 4671 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4686

At the request of Mr. CORNYN, the name of the Senator from Alabama (Mr. TUBERVILLE) was added as a cosponsor of amendment No. 4686 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4713

At the request of Mr. PADILLA, the names of the Senator from Massachusetts (Mr. MARKEY) and the Senator from Michigan (Mr. PETERS) were added as cosponsors of amendment No. 4713 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4719

At the request of Mr. BROWN, the name of the Senator from New York (Mrs. GILLIBRAND) was added as a cosponsor of amendment No. 4719 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year

2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4722

At the request of Mr. SANDERS, the names of the Senator from Massachusetts (Ms. WARREN) and the Senator from Wisconsin (Ms. BALDWIN) were added as cosponsors of amendment No. 4722 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

AMENDMENT NO. 4733

At the request of Mr. RUBIO, the name of the Senator from Colorado (Mr. HICKENLOOPER) was added as a cosponsor of amendment No. 4733 intended to be proposed to H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Ms. COLLINS (for herself and Mr. DURBIN):

S. 3233. A bill to help increase the development, distribution, and use of clean cookstoves and fuels to improve health, protect the climate and environment, empower women, create jobs, and help consumers save time and money; to the Committee on Foreign Relations.

Ms. COLLINS. Mr. President, I rise today to introduce the Clean Cooking Support Act. I am pleased to be joined in this effort by my friend and colleague, Senator DURBIN. Our bill aims to address a serious global public health and environmental issue where leadership by the United States can make a real difference.

Today, close to 3 billion people, or one-third of the global population, rely on ''dirty cooking,'' such as open fires or inefficient, polluting, and unsafe cookstoves that use agricultural waste, coal, dung, wood, charcoal, or other solid fuels, to cook their meals. The majority of people using these types of cookstoves and fuels are in developing countries in Asia, Africa, and Latin America.

Exposure to smoke from these traditional cooking methods and open fires, referred to as ''household air pollution,'' causes chronic and acute diseases such as lung cancer, heart disease, and stroke. Alarmingly, the household air pollution caused by traditional cookstoves and open tires causes 4 million premature deaths annually, including 400,000 children younger than 5 years of age, most of whom live in sub-Saharan Africa. Women and girls are disproportionately affected, as they spend hours cooking, inhaling toxic smoke, and collecting fuels.

These cookstoves also create serious environmental problems. Household air pollution does not remain in the home; it contributes to more than 10 percent of global ambient air pollution. According to the EPA, greenhouse gas emissions from nonrenewable wood fuels for cooking amount to 2 percent of the global CO2 emissions, on par with the global CO2 emissions from the aviation or shipping industries. In 2019, more than 600,000 deaths were attributed to ambient air pollution stemming from the household combustion of solid fuels.

These cookstoves should be replaced with modern alternatives to reverse these alarming health and environmental trends. Since 2010, the Clean Cooking Alliance, an innovative public-private partnership hosted by the United Nations Foundation, has supported the adoption of clean cooking worldwide, with the goal of achieving universal access to clean cooking by 2030. Recognizing the serious health and environmental issues posed by traditional cookstoves, the Alliance aims to save lives, improve livelihoods, empower women, and combat pollution by creating a thriving global market for clean and efficient household cooking solutions. In April, President Biden announced that the U.S. is resuming and strengthening its commitment to the Clean Cooking Alliance, and during a recent presentation at the 2021 United Nations Climate Change Conference that covered clean cooking and household energy, EPA Administrator Michael Regan reaffirmed this undertaking as well.

Our legislation reinforces our country's policy on promoting clean cookstoves and seeks to take a whole-of-government approach to address household air pollution. Specifically, the Clean Cooking Support Act would create an interagency working group, with representatives from at least six different Federal agencies, committed to increasing access to clean cooking fuels and technologies worldwide. Our legislation explicitly spells out the role of each Federal agency in the advancement of clean cooking as well. The Department of Energy, for instance, is tasked with research and development to spur the production of low-cost, low-emission, and high-efficiency cookstoves, while the Department of State is directed to engage in diplomatic activities across the globe to support the clean cooking and fuels sector. Finally, our bill would authorize funding for the U.S. Government to continue such activities through 2027, to ensure that these important efforts to prevent unnecessary illness and reduce pollution around the globe continue.

Our legislation would directly benefit some of the world's poorest people, including the women and girls who are disproportionately affected, and reduce harmful pollution that affects us all. I urge my colleagues to join me and Senator DURBIN in supporting the Clean Cooking Support Act.

By Mr. DURBIN (for himself, Mr. WHITEHOUSE, Ms. WARREN, Mr. BROWN, Mr. BLUMENTHAL, Ms. HIRONO, Mr. MARKEY, and Mr. REED):

S. 3251. A bill to provide that chapter 1 of title 9 of the United States Code, relating to the enforcement of arbitration agreements, shall not apply to enrollment agreements made between students and certain institutions of higher education, and to prohibit limitations on the ability of students to pursue claims against certain institutions of higher education; to the Committee on Health, Education, Labor, and Pensions.

Mr. DURBIN. Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 3251

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Court Legal Access and Student Support Act of 2021'' or the ''CLASS Act of 2021''.

SEC. 2. INAPPLICABILITY OF CHAPTER 1 OF TITLE 9, UNITED STATES CODE, TO ENROLLMENT AGREEMENTS MADE BETWEEN STUDENTS AND CERTAIN INSTITUTIONS OF HIGHER EDUCATION.

(a) IN GENERAL.—Chapter 1 of title 9 of the United States Code (relating to the enforcement of arbitration agreements) shall not apply to an enrollment agreement made between a student and an institution of higher education.

(b) DEFINITION.—In this section, the term ''institution of higher education'' has the meaning given such term in section 102 of the Higher Education Act of 1965 (20 U.S.C. 1002).

SEC. 3. PROHIBITION ON LIMITATIONS ON ABILITY OF STUDENTS TO PURSUE CLAIMS AGAINST CERTAIN INSTITUTIONS OF HIGHER EDUCATION.

Section 487(a) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)) is amended by adding at the end the following:

''(30) The institution will not require any student to agree to, and will not enforce, any limitation or restriction (including a limitation or restriction on any available choice of applicable law, a jury trial, or venue) on the ability of a student to pursue a claim, individually or with others, against an institution in court.''.

SEC. 4. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 1 year after the date of enactment of this Act.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 456—EXPRESSING SUPPORT FOR A FREE, FAIR, AND PEACEFUL DECEMBER 4, 2021, ELECTION IN THE GAMBIA

Mr. DURBIN (for himself, Mr. RISCH, Mr. LEAHY, Mr. COONS, Mr. ROUNDS, Mr. BOOZMAN, and Mr. CARDIN) submitted the following resolution; which was referred to the Committee on Foreign Relations:

S. RES. 456

Whereas, in 1965, The Gambia became independent from Great Britain;

Whereas, in 1970, The Gambia became a republic following a public referendum, and Dawda Jawara was elected president and subsequently reelected an additional five times;

Whereas, from 1970 to 1994, The Gambia was one of Africa's longest running democracies and home to the continent's human rights body, the African Commission on Human and People's Rights;

Whereas, in 1994, President Jawara was forcibly removed from office in a coup by the Armed Forces Provisional Ruling Council (AFPRC), led by Lieutenant Yahya Jammeh;

Whereas, after two years of direct AFPRC rule that was heavily criticized by the international community, a flawed constitutional reform process occurred and The Gambia scheduled a new presidential election;

Whereas, in the lead up to the September 1996 presidential election, the Jammeh military government outlawed the country's main opposition parties, restricted media freedom, prohibited meetings between rival candidates and foreign diplomats, and used soldiers to attack opposition rallies;

Whereas Jammeh won the 1996 presidential election in a process widely regarded as flawed by international observers;

Whereas President Jammeh won reelection in 2001, 2006, and 2011 in electoral processes marred by political repression, intimidation, and technical flaws;

Whereas Jammeh's presidency saw targeted violence and widespread gross human rights violations, particularly against members of the media, including the murder of editor Deyda Hydara and the disappearance of journalist Ebrima Manneh;

Whereas President Jammeh personally ordered the kidnapping and torture of individuals he accused of ''witchcraft'' and threatened others over their sexual orientation;

Whereas thousands of Gambians fled into exile out of concern for their safety, becoming refugees in Africa at large and elsewhere;

Whereas the Jammeh government's human rights record was widely criticized by regional and international human rights groups, as well as the United States, European Union, and members of the United States Senate;

Whereas, in December 2016, opposition grand coalition candidate Adama Barrow, who campaigned on the promise of electoral and constitutional reform, won an upset election victory against President Jammeh;

Whereas, immediately after the 2016 election, Jammeh publicly accepted the defeat, but then later rejected the results and refused to depart the presidency;

Whereas Jammeh's refusal to accept defeat was widely condemned, with the African Union refusing to recognize him as president and the Economic Community of West African States deploying an international intervention force to The Gambia;

Whereas, on January 19, 2017, Barrow was sworn in as president at the Gambian Embassy in Senegal;

Whereas, on January 20, 2017, Jammeh and his family departed The Gambia, reportedly stealing more than $1,000,000,000 from state coffers, eventually to appear in Equatorial Guinea, where he remains in political exile with impunity;

Whereas President Barrow initially agreed to limit his term to a three-year transition ending on January 19, 2020, but later stated his intent to serve the full five-year constitutional term;

Whereas the Gambian Truth, Reconciliation, and Reparations Commission (TRRC) was established by an act of the Gambian Parliament to examine abuses committed during the Jammeh era and make recommendations as to whom to hold accountable;

Whereas more than 370 victims and former government officials testified at widely viewed TRRC hearings that documented widespread human rights abuses;

Whereas the TRRC's anticipated September 2021 final report submission to President Barrow was delayed; and

Whereas The Gambia will hold the first post-Jammeh era presidential election on December 4, 2021, which will include six presidential candidates: Now, therefore, be it

Resolved, That the Senate—

(1) congratulates the Gambian people on the successful 2016 presidential election;

(2) supports the courageous and necessary work of the Truth, Reconciliation, and Reparations Commission to bring accountability, healing, and reconciliation to the nation;

(3) calls on all parties and presidential candidates to participate in a free, fair, credible, and peaceful December 4, 2021, presidential election in The Gambia; and

(4) expresses the support of the American people in The Gambia's continued and noteworthy democratic path forward.

SENATE RESOLUTION 457—EXPRESSING SUPPORT FOR THE DESIGNATION OF NOVEMBER 9, 2021, AS ''NATIONAL MICROTIA AND ATRESIA AWARENESS DAY''

Ms. WARREN (for herself, Mrs. CAPITO, and Mr. MARKEY) submitted the following resolution; which was referred to the Committee on Health, Education, Labor, and Pensions:

S. RES. 457

Whereas microtia is a congenital anomaly, affecting the outer ear, where the ear does not fully develop during the first trimester of pregnancy;

Whereas microtia is often accompanied by aural atresia, which is the absence or closure of the external auditory ear canal resulting in hearing loss;

Whereas an estimated 750,000 people worldwide have microtia;

Whereas microtia is diagnosed at birth, affecting 1 ear or both ears, but there is no understanding as to why microtia occurs;

Whereas aural atresia is usually diagnosed at birth, affecting 1 ear or both ears, but in some cases may not be recognized until later in life;

Whereas doctors and nurses may be well versed in the conditions and quickly educate and prepare parents;

Whereas, in certain settings, the conditions are rare enough that misinformation or lack of information quickly evaporates any remaining sense of celebration that accompanies a birth; and

Whereas living with facial challenges such as craniofacial microsomia and hearing loss, as well as the longing for social acceptance, are some of the daily concerns for individuals who are born with microtia or aural atresia: Now, therefore, be it

Resolved, That the Senate—

(1) expresses support for the designation of November 9, 2021, as ''National Microtia and Atresia Awareness Day'';

(2) encourages each person of the United States—

(A) to celebrate the community that is made up of not only children and adults with microtia or aural atresia, but families, teachers, advocates, and medical professionals from around the world who foster awareness and assistance; and

(B) to help promote public awareness of microtia, aural atresia, and the hope that future generations of families will leave the hospital equipped with more answers than questions, along with their dream for their child intact;

(3) supports efforts to remove unnecessary barriers and replace them with resources and tools that aim to eliminate bullying and clear the way for an even more successful future for those with microtia or atresia;

(4) encourages Federal, State, and local policymakers to work together—

(A) to raise awareness about microtia or atresia;

(B) to improve proper diagnosis of microtia or atresia; and

(C) to support advancements in technology that improve the lives of those with microtia and aural atresia; and

(5) encourages the President to issue a proclamation calling upon the people of the United States to observe the day with appropriate awareness and educational activities.

SENATE RESOLUTION 458—RECOGNIZING THE 75TH ANNIVERSARY OF THE ESTABLISHMENT OF THE UNITED NATIONS CHILDREN'S FUND

Mr. COONS submitted the following resolution; which was referred to the Committee on Foreign Relations:

S. RES. 458

Whereas, for 75 years, the United Nations Children's Fund (commonly known as ''UNICEF'') has worked tirelessly to support the rights and well-being of every child, in partnership with the United States;

Whereas UNICEF was established in December 1946 to provide relief for children and adolescents in war-ravished countries and for child health purposes generally and to provide, without discrimination, assistance to vulnerable children around the world;

Whereas, in 1965, the Nobel Prize was awarded to UNICEF for the ''promotion of brotherhood among nations'';

Whereas UNICEF has been and remains a formidable and stalwart advocate for children around the world;

Whereas UNICEF operates in more than 190 countries and territories to save the lives, to defend the rights, and fulfill the potential of children from early childhood through adolescence;

Whereas UNICEF partners with United States service organizations, including with Rotary International to eradicate polio, Kiwanis International to fight maternal and neonatal tetanus and iodine deficiency disorders, the American Red Cross to decrease the incidence of childhood measles, Lions Club International to promote and support education initiatives globally, Special Olympics International to protect and uphold the

rights of children with disabilities, and many other organizations;

Whereas, since 1990, continuing efforts by UNICEF in partnership with the United States and other countries have helped slash child mortality rates by more than half;

Whereas UNICEF provides critical water, sanitation, and hygiene services and supplies for millions of people in 153 countries;

Whereas UNICEF trains social service workers to deliver essential services and to provide community-based mental health and psychosocial interventions that reach children, adolescents, parents, and caregivers in 117 countries;

Whereas UNICEF helps provide education to millions of children and works to ensure that every child has access to education and the opportunity to develop the skills needed for life and work;

Whereas UNICEF plays a key role in the global response by the United Nations to the COVID–19 pandemic and in the global vaccine distribution plan;

Whereas, beyond the COVID–19 pandemic, UNICEF responds to new and ongoing humanitarian situations in 152 countries;

Whereas UNICEF remains a trusted and reliable source for the secure delivery of vaccines and medicines around the world, particularly for vulnerable populations;

Whereas UNICEF provides personal protective equipment and facilitates training on infection prevention and control for millions of health workers; and

Whereas UNICEF, through its work on the front lines of the COVID–19 pandemic, seeks not only to facilitate recovery from the COVID–19 crisis, but also to reimagine the future for every child by implementing solutions to respond effectively to the COVID–19 pandemic and strengthening systems to better respond to future crises: Now, therefore, be it

Resolved, That the Senate—

(1) recognizes the 75th anniversary of the establishment of the United Nations Children's Fund (commonly known as ''UNICEF'');

(2) applauds UNICEF for the critical role it plays in protecting the rights and lives of vulnerable children around the world, including the global fight against COVID–19;

(3) recommits to the United States partnership with and support for UNICEF; and

(4) pledges to work with UNICEF to reimagine the future for every child as the world recovers and rebuilds from the COVID–19 pandemic.

AMENDMENTS SUBMITTED AND PROPOSED

SA 4783. Mr. HAGERTY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table.

SA 4784. Mr. KING (for himself, Mr. ROUNDS, Mr. SASSE, Ms. ROSEN, Ms. HASSAN, and Mr. OSSOFF) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4785. Mr. OSSOFF (for himself, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4786. Mr. MENENDEZ (for himself, Mr. SCHUMER, Mr. BOOKER, Mrs. GILLIBRAND, Mr. BLUMENTHAL, and Mr. MURPHY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4787. Mrs. SHAHEEN (for herself and Ms. COLLINS) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4788. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4789. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4790. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4791. Mr. MORAN (for himself and Ms. ROSEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4792. Mrs. MURRAY (for herself and Mr. MANCHIN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4793. Mr. LEE (for himself and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4794. Mr. RISCH (for himself, Mr. PORTMAN, Mr. CRUZ, Mr. BARRASSO, Mr. JOHNSON, Mr. COTTON, and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4795. Mr. SHELBY (for himself, Mr. INHOFE, Mr. WICKER, Mr. BLUNT, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. COTTON, Mr. BOOZMAN, Ms. COLLINS, Mr. KENNEDY, Ms. MURKOWSKI, Mr. CRAMER, Mr. TILLIS, and Mr. HOEVEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4796. Mr. PAUL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4797. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4798. Mr. CASSIDY (for himself, Mr. WHITEHOUSE, and Ms. WARREN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4799. Mr. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, Ms. COLLINS, Mr. KING, Mr. RUBIO, Mr. RISCH, Ms. ROSEN, Mr. CORNYN, and Mr. BURR) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4800. Ms. KLOBUCHAR (for herself and Mr. BLUNT) submitted an amendment intended to be proposed by her to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4801. Mr. KENNEDY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4802. Mr. OSSOFF (for himself, Mr. TILLIS, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, Mr. SCOTT of South Carolina, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4803. Ms. DUCKWORTH (for herself, Mr. KELLY, Ms. HIRONO, Ms. ROSEN, Mr. BENNET, Mr. HEINRICH, Mr. MORAN, Mr. YOUNG, Mrs. FEINSTEIN, Mrs. GILLIBRAND, Mr. KING, Mrs. SHAHEEN, Ms. KLOBUCHAR, Mr. DURBIN, Mr. PETERS, and Mr. BLUMENTHAL) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4804. Mr. YOUNG submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4805. Ms. CORTEZ MASTO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4806. Ms. SMITH (for herself and Mr. YOUNG) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4807. Ms. SMITH (for herself, Mr. CASSIDY, and Ms. WARREN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4808. Mrs. FEINSTEIN (for herself, Ms. ERNST, Mr. DURBIN, Ms. COLLINS, Ms. HIRONO, Ms. ROSEN, Mr. PETERS, Mr. CORNYN, and Ms. DUCKWORTH) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4809. Mr. WARNER submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4810. Mrs. GILLIBRAND (for herself, Mr. RUBIO, Mr. HEINRICH, Mr. BLUNT, and Mr. GRAHAM) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4811. Mr. TUBERVILLE (for himself and Mr. BRAUN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4812. Mr. TUBERVILLE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED

and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4813. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4814. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4815. Mr. SANDERS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4816. Mr. COONS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4817. Ms. SINEMA submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4818. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4819. Mr. SULLIVAN (for himself and Mr. WHITEHOUSE) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4820. Mr. COTTON (for himself, Mr. MANCHIN, Mr. TUBERVILLE, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4821. Mr. BROWN (for himself and Mr. WARNER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4822. Mrs. BLACKBURN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4823. Mr. MARKEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4824. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4825. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4826. Mr. TOOMEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4827. Mr. ROUNDS (for himself and Mr. VAN HOLLEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4828. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4829. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4830. Mr. MANCHIN (for himself, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. ROMNEY, Mr. COTTON, Mrs. BLACKBURN, and Mr. TESTER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4831. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4832. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

SA 4833. Mr. BARRASSO (for himself, Mr. CRUZ, and Mr. JOHNSON) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 4783. Mr. HAGERTY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title XII, add the following:

SEC. 1283. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES AGAINST ISIS AND ASSOCIATED FORCES IN IRAQ.

The President is authorized to use the Armed Forces of the United States as the President determines to be necessary and appropriate in order to defend the national security of the United States against the threat posed by the Islamic State of Iraq and Syria (ISIS) and associated forces in Iraq.

SEC. 1284. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES TO PROTECT UNITED STATES DIPLOMATS AND UNITED STATES DIPLOMATIC FACILITIES IN IRAQ AGAINST TERRORIST ATTACKS.

The President is authorized to use the Armed Forces of the United States as the President determines to be necessary and appropriate in order to protect United States diplomats and United States diplomatic facilities in Iraq against terrorist attacks.

SEC. 1285. RULE OF CONSTRUCTION REGARDING THE CONSTITUTIONAL POWERS OF THE PRESIDENT AS COMMANDER-IN-CHIEF.

Nothing in this Act shall be construed to infringe upon the constitutional powers of the President as Commander-in-Chief under Article II of the Constitution of the United States.

SA 4784. Mr. KING (for himself, Mr. ROUNDS, Mr. SASSE, Ms. ROSEN, Ms. HASSAN, and Mr. OSSOFF) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—DEFENSE OF UNITED STATES INFRASTRUCTURE

SEC. 5001. SHORT TITLE.

This division may be cited as the ''Defense of United States Infrastructure Act of 2021''.

SEC. 5002. DEFINITIONS.

In this division:

(1) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(2) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given such term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(3) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

(4) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

TITLE LI—INVESTING IN CYBER RESILIENCY IN CRITICAL INFRASTRUCTURE

SEC. 5101. NATIONAL RISK MANAGEMENT CYCLE.

(a) AMENDMENTS.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2202(c) (6 U.S.C. 652(c))—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in the first paragraph designated as paragraph (12), relating to the Cybersecurity State Coordinator—

(i) by striking ''section 2215'' and inserting ''section 2217''; and

(ii) by striking ''and'' at the end; and

(C) by redesignating the second and third paragraphs designated as paragraph (12) as paragraphs (13) and (14), respectively;

(2) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(3) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(4) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(5) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217;

(6) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216; and

(7) by adding at the end the following:

''SEC. 2220A. NATIONAL RISK MANAGEMENT CYCLE.

''(a) NATIONAL CRITICAL FUNCTIONS DEFINED.—In this section, the term 'national critical functions' means the functions of

government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

''(b) NATIONAL RISK MANAGEMENT CYCLE.—

''(1) RISK IDENTIFICATION AND ASSESSMENT.—

''(A) IN GENERAL.—The Secretary, acting through the Director, shall establish a recurring process by which to identify, assess, and prioritize risks to critical infrastructure, considering both cyber and physical threats, the associated likelihoods, vulnerabilities, and consequences, and the resources necessary to address them.

''(B) CONSULTATION.—In establishing the process required under subparagraph (A), the Secretary shall consult with, and request and collect information to support analysis from, Sector Risk Management Agencies, critical infrastructure owners and operators, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the National Cyber Director.

''(C) PUBLICATION.—Not later than 180 days after the date of enactment of this section, the Secretary shall publish in the Federal Register procedures for the process established under subparagraph (A), subject to any redactions the Secretary determines are necessary to protect classified or other sensitive information.

''(D) REPORT.—The Secretary shall submit to the President, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a report on the risks identified by the process established under subparagraph (A)—

''(i) not later than 1 year after the date of enactment of this section; and

''(ii) not later than 1 year after the date on which the Secretary submits a periodic evaluation described in section 9002(b)(2) of title XC of division H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283).

''(2) NATIONAL CRITICAL INFRASTRUCTURE RESILIENCE STRATEGY.—

''(A) IN GENERAL.—Not later than 1 year after the date on which the Secretary delivers each report required under paragraph (1), the President shall deliver to majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a national critical infrastructure resilience strategy designed to address the risks identified by the Secretary.

''(B) ELEMENTS.—Each strategy delivered under subparagraph (A) shall—

''(i) identify, assess, and prioritize areas of risk to critical infrastructure that would compromise or disrupt national critical functions impacting national security, economic security, or public health and safety;

''(ii) assess the implementation of the previous national critical infrastructure resilience strategy, as applicable;

''(iii) identify and outline current and proposed national-level actions, programs, and efforts to be taken to address the risks identified;

''(iv) identify the Federal departments or agencies responsible for leading each national-level action, program, or effort and the relevant critical infrastructure sectors for each; and

''(v) request any additional authorities necessary to successfully execute the strategy.

''(C) FORM.—Each strategy delivered under subparagraph (A) shall be unclassified, but may contain a classified annex.

''(3) CONGRESSIONAL BRIEFING.—Not later than 1 year after the date on which the President delivers a strategy under this section, and every year thereafter, the Secretary, in coordination with Sector Risk Management Agencies, shall brief the appropriate committees of Congress on—

''(A) the national risk management cycle activities undertaken pursuant to the strategy; and

''(B) the amounts and timeline for funding that the Secretary has determined would be necessary to address risks and successfully execute the full range of activities proposed by the strategy.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity education and training programs.
''Sec. 2220A. National risk management cycle.''.

(2) ADDITIONAL TECHNICAL AMENDMENT.—

(A) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

(B) EFFECTIVE DATE.—The amendment made by subparagraph (A) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

TITLE LII—IMPROVING THE ABILITY OF THE FEDERAL GOVERNMENT TO ASSIST IN ENHANCING CRITICAL INFRASTRUCTURE CYBER RESILIENCE

SEC. 5201. INSTITUTE A 5-YEAR TERM FOR THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) IN GENERAL.—Subsection (b)(1) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652), is amended by inserting ''The term of office of an individual serving as Director shall be 5 years.'' after ''who shall report to the Secretary.''.

(b) TRANSITION RULES.—The amendment made by subsection (a) shall take effect on the first appointment of an individual to the position of Director of the Cybersecurity and Infrastructure Security Agency, by and with the advice and consent of the Senate, that is made on or after the date of enactment of this Act.

SEC. 5202. CYBER THREAT INFORMATION COLLABORATION ENVIRONMENT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE INFORMATION.—The term ''critical infrastructure information'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(2) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(3) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(4) ENVIRONMENT.—The term ''environment'' means the information collaboration environment established under subsection (b).

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''information sharing and analysis organization'' has the meaning given such term in section 2222 of the Homeland Security Act of 2002 (6 U.S.C. 671).

(6) NON-FEDERAL ENTITY.—The term ''non-Federal entity'' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(b) PROGRAM.—The Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall carry out a program under which the Secretary shall develop an information collaboration environment consisting of a digital environment containing technical tools for information analytics and a portal through which relevant parties may submit and automate information inputs and access the environment in order to enable interoperable data flow that enable Federal and non-Federal entities to identify, mitigate, and prevent malicious cyber activity to—

(1) provide limited access to appropriate and operationally relevant data from unclassified and classified intelligence about cybersecurity risks and cybersecurity threats, as well as malware forensics and data from network sensor programs, on a platform that enables query and analysis;

(2) enable cross-correlation of data on cybersecurity risks and cybersecurity threats at the speed and scale necessary for rapid detection and identification;

(3) facilitate a comprehensive understanding of cybersecurity risks and cybersecurity threats; and

(4) facilitate collaborative analysis between the Federal Government and public and private sector critical infrastructure entities and information and analysis organizations.

(c) IMPLEMENTATION OF INFORMATION COLLABORATION ENVIRONMENT.—

(1) EVALUATION.—Not later than 180 days after the date of enactment of this Act, the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall—

(A) identify, inventory, and evaluate existing Federal sources of classified and unclassified information on cybersecurity threats;

(B) evaluate current programs, applications, or platforms intended to detect, identify, analyze, and monitor cybersecurity risks and cybersecurity threats;

(C) consult with public and private sector critical infrastructure entities to identify public and private critical infrastructure cyber threat capabilities, needs, and gaps; and

(D) identify existing tools, capabilities, and systems that may be adapted to achieve the purposes of the environment in order to maximize return on investment and minimize cost.

(2) IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 1 year after completing the evaluation required under paragraph (1)(B), the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, and in consultation with the Secretary of Defense, the Director of National Intelligence, and

the Attorney General, shall begin implementation of the environment to enable participants in the environment to develop and run analytic tools referred to in subsection (b) on specified data sets for the purpose of identifying, mitigating, and preventing malicious cyber activity that is a threat to public and private critical infrastructure.

(B) REQUIREMENTS.—The environment and the use of analytic tools referred to in subsection (b) shall—

(i) operate in a manner consistent with relevant privacy, civil rights, and civil liberties policies and protections, including such policies and protections established pursuant to section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485);

(ii) account for appropriate data interoperability requirements;

(iii) enable integration of current applications, platforms, data, and information, including classified information, in a manner that supports the voluntary integration of unclassified and classified information on cybersecurity risks and cybersecurity threats;

(iv) incorporate tools to manage access to classified and unclassified data, as appropriate;

(v) ensure accessibility by entities the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, determines appropriate;

(vi) allow for access by critical infrastructure stakeholders and other private sector partners, at the discretion of the Secretary, in consultation with the Secretary of Defense, the Director of National Intelligence, and the Attorney General;

(vii) deploy analytic tools across classification levels to leverage all relevant data sets, as appropriate;

(viii) identify tools and analytical software that can be applied and shared to manipulate, transform, and display data and other identified needs; and

(ix) anticipate the integration of new technologies and data streams, including data from government-sponsored network sensors or network-monitoring programs deployed in support of non-Federal entities.

(3) ANNUAL REPORT REQUIREMENT ON THE IMPLEMENTATION, EXECUTION, AND EFFECTIVENESS OF THE PROGRAM.—Not later than 1 year after the date of enactment of this Act, and every year thereafter until the date that is 1 year after the program under this section terminates under subsection (g), the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives a report that details—

(A) Federal Government participation in the environment, including the Federal entities participating in the environment and the volume of information shared by Federal entities into the environment;

(B) non-Federal entities' participation in the environment, including the non-Federal entities participating in the environment and the volume of information shared by non-Federal entities into the environment;

(C) the impact of the environment on positive security outcomes for the Federal Government and non-Federal entities;

(D) barriers identified to fully realizing the benefit of the environment both for the Federal Government and non-Federal entities;

(E) additional authorities or resources necessary to successfully execute the environment; and

(F) identified shortcomings or risks to data security and privacy, and the steps necessary to improve the mitigation of the shortcomings or risks.

(d) CYBER THREAT DATA INTEROPERABILITY REQUIREMENTS.—

(1) ESTABLISHMENT.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall identify or establish data interoperability requirements for non-Federal entities to participate in the environment.

(2) DATA STREAMS.—The Secretary, in coordination with the heads of appropriate departments and agencies, shall identify, designate, and periodically update programs that shall participate in or be interoperable with the environment, in a manner consistent with data security standards under Federal law, which may include—

(A) network-monitoring and intrusion detection programs;

(B) cyber threat indicator sharing programs;

(C) certain government-sponsored network sensors or network-monitoring programs;

(D) incident response and cybersecurity technical assistance programs; or

(E) malware forensics and reverse-engineering programs.

(3) DATA GOVERNANCE.—The Secretary, in coordination with the Secretary of Defense, the Director of National Intelligence, and the Attorney General, shall establish procedures and data governance structures, as necessary, to protect data shared in the environment, comply with Federal regulations and statutes, and respect existing consent agreements with private sector critical infrastructure entities that apply to critical infrastructure information.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall change existing ownership or protection of, or policies and processes for access to, agency data.

(e) NATIONAL SECURITY SYSTEMS.—Nothing in this section shall apply to national security systems, as defined in section 3552 of title 44, United States Code, or to cybersecurity threat intelligence related to such systems, without the consent of the relevant element of the intelligence community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(f) PROTECTION OF INTELLIGENCE SOURCES AND METHODS.—The Director of National Intelligence shall ensure that any information sharing conducted under this section shall protect intelligence sources and methods from unauthorized disclosure in accordance with section 102A(i) of the National Security Act (50 U.S.C. 3024(i)).

(g) DURATION.—The program under this section shall terminate on the date that is 5 years after the date of enactment of this Act.

TITLE LIII—ENABLING THE NATIONAL CYBER DIRECTOR

SEC. 5401. ESTABLISHMENT OF HIRING AUTHORITIES FOR THE OFFICE OF THE NATIONAL CYBER DIRECTOR.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the National Cyber Director.

(2) EXCEPTED SERVICE.—The term ''excepted service'' has the meaning given such term in section 2103 of title 5, United States Code.

(3) OFFICE.—The term ''Office'' means the Office of the National Cyber Director.

(4) QUALIFIED POSITION.—The term ''qualified position'' means a position identified by the Director under subsection (b)(1)(A), in which the individual occupying such position performs, manages, or supervises functions that execute the responsibilities of the Office.

(b) HIRING PLAN.—The Director shall, for purposes of carrying out the functions of the Office—

(1) craft an implementation plan for positions in the excepted service in the Office, which shall propose—

(A) qualified positions in the Office, as the Director determines necessary to carry out the responsibilities of the Office; and

(B) subject to the requirements of paragraph (2), rates of compensation for an individual serving in a qualified position;

(2) propose rates of basic pay for qualified positions, which shall—

(A) be determined in relation to the rates of pay provided for employees in comparable positions in the Office, in which the employee occupying the comparable position performs, manages, or supervises functions that execute the mission of the Office; and

(B) subject to the same limitations on maximum rates of pay and consistent with section 5341 of title 5, United States Code, adopt such provisions of that title to provide for prevailing rate systems of basic pay and apply those provisions to qualified positions for employees in or under which the Office may employ individuals described by section 5342(a)(2)(A) of such title; and

(3) craft proposals to provide—

(A) employees in qualified positions compensation (in addition to basic pay), including benefits, incentives, and allowances, consistent with, and not in excess of the level authorized for, comparable positions authorized by title 5, United States Code; and

(B) employees in a qualified position for which the Director proposes a rate of basic pay under paragraph (2) an allowance under section 5941 of title 5, United States Code, on the same basis and to the same extent as if the employee was an employee covered by such section, including eligibility conditions, allowance rates, and all other terms and conditions in law or regulation.

SA 4785. Mr. OSSOFF (for himself, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. DR. DAVID SATCHER CYBERSECURITY EDUCATION GRANT PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Cybersecurity Opportunity Act''.

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) ENROLLMENT OF NEEDY STUDENTS.—The term ''enrollment of needy students'' has the meaning given the term in section 312(d) of the Higher Education Act of 1965 (20 U.S.C. 1058(d)).

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(5) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution listed in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(c) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—Subject to the availability of appropriations, the Director shall carry out the Dr. David Satcher Cybersecurity Education Grant Program by—

(A) awarding grants to assist institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to establish or expand cybersecurity programs, to build and upgrade institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities, and to support such institutions on the path to producing qualified entrants in the cybersecurity workforce or becoming a National Center of Academic Excellence in Cybersecurity; and

(B) awarding grants to build capacity at institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to expand cybersecurity education opportunities, cybersecurity programs, cybersecurity research, and cybersecurity partnerships with public and private entities.

(2) RESERVATION.—The Director shall award not less than 50 percent of the amount available for grants under this section to historically Black colleges and universities and minority-serving institutions.

(3) COORDINATION.—The Director shall carry out this section in consultation with appropriate Federal agencies.

(4) SUNSET.—The Director's authority to award grants under paragraph (1) shall terminate on the date that is 5 years after the date the Director first awards a grant under paragraph (1).

(d) APPLICATIONS.—An eligible institution seeking a grant under subsection (a) shall submit an application to the Director at such time, in such manner, and containing such information as the Director may reasonably require, including a statement of how the institution will use the funds awarded through the grant to expand cybersecurity education opportunities at the eligible institution.

(e) ACTIVITIES.—An eligible institution that receives a grant under this section may use the funds awarded through such grant for increasing research, education, technical, partnership, and innovation capacity, including for—

(1) building and upgrading institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities;

(2) building and upgrading institutional capacity to provide hands-on research and training experiences for undergraduate and graduate students; and

(3) outreach and recruitment to ensure students are aware of such new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities.

(f) REPORTING REQUIREMENTS.—Not later than—

(1) 1 year after the effective date of this section, as provided in subsection (h), and annually thereafter until the Director submits the report under paragraph (2), the Director shall prepare and submit to Congress a report on the status and progress of implementation of the grant program under this section, including on the number and nature of institutions participating, the number and nature of students served by institutions receiving grants, the level of funding provided to grant recipients, the types of activities being funded by the grants program, and plans for future implementation and development; and

(2) 5 years after the effective date of this section, as provided in subsection (h), the Director shall prepare and submit to Congress a report on the status of cybersecurity education programming and capacity-building at institutions receiving grants under this section, including changes in the scale and scope of these programs, associated facilities, or in accreditation status, and on the educational and employment outcomes of students participating in cybersecurity programs that have received support under this section.

(g) PERFORMANCE METRICS.—The Director shall establish performance metrics for grants awarded under this section.

(h) EFFECTIVE DATE.—This section shall take effect 1 year after the date of enactment of this Act.

SA 4786. Mr. MENENDEZ (for himself, Mr. SCHUMER, Mr. BOOKER, Mrs. GILLIBRAND, Mr. BLUMENTHAL, and Mr. MURPHY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. APPROPRIATIONS FOR CATCH-UP PAYMENTS.

Section 404(d)(4)(C) of the Justice for United States Victims of State Sponsored Terrorism Act (34 U.S.C. 20144(d)(4)(C)) is amended by adding at the end the following:

''(iv) FUNDING.—

''(I) APPROPRIATIONS.—

''(aa) IN GENERAL.—There are authorized to be appropriated and there are appropriated to the Fund such sums as may be necessary to carry out this subparagraph, to remain available until expended.

''(bb) EMERGENCY DESIGNATION.—The amounts provided under this subclause are designated as an emergency requirement pursuant to section 4(g) of the Statutory Pay-As-You-Go Act of 2010 (2 U.S.C. 933(g)).

''(cc) DESIGNATION IN THE HOUSE AND SENATE.—This subclause is designated by the Congress as being for an emergency requirement pursuant to section 4001(a)(1) and section 4001(b) of S. Con. Res. 14 (117th Congress), the concurrent resolution on the budget for fiscal year 2022.

''(II) LIMITATION.—Amounts appropriated pursuant to subclause (I) may not be used for a purpose other than to make lump sum catch-up payments under this subparagraph.''.

SA 4787. Mrs. SHAHEEN (for herself and Ms. COLLINS) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title VII, add the following:

Subtitle D—Access to Contraception

SEC. 761. SHORT TITLE.

This subtitle may be cited as the ''Access to Contraception for Servicemembers and Dependents Act of 2021''.

SEC. 762. FINDINGS.

Congress finds the following:

(1) Women are serving in the Armed Forces at increasing rates, playing a critical role in the national security of the United States. Women comprise more than 18 percent of members of the Armed Forces, and as of fiscal year 2019, more than 390,000 women serve on active duty in the Armed Forces or in the reserve components. An estimated several thousand transgender men also serve on active duty in the Armed Forces and in the reserve components, in addition to non-binary members and those who identify with a different gender.

(2) Ninety-five percent of women serving in the Armed Forces are of reproductive age and as of 2019, more than 700,000 female spouses and dependents of members of the Armed Forces on active duty are of reproductive age.

(3) The TRICARE program covered more than 1,570,000 women of reproductive age in 2019, including spouses and dependents of members of the Armed Forces on active duty. Additionally, thousands of transgender dependents of members of the Armed Forces are covered by the TRICARE program.

(4) The right to access contraception is grounded in the principle that contraception and the ability to determine if and when to have children are inextricably tied to one's wellbeing, equality, and ability to determine the course of one's life. These protections have helped access to contraception become a driving force in improving the health and financial security of individuals and their families.

(5) Access to contraception is critical to the health of every individual capable of becoming pregnant. This subtitle is intended to apply to all individuals with the capacity for pregnancy, including cisgender women, transgender men, non-binary individuals, those who identify with a different gender, and others.

(6) Studies have shown that when cost barriers to the full range of methods of contraception are eliminated, patients are more likely to use the contraceptive method that meets their needs, and therefore use contraception correctly and more consistently, reducing the risk of unintended pregnancy.

(7) Under the TRICARE program, members of the Armed Forces on active duty have full coverage of all prescription drugs, including contraception, without cost-sharing requirements, in line with the Patient Protection and Affordable Care Act (Public Law 111–148), which requires coverage of all contraceptive methods approved by the Food and Drug Administration for women and related services and education and counseling. However, members not on active duty and dependents of members do not have similar coverage of all methods of contraception approved by the Food and Drug Administration without cost-sharing when they obtain the contraceptive outside of a military medical treatment facility.

(8) In order to fill gaps in coverage and access to preventive care critical for women's

health, the Patient Protection and Affordable Care Act (Public Law 111–148) requires all non-grandfathered individual and group health plans to cover without cost-sharing preventive services, including a set of evidence-based preventive services for women supported by the Health Resources and Services Administration of the Department of Health and Human Services. These women's preventive services include the full range of female-controlled contraceptive methods, effective family planning practices, and sterilization procedures, approved by the Food and Drug Administration. The Health Resources and Services Administration has affirmed that contraceptive care includes contraceptive counseling, initiation of contraceptive use, and follow-up care (such as management, evaluation, and changes to and removal or discontinuation of the contraceptive method).

(9) The Defense Advisory Committee on Women in the Services has recommended that all the Armed Forces, to the extent that they have not already, implement initiatives that inform members of the Armed Forces of the importance of family planning, educate them on methods of contraception, and make various methods of contraception available, based on the finding that family planning can increase the overall readiness and quality of life of all members of the Armed Forces.

(10) The military departments received more than 7,800 reports of sexual assaults involving members of the Armed Forces as victims or subjects during fiscal year 2019. Through regulations, the Department of Defense already supports a policy of ensuring that members of the Armed Forces who are sexually assaulted have access to emergency contraception, and the initiation of contraception if desired and medically appropriate.

SEC. 763. CONTRACEPTION COVERAGE PARITY UNDER THE TRICARE PROGRAM.

(a) PHARMACY BENEFITS PROGRAM.—Section 1074g(a)(6) of title 10, United States Code, is amended by adding at the end the following new subparagraph:

''(D) Notwithstanding subparagraphs (A), (B), and (C), cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any eligible covered beneficiary for any prescription contraceptive on the uniform formulary provided through a retail pharmacy described in paragraph (2)(E)(ii) or through the national mail-order pharmacy program.''.

(b) TRICARE SELECT.—Section 1075 of such title is amended—

(1) in subsection (c), by adding at the end the following new paragraph:

''(4)(A) Notwithstanding any other provision of this section, cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any beneficiary under this section for a service described in subparagraph (B) that is provided by a network provider.

''(B) A service described in this subparagraph is any method of contraception approved by the Food and Drug Administration, any contraceptive care (including with respect to insertion, removal, and follow up), any sterilization procedure, or any patient education or counseling service provided in connection with any such method, care, or procedure.''; and

(2) in subsection (f), by striking ''calculated as'' and inserting ''calculated (except as provided in subsection (c)(4)) as''.

(c) TRICARE PRIME.—Section 1075a of such title is amended by adding at the end the following new subsection:

''(d) PROHIBITION ON COST-SHARING FOR CERTAIN SERVICES.—(1) Notwithstanding subsections (a), (b), and (c), cost-sharing requirements may not be imposed and cost-sharing amounts may not be collected with respect to any beneficiary enrolled in TRICARE Prime for a service described in paragraph (2) that is provided under TRICARE Prime.

''(2) A service described in this paragraph is any method of contraception approved by the Food and Drug Administration, any contraceptive care (including with respect to insertion, removal, and follow up), any sterilization procedure, or any patient education or counseling service provided in connection with any such method, care, or procedure.''.

SEC. 764. PREGNANCY PREVENTION ASSISTANCE AT MILITARY MEDICAL TREATMENT FACILITIES FOR SEXUAL ASSAULT SURVIVORS.

(a) IN GENERAL.—Chapter 55 of title 10, United States Code, is amended by inserting after section 1074o the following new section:

''§ 1074p. Provision of pregnancy prevention assistance at military medical treatment facilities

''(a) INFORMATION AND ASSISTANCE.—The Secretary of Defense shall promptly furnish to sexual assault survivors at each military medical treatment facility the following:

''(1) Comprehensive, medically and factually accurate, and unbiased written and oral information about all methods of emergency contraception approved by the Food and Drug Administration.

''(2) Upon request by the sexual assault survivor, emergency contraception or, if applicable, a prescription for emergency contraception.

''(3) Notification of the right of the sexual assault survivor to confidentiality with respect to the information and care and services furnished under this section.

''(b) INFORMATION.—The Secretary shall ensure that information provided pursuant to subsection (a) is provided in language that—

''(1) is clear and concise;

''(2) is readily comprehensible; and

''(3) meets such conditions (including conditions regarding the provision of information in languages other than English) as the Secretary may prescribe in regulations to carry out this section.

''(c) DEFINITIONS.—In this section:

''(1) The term 'sexual assault survivor' means any individual who presents at a military medical treatment facility and—

''(A) states to personnel of the facility that the individual experienced a sexual assault;

''(B) is accompanied by another person who states that the individual experienced a sexual assault; or

''(C) whom the personnel of the facility reasonably believes to be a survivor of sexual assault.

''(2) The term 'sexual assault' means the conduct described in section 1565b(c) of this title that may result in pregnancy.''.

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of such chapter is amended by inserting after the item relating to section 1074o the following new item:

''1074p. Provision of pregnancy prevention assistance at military medical treatment facilities.''.

SEC. 765. EDUCATION ON FAMILY PLANNING FOR MEMBERS OF THE ARMED FORCES.

(a) EDUCATION PROGRAMS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary of Defense shall establish a uniform standard curriculum to be used in education programs on family planning for all members of the Armed Forces, including both men and women members.

(2) TIMING.—Education programs under paragraph (1) shall be provided to members of the Armed Forces as follows:

(A) During the first year of service of the member.

(B) At such other times as each Secretary of a military department determines appropriate with respect to members of the Armed Forces under the jurisdiction of such Secretary.

(3) SENSE OF CONGRESS.—It is the sense of Congress that the education programs under paragraph (1) should be evidence-informed and use the latest technology available to efficiently and effectively deliver information to members of the Armed Forces.

(b) ELEMENTS.—The uniform standard curriculum for education programs under subsection (a) shall include the following:

(1) Information for members of the Armed Forces on active duty to make informed decisions regarding family planning.

(2) Information about the prevention of unintended pregnancy and sexually transmitted infections, including human immunodeficiency virus (commonly known as ''HIV'').

(3) Information on—

(A) the importance of providing comprehensive family planning for members of the Armed Forces, including commanding officers; and

(B) the positive impact family planning can have on the health and readiness of the Armed Forces.

(4) Current, medically accurate information.

(5) Clear, user-friendly information on—

(A) the full range of methods of contraception approved by the Food and Drug Administration; and

(B) where members of the Armed Forces can access their chosen method of contraception.

(6) Information on all applicable laws and policies so that members of the Armed Forces are informed of their rights and obligations.

(7) Information on the rights of patients to confidentiality.

(8) Information on the unique circumstances encountered by members of the Armed Forces and the effects of such circumstances on the use of contraception.

SA 4788. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

On page 621, strike lines 14 through 24 and insert the following:

cross-strait relations;

(7) reinforcing the status of the Republic of Singapore as a Major Security Cooperation Partner of the United States and continuing to strengthen defense and security cooperation between the military forces of the Republic of Singapore and the Armed Forces of the United States, including through participation in combined exercises and training, including the use of the Foreign Military Sales Training Center at Ebbing Air National Guard Base in Fort Smith, Arkansas; and

(8) ensuring that the allies and partners referred to in paragraphs (1) through (7) contribute more than 50 percent of the total cost of mutual defense efforts in the Indo-Pacific region.

SA 4789. Mr. LEE submitted an amendment intended to be proposed to

amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

On page 578, strike lines 14 through 19 and insert the following:

(1) by striking ''fiscal year 2021'' and inserting ''fiscal year 2022''; and

(2) by striking '', as specified in the funding tables in division D of this Act''.

SA 4790. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

Strike section 1061.

SA 4791. Mr. MORAN (for himself and Ms. ROSEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle C of title VII, add the following:

SEC. 744. GRANT PROGRAM FOR INCREASED COOPERATION ON POST-TRAUMATIC STRESS DISORDER RESEARCH BETWEEN UNITED STATES AND ISRAEL.

(a) FINDINGS AND SENSE OF CONGRESS.—

(1) FINDINGS.—Congress makes the following findings:

(A) The Department of Veterans Affairs reports that between 11 and 20 percent of veterans who served in Operation Iraqi Freedom and Operation Enduring Freedom have post-traumatic stress disorder (in this paragraph referred to as ''PTSD'') in a given year. In addition, that figure amounts to about 12 percent of Gulf War veterans and up to 30 percent of Vietnam veterans.

(B) The Department of Veterans Affairs reports that among women veterans of the conflicts in Iraq and Afghanistan, almost 20 percent have been diagnosed with PTSD.

(C) It is thought that 70 percent of individuals in the United States have experienced at least one traumatic event in their lifetime, and approximately 20 percent of those individuals have struggled or continue to struggle with symptoms of PTSD.

(D) Studies show that PTSD has links to homelessness and substance abuse in the United States. The Department of Veterans Affairs estimates that approximately 11 percent of the homeless population are veterans and the Substance Abuse and Mental Health Services Administration estimates that about seven percent of veterans have a substance abuse disorder.

(E) Our ally Israel, under constant attack from terrorist groups, experiences similar issues with Israeli veterans facing symptoms of PTSD. The National Center for Traumatic Stress and Resilience at Tel Aviv University found that five to eight percent of combat soldiers experience some form of PTSD, and during wartime, that figure rises to 15 to 20 percent.

(F) Current treatment options in the United States focus on cognitive therapy, exposure therapy, or eye movement desensitization and reprocessing, but the United States must continue to look for more effective treatments. Several leading hospitals, academic institutions, and nonprofit organizations in Israel dedicate research and services to treating PTSD.

(2) SENSE OF CONGRESS.—It is the sense of Congress that the Secretary of Defense, acting through the Psychological Health and Traumatic Brain Injury Research Program, should seek to explore scientific collaboration between academic institutions and nonprofit research entities in the United States and institutions in Israel with expertise in researching, diagnosing, and treating post-traumatic stress disorder.

(b) GRANT PROGRAM.—

(1) IN GENERAL.—The Secretary of Defense, in coordination with the Secretary of Veterans Affairs and the Secretary of State, shall award grants to eligible entities to carry out collaborative research between the United States and Israel with respect to post-traumatic stress disorders.

(2) AGREEMENT.—The Secretary of Defense shall carry out the grant program under this section in accordance with the Agreement on the United States-Israel binational science foundation with exchange of letters, signed at New York September 27, 1972, and entered into force on September 27, 1972.

(c) ELIGIBLE ENTITIES.—To be eligible to receive a grant under this section, an entity shall be an academic institution or a nonprofit entity located in the United States.

(d) AWARD.—The Secretary shall award grants under this section to eligible entities that—

(1) carry out a research project that—

(A) addresses a requirement in the area of post-traumatic stress disorders that the Secretary determines appropriate to research using such grant; and

(B) is conducted by the eligible entity and an entity in Israel under a joint research agreement; and

(2) meet such other criteria that the Secretary may establish.

(e) APPLICATION.—To be eligible to receive a grant under this section, an eligible entity shall submit an application to the Secretary at such time, in such manner, and containing such commitments and information as the Secretary may require.

(f) REPORTS.—Not later than 180 days after the date on which an eligible entity completes a research project using a grant under this section, the Secretary shall submit to Congress a report that contains—

(1) a description of how the eligible entity used the grant; and

(2) an evaluation of the level of success of the research project.

(g) TERMINATION.—The authority to award grants under this section shall terminate on the date that is seven years after the date on which the first such grant is awarded.

SA 4792. Mrs. MURRAY (for herself and Mr. MANCHIN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XXXI, add the following:

Subtitle F—Toxic Exposure Safety

SEC. 3161. SHORT TITLE.

This subtitle may be cited as the ''Toxic Exposure Safety Act of 2021''.

SEC. 3162. PROVIDING INFORMATION REGARDING DEPARTMENT OF ENERGY FACILITIES.

Subtitle E of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s et seq.) is amended by inserting after section 3681 the following:

''SEC. 3681A. COMPLETION AND UPDATES OF SITE EXPOSURE MATRICES.

''(a) DEFINITION.—In this section, the term 'site exposure matrices' means an exposure assessment of a Department of Energy facility that identifies the toxic substances or processes that were used in each building or process of the facility, including the trade name (if any) of the substance.

''(b) IN GENERAL.—Not later than 180 days after the date of enactment of the Toxic Exposure Safety Act of 2021, the Secretary of Labor shall, in coordination with the Secretary of Energy, create or update site exposure matrices for each Department of Energy facility based on the records, files, and other data provided by the Secretary of Energy and such other information as is available, including information available from the former worker medical screening programs of the Department of Energy.

''(c) PERIODIC UPDATE.—Beginning 90 days after the initial creation or update described in subsection (b), and each 90 days thereafter, the Secretary shall update the site exposure matrices with all information available as of such time from the Secretary of Energy.

''(d) INFORMATION.—The Secretary of Energy shall furnish to the Secretary of Labor any information that the Secretary of Labor finds necessary or useful for the production of the site exposure matrices under this section, including records from the Department of Energy former worker medical screening program.

''(e) PUBLIC AVAILABILITY.—The Secretary of Labor shall make available to the public, on the primary website of the Department of Labor—

''(1) the site exposure matrices, as periodically updated under subsections (b) and (c);

''(2) each site profile prepared under section 3633(a);

''(3) any other database used by the Secretary of Labor to evaluate claims for compensation under this title; and

''(4) statistical data, in the aggregate and disaggregated by each Department of Energy facility, regarding—

''(A) the number of claims filed under this subtitle;

''(B) the types of illnesses claimed;

''(C) the number of claims filed for each type of illness and, for each claim, whether the claim was approved or denied;

''(D) the number of claimants receiving compensation; and

''(E) the length of time required to process each claim, as measured from the date on which the claim is filed to the final disposition of the claim.

''(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Secretary of Energy, for fiscal year 2022 and each succeeding year, such sums as may be

necessary to support the Secretary of Labor in creating or updating the site exposure matrices.''.

SEC. 3163. ASSISTING CURRENT AND FORMER EMPLOYEES UNDER THE EEOICPA.

(a) PROVIDING INFORMATION AND OUTREACH.—Subtitle A of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384d et seq.) is amended—

(1) by redesignating section 3614 as section 3616; and

(2) by inserting after section 3613 the following:

''SEC. 3614. INFORMATION AND OUTREACH.

''(a) ESTABLISHMENT OF TOLL-FREE INFORMATION PHONE NUMBER.—By not later than January 1, 2023, the Secretary of Labor shall establish a toll-free phone number that current or former employees of the Department of Energy, or current or former Department of Energy contractor employees, may use in order to receive information regarding—

''(1) the compensation program under subtitle B or E;

''(2) information regarding the process of submitting a claim under either compensation program;

''(3) assistance in completing the occupational health questionnaire required as part of a claim under subtitle B or E;

''(4) the next steps to take if a claim under subtitle B or E is accepted or denied; and

''(5) such other information as the Secretary determines necessary to further the purposes of this title.

''(b) ESTABLISHMENT OF RESOURCE AND ADVOCACY CENTERS.—

''(1) IN GENERAL.—By not later than January 1, 2024, the Secretary of Energy, in coordination with the Secretary of Labor, shall establish a resource and advocacy center at each Department of Energy facility where cleanup operations are being carried out, or have been carried out, under the environmental management program of the Department of Energy. Each such resource and advocacy center shall assist current or former Department of Energy employees and current or former Department of Energy contractor employees, by enabling the employees and contractor employees to—

''(A) receive information regarding all related programs available to them relating to potential claims under this title, including—

''(i) programs under subtitles B and E; and

''(ii) the former worker medical screening program of the Department of Energy; and

''(B) navigate all such related programs.

''(2) COORDINATION.—The Secretary of Energy shall integrate other programs available to current and former employees, and current or former Department of Energy contractor employees, which are related to the purposes of this title, with the resource and advocacy centers established under paragraph (1), as appropriate.

''(c) INFORMATION.—The Secretary of Labor shall develop and distribute, through the resource and advocacy centers established under subsection (b) and other means, information (which may include responses to frequently asked questions) for current or former employees or current or former Department of Energy contractor employees about the programs under subtitles B and E and the claims process under such programs.

''(d) COPY OF EMPLOYEE'S CLAIMS RECORDS.—

''(1) IN GENERAL.—The Secretary of Labor shall, upon the request of a current or former employee or Department of Energy contractor employee, provide the employee with a complete copy of all records or other materials held by the Department of Labor relating to the employee's claim under subtitle B or E.

''(2) CHOICE OF FORMAT.—The Secretary of Labor shall provide the copy of records described in paragraph (1) to an employee in electronic or paper form, as selected by the employee.

''(e) CONTACT OF EMPLOYEES BY INDUSTRIAL HYGIENISTS.—The Secretary of Labor shall allow industrial hygienists to contact and interview current or former employees or Department of Energy contractor employees regarding the employee's claim under subtitle B or E.''.

(b) EXTENDING APPEAL PERIOD.—Section 3677(a) of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s–6(a)) is amended by striking ''60 days'' and inserting ''180 days''.

(c) FUNDING.—Section 3684 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s–13) is amended—

(1) by striking ''There is authorized'' and inserting the following:

''(a) IN GENERAL.—There is authorized'';

(2) by inserting before the period at the end the following: '', including the amounts necessary to carry out the requirements of section 3681A''; and

(3) by adding at the end the following:

''(b) ADMINISTRATIVE COSTS FOR DEPARTMENT OF ENERGY.—There is authorized to be appropriated to the Secretary of Energy for fiscal year 2022 and each succeeding year such sums as may be necessary to support the Secretary in carrying out the requirements of this title, including section 3681A.''.

(d) ADVISORY BOARD ON TOXIC SUBSTANCES AND WORKER HEALTH.—Section 3687 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s–16) is amended—

(1) in subsection (b)—

(A) in paragraph (1)(F), by striking ''and'' after the semicolon;

(B) in paragraph (2), by striking the period at the end and inserting a semicolon; and

(C) by adding at the end the following:

''(3) develop recommendations for the Secretary of Health and Human Services regarding whether there is a class of Department of Energy employees, Department of Energy contractor employees, or other employees at any Department of Energy facility who were at least as likely as not exposed to toxic substances at that facility but for whom it is not feasible to estimate with sufficient accuracy the dose they received; and

''(4) review all existing, as of the date of the review, rules and guidelines issued by the Secretary regarding presumption of causation and provide the Secretary with recommendations for new rules and guidelines regarding presumption of causation.'';

(2) in subsection (c)(3), by inserting ''or the Board'' after ''The Secretary'';

(3) by redesignating subsections (h), (i), and (j) as subsections (i), (j), and (k), respectively; and

(4) by inserting after subsection (g) the following:

''(h) REQUIRED RESPONSES TO BOARD RECOMMENDATIONS.—Not later than 90 days after the date on which the Secretary of Labor and the Secretary of Health and Human Services receive recommendations in accordance with paragraph (1), (3), or (4) of subsection (b), each such Secretary shall submit formal responses to each recommendation to the Board and Congress.''.

SEC. 3164. RESEARCH PROGRAM ON EPIDEMIOLOGICAL IMPACTS OF TOXIC EXPOSURES.

(a) DEFINITIONS.—In this section—

(1) the term ''Department of Energy facility'' has the meaning given the term in section 3621 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384l);

(2) the term ''institution of higher education'' has the meaning given such term in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001); and

(3) the term ''Secretary'' means the Secretary of Health and Human Services.

(b) ESTABLISHMENT.—The Secretary, acting through the Director of the National Institute of Environmental Health Sciences and in collaboration with the Director of the Centers for Disease Control and Prevention, shall conduct or support research on the epidemiological impacts of exposures to toxic substances at Department of Energy facilities.

(c) USE OF FUNDS.—Research under subsection (b) may include research on the epidemiological, clinical, or health impacts on individuals who were exposed to toxic substances in or near the tank or other storage farms and other relevant Department of Energy facilities through their work at such sites.

(d) ELIGIBILITY AND APPLICATION.—Any institution of higher education or the National Academy of Sciences may apply for funding under this section by submitting to the Secretary an application at such time, in such manner, and containing or accompanied by such information as the Secretary may require.

(e) RESEARCH COORDINATION.—The Secretary shall coordinate activities under this section with similar activities conducted by the Department of Health and Human Services to the extent that other agencies have responsibilities that are related to the study of epidemiological, clinical, or health impacts of exposures to toxic substances.

(f) HEALTH STUDIES REPORT TO SECRETARY.—Not later than 1 year after the end of the funding period for research under this section, the funding recipient shall prepare and submit to the Secretary a final report that—

(1) summarizes the findings of the research;

(2) includes recommendations for any additional studies;

(3) describes any classes of employees that, based on the results of the report, could warrant the establishment of a Special Exposure Cohort under the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.) for toxic substances exposures; and

(4) describes any illnesses to be included as covered illnesses under such Act (42 U.S.C. 7384 et seq.).

(g) REPORT TO CONGRESS.—

(1) IN GENERAL.—Not later than 120 days after the date on which the reports under subsection (f) are due, the Secretary shall—

(A) identify a list of cancers and other illnesses associated with toxic substances that pose, or posed, a hazard in the work environment at any Department of Energy facility; and

(B) prepare and submit to the relevant committees of Congress a report—

(i) summarizing the findings from the reports required under subsection (f);

(ii) identifying any new illnesses that, as a result of the study, will be included as covered illnesses, pursuant to subsection (f)(4) and section 3671(2) of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7385s(2)); and

(iii) including the Secretary's recommendations for additional health studies relating to toxic substances, if the Secretary determines it necessary.

(2) RELEVANT COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term ''relevant committees of Congress'' means—

(A) the Committee on Armed Services, Committee on Appropriations, Committee on

Energy and Natural Resources, and Committee on Health, Education, Labor, and Pensions of the Senate; and

(B) the Committee on Armed Services, Committee on Appropriations, Committee on Energy and Commerce, and Committee on Education and Labor of the House of Representatives.

(h) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $3,000,000 for each of fiscal years 2022 through 2026.

SEC. 3165. NATIONAL ACADEMY OF SCIENCES REVIEW.

Subtitle A of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384d et seq.), as amended by section 3163, is further amended by inserting after section 3614 the following:

"SEC. 3615. NATIONAL ACADEMY OF SCIENCES REVIEW.

''(a) PURPOSE.—The purpose of this section is to enable the National Academy of Sciences, a non-Federal entity with appropriate expertise, to review and evaluate the available scientific evidence regarding associations between diseases and exposure to toxic substances found at Department of Energy cleanup sites.

''(b) DEFINITIONS.—In this section:

''(1) DEPARTMENT OF ENERGY CLEANUP SITE.—The term 'Department of Energy cleanup site' means a Department of Energy facility where cleanup operations are being carried out, or have been carried out, under the environmental management program of the Department of Energy.

''(2) HEALTH STUDIES REPORT.—The term 'health studies report' means the report submitted under section 3164(f) of the Toxic Exposure Safety Act of 2021.

''(c) AGREEMENT.—The Secretary of Health and Human Services shall seek to enter into an agreement with the National Academy of Sciences, not later than 60 days after the issuance of the health studies report, to carry out the requirements of this section.

''(d) REVIEW OF SCIENTIFIC AND MEDICAL EVIDENCE.—

''(1) IN GENERAL.—Under the agreement described in subsection (c), the National Academy of Sciences shall, for the period of the agreement—

''(A) for each area recommended for additional study under the health studies report under section 3164(f)(2) of the Toxic Exposure Safety Act of 2021, review and summarize the scientific evidence relating to the area, including—

''(i) studies by the Department of Energy and Department of Labor; and

''(ii) any other available and relevant scientific studies, to the extent that such studies are relevant to the occupational exposures that have occurred at Department of Energy cleanup sites; and

''(B) review and summarize the scientific and medical evidence concerning the association between exposure to toxic substances found at Department of Energy cleanup sites and resultant diseases.

''(2) SCIENTIFIC DETERMINATIONS CONCERNING DISEASES.—In conducting each review of scientific evidence under subparagraphs (A) and (B) of paragraph (1), the National Academy of Sciences shall—

''(A) assess the strength of such evidence;

''(B) assess whether a statistical association between exposure to a toxic substance and a disease exists, taking into account the strength of the scientific evidence and the appropriateness of the statistical and epidemiological methods used to detect an association;

''(C) assess the increased risk of disease among those exposed to the toxic substance during service during the production and cleanup eras of the Department of Energy cleanup sites;

''(D) survey the impact to health of the toxic substance, focusing on hematologic, renal, urologic, hepatic, gastrointestinal, neurologic, dermatologic, respiratory, endocrine, ocular, ear, nasal, and oropharyngeal diseases, including dementia, leukemia, chemical sensitivities, and chronic obstructive pulmonary disease; and

''(E) determine whether a plausible biological mechanism or other evidence of a causal relationship exists between exposure to the toxic substance and disease.

''(e) ADDITIONAL SCIENTIFIC STUDIES.—If the National Academy of Sciences determines, in the course of conducting the studies under subsection (d), that additional studies are needed to resolve areas of continuing scientific uncertainty relating to toxic exposure at Department of Energy cleanup sites, the National Academy of Sciences shall include, in the next report submitted under subsection (f), recommendations for areas of additional study, consisting of—

''(1) a list of diseases and toxins that require further evaluation and study;

''(2) a review the current information available, as of the date of the report, relating to such diseases and toxins;

''(3) the value of the information that would result from the additional studies; and

''(4) the cost and feasibility of carrying out additional studies.

''(f) REPORTS.—

''(1) IN GENERAL.—By not later than 18 months after the date of the agreement under subsection (c), and every 2 years thereafter, the National Academy of Sciences shall under such agreement prepare and submit a report to—

''(A) the Secretary;

''(B) the Committee on Health, Education, Labor, and Pensions and the Committee on Energy and Natural Resources of the Senate; and

''(C) the Committee on Natural Resources, the Committee on Education and Labor, and the Committee on Energy and Commerce of the House of Representatives.

''(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for the 18-month or 2-year period covered by the report—

''(A) a description of—

''(i) the reviews and studies conducted under this section;

''(ii) the determinations and conclusions of the National Academy of Sciences with respect to such reviews and studies; and

''(iii) the scientific evidence and reasoning that led to such conclusions;

''(B) the recommendations for further areas of study made under subsection (e) for the reporting period;

''(C) a description of any classes of employees that, based on the results of the reviews and studies, could qualify as a Special Exposure Cohort; and

''(D) the identification of any illness that the National Academy of Sciences has determined, as a result of the reviews and studies, should be a covered illness.

''(g) LIMITATION ON AUTHORITY.—The authority to enter into agreements under this section shall be effective for a fiscal year to the extent that appropriations are available.

''(h) SUNSET.—This section shall cease to be effective 10 years after the last day of the fiscal year in which the National Academy of Sciences transmits to the Secretary the first report under subsection (f).''.

SEC. 3166. CONFORMING AMENDMENTS.

The Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 7384 et seq.) is amended—

(1) in the table of contents—

(A) by redesignating the item relating to section 3614 as the item relating to section 3616;

(B) by inserting after the item relating to section 3613 the following:

''Sec. 3614. Information and outreach.

''Sec. 3615. National Academy of Sciences review.'';

and

(C) by inserting after the item relating to section 3681 the following:

''Sec. 3681A. Completion and updates of site exposure matrices.'';

and

(2) in each of subsections (b)(1) and (c) of section 3612, by striking ''3614(b)'' and inserting ''3616(b)''.

SA 4793. Mr. LEE (for himself and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

In section 511, beginning in subsection (d)(4), strike the period at the end of subparagraph (B)(ii) and all that follows through subsection (g) and insert the following: ''; and

(C) by adding at the end the following new subsection:

''(p) No person may be inducted for training and service under this title if such person—

''(1) has a dependent child and the other parent of the dependent child has been inducted for training or service under this title unless the person volunteers for such induction; or

''(2) has a dependent child who has no other living parent.''.

(5) Section 10(b)(3) (50 U.S.C. 3809(b)(3)) is amended by striking ''the President is requested'' and all that follows through ''race or national origin'' and inserting ''the President is requested to appoint the membership of each local board so that each board has both male and female members and, to the maximum extent practicable, it is proportionately representative of those registrants within its jurisdiction in each applicable basis set forth in section 703(a) of the Civil Rights Act of 1964 (42 U.S.C. 2002e–2(a)), but no action by any board shall be declared invalid on the ground that such board failed to conform to such representation quota''.

(6) Section 16(a) (50 U.S.C. 3814(a)) is amended by striking ''men'' and inserting ''persons''.

(e) MAINTAINING THE HEALTH OF THE SELECTIVE SERVICE SYSTEM.—Section 10(a) (50 U.S.C. 3809(a)) is amended by adding at the end the following new paragraph:

''(5) The Selective Service System shall conduct exercises periodically of all mobilization plans, systems, and processes to evaluate and test the effectiveness of such plans, systems, and processes. Once every 4 years, the exercise shall include the full range of internal and interagency procedures to ensure functionality and interoperability and may take place as part of the Department of Defense mobilization exercise under section 10208 of title 10, United States Code. The Selective Service System shall conduct a public awareness campaign in conjunction

with each exercise to communicate the purpose of the exercise to the public.''.

(f) TECHNICAL AND CONFORMING AMENDMENTS.—The Military Selective Service Act is amended—

(1) in section 4 (50 U.S.C. 3803)—

(A) in subsection (a) in the third undesignated paragraph—

(i) by striking ''his acceptability in all respects, including his'' and inserting ''such person's acceptability in all respects, including such person's''; and

(ii) by striking ''he may prescribe'' and inserting ''the President may prescribe'';

(B) in subsection (c)—

(i) in paragraph (2), by striking ''any enlisted member'' and inserting ''any person who is an enlisted member''; and

(ii) in paragraphs (3), (4), and (5), by striking ''in which he resides'' and inserting ''in which such person resides'';

(C) in subsection (g), by striking ''coordinate with him'' and inserting ''coordinate with the Director''; and

(D) in subsection (k)(1), by striking ''finding by him'' and inserting ''finding by the President'';

(2) in section 5(d) (50 U.S.C. 3805(d)), by striking ''he may prescribe'' and inserting ''the President may prescribe'';

(3) in section 6 (50 U.S.C. 3806)—

(A) in subsection (c)(2)(D), by striking ''he may prescribe'' and inserting ''the President may prescribe'';

(B) in subsection (d)(3), by striking ''he may deem appropriate'' and inserting ''the President considers appropriate''; and

(C) in subsection (h), by striking ''he may prescribe'' each place it appears and inserting ''the President may prescribe'';

(4) in section 10 (50 U.S.C. 3809)—

(A) in subsection (b)—

(i) in paragraph (3)—

(I) by striking ''He shall create'' and inserting ''The President shall create''; and

(II) by striking ''upon his own motion'' and inserting ''upon the President's own motion'';

(ii) in paragraph (4), by striking ''his status'' and inserting ''such individual's status''; and

(iii) in paragraphs (4), (6), (8), and (9), by striking ''he may deem'' each place it appears and inserting ''the President considers''; and

(B) in subsection (c), by striking ''vested in him'' and inserting ''vested in the President'';

(5) in section 13(b) (50 U.S.C. 3812(b)), by striking ''regulation if he'' and inserting ''regulation if the President'';

(6) in section 15 (50 U.S.C. 3813)—

(A) in subsection (b), by striking ''his'' each place it appears and inserting ''the registrant's''; and

(B) in subsection (d), by striking ''he may deem'' and inserting ''the President considers'';

(7) in section 16(g) (50 U.S.C. 3814(g))—

(A) in paragraph (1), by striking ''who as his regular and customary vocation'' and inserting ''who, as such person's regular and customary vocation,''; and

(B) in paragraph (2)—

(i) by striking ''one who as his customary vocation'' and inserting ''a person who, as such person's customary vocation,''; and

(ii) by striking ''he is a member'' and inserting ''such person is a member'';

(8) in section 18(a) (50 U.S.C. 3816(a)), by striking ''he is authorized'' and inserting ''the President is authorized'';

(9) in section 21 (50 U.S.C. 3819)—

(A) by striking ''he is sooner'' and inserting ''sooner'';

(B) by striking ''he'' each subsequent place it appears and inserting ''such member''; and

(C) by striking ''his consent'' and inserting ''such member's consent'';

(10) in section 22(b) (50 U.S.C. 3820(b)), in paragraphs (1) and (2), by striking ''his'' each place it appears and inserting ''the registrant's''; and

(11) except as otherwise provided in this section—

(A) by striking ''he'' each place it appears and inserting ''such person'';

(B) by striking ''his'' each place it appears and inserting ''such person's'';

(C) by striking ''him'' each place it appears and inserting ''such person''; and

(D) by striking ''present himself'' each place it appears in section 12 (50 U.S.C. 3811) and inserting ''appear''.

(g) ENACTMENT OF AUTHORIZATION REQUIRED FOR DRAFT.—

(1) FINDINGS.—Congress makes the following findings:

(A) Clause 12 of section 8 of article I of the Constitution of the United States empowers Congress with the responsibility to ''raise and support Armies''.

(B) The United States first required military conscription in the American Civil War under the Civil War Military Draft Act of 1863.

(C) The Selective Services Act of 1917 authorized the President to draft additional forces beyond the volunteer force to support exceedingly high demand for additional forces when the U.S. entered the first World War.

(D) The Selective Training and Service Act of 1940 was the first authorization by Congress for conscription in peacetime but limited the President's induction authority to ''no greater number of men than the Congress shall hereafter make specific appropriation for from time to time''.

(E) Congress allowed induction authority to lapse in 1947.

(F) Congress reinstated the President's induction authority under the Selective Service Act of 1948 to raise troops for United States participation in the Korean War.

(G) Congress maintained the President's induction authority under the Selective Service Act of 1948 through the beginning of the Vietnam War.

(H) Congress passed additional reforms to the draft under the Military Selective Service Act of 1967 in response to issues arising from United States engagement in the Vietnam War.

(I) Congress prohibited any further use of the draft after July 1, 1973.

(J) If a president seeks to reactivate the use of the draft, Congress would have to enact a law providing authorization for this purpose

(2) AMENDMENT.—Section 17 of the Military Selective Service Act (50 U.S.C. 3815) is amended by adding at the end the following new subsection:

''(d) No person shall be inducted for training and service in the Armed Forces unless Congress first passes and there is enacted a law expressly authorizing such induction into service.''.

(h) EFFECTIVE DATE.—The amendments made by this section shall take effect on the date of the enactment of this Act, except that the amendments made by subsections (d) and (g) shall take effect 1 year after such date of enactment.

SA 4794. Mr. RISCH (for himself, Mr. PORTMAN, Mr. CRUZ, Mr. BARRASSO, Mr. JOHNSON, Mr. COTTON, and Mr. DAINES) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle D of title XII, add the following:

SEC. 1237. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Not later than 15 days after the date of the enactment of this Act, the President shall—

(1) impose sanctions under subsection (b) with respect to any corporate officer of an entity established for or responsible for the planning, construction, or operation of the Nord Stream 2 pipeline or a successor entity; and

(2) impose sanctions under subsection (c) with respect to any entity described in paragraph (1).

(b) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE OF IDENTIFIED PERSONS AND CORPORATE OFFICERS.—

(1) IN GENERAL.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (a)(1) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien described in subsection (a)(1) shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

(c) BLOCKING OF PROPERTY OF IDENTIFIED PERSONS.—The President shall exercise all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of an entity described in subsection (a)(1) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(d) EXCEPTIONS.—

(1) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under this section shall not apply to any authorized intelligence, law enforcement, or national security activities of the United States.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under this section shall not apply with respect to the admission of an alien to the United States if the admission of the alien is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or other applicable international obligations.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—Notwithstanding any other provision of this section, the authorities and requirements to impose sanctions under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term ''good'' means any article, natural or man-made substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(e) CONDITIONS FOR REMOVAL OF SANCTIONS.—Subject to review by Congress under section 216 of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511), the President may waive the application of sanctions under this section if the President—

(1) determines that the waiver is in the national security interest of the United States; and

(2) submits to the appropriate congressional committees a report on the waiver and the reason for the waiver.

(f) IMPLEMENTATION; PENALTIES.—

(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this section or any regulation, license, or order issued to carry out this section shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(g) SUNSET.—The authority to impose sanctions under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(h) DEFINITIONS.—In this section:

(1) ADMISSION; ADMITTED; ALIEN.—The terms ''admission'' , ''admitted'' , and ''alien'' have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives.

(3) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person within the United States.

SEC. 1238. CONGRESSIONAL REVIEW OF WAIVER UNDER PROTECTING EUROPE'S ENERGY SECURITY ACT OF 2019.

Section 7503(f) of the Protecting Europe's Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note) is amended, in the matter preceding paragraph (1), by striking ''The President'' and inserting ''Subject to review by Congress under section 216 of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511), the President''.

SEC. 1239. APPLICATION OF CONGRESSIONAL REVIEW UNDER COUNTERING AMERICA'S ADVERSARIES THROUGH SANCTIONS ACT.

Section 216(a)(2) of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(2)) is amended—

(1) in subparagraph (A)—

(A) in clause (i), by inserting ''(other than sanctions described in clause (i)(IV) of that subparagraph)'' after ''subparagraph (B)''; and

(B) in clause (ii), by inserting ''or otherwise remove'' after ''waive''; and

(2) in subparagraph (B)(i)—

(A) in subclause (II), by striking ''; or'' and inserting a semicolon;

(B) in subclause (III), by striking ''; and'' and inserting a semicolon; and

(C) by adding at the end the following:

''(IV) section 7503 of the Protecting Europe's Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note); or

''(V) section 1237 of the National Defense Authorization Act for Fiscal Year 2022; and''.

SEC. 1240. INCLUSION OF MATTER RELATING TO NORD STREAM 2 IN REPORT UNDER COUNTERING AMERICA'S ADVERSARIES THROUGH SANCTIONS ACT.

Each report submitted under section 216(a)(1) of the Countering America's Adversaries Through Sanctions Act (22 U.S.C. 9511(a)(1)) relating to sanctions under section 1237 of this Act or section 7503 of the Protecting Europe's Energy Security Act of 2019 (title LXXV of Public Law 116–92; 22 U.S.C. 9526 note) shall include—

(1) an assessment of the security risks posed by Nord Stream 2, including—

(A) the presence along Nord Stream 2 or Nord Stream 1 infrastructure or pipeline corridors of undersea surveillance systems and sensors, fiber optic terminals, or other systems that are capable of conducting military or intelligence activities unrelated to civilian energy transmission, including those designed to enhance Russian Federation antisubmarine warfare, surveillance, espionage, or sabotage capabilities;

(B) the use of Nord Stream-affiliated infrastructure, equipment, personnel, vessels, financing, or other assets—

(i) to facilitate, carry out, or conceal Russian Federation maritime surveillance, espionage, or sabotage activities;

(ii) to justify the presence of Russian Federation naval vessels or military personnel or equipment in international waters or near North Atlantic Treaty Organization or partner countries;

(iii) to disrupt freedom of navigation; or

(iv) to pressure or intimidate countries in the Baltic Sea;

(C) the involvement in the Nord Stream 2 pipeline or its affiliated entities of current or former Russian, Soviet, or Warsaw Pact intelligence and military personnel and any business dealings between Nord Stream 2 and entities affiliated with the intelligence or defense sector of the Russian Federation; and

(D) malign influence activities of the Government of the Russian Federation, including strategic corruption and efforts to influence European decision-makers, supported or financed through the Nord Stream 2 pipeline;

(2) an assessment of whether the Russian Federation maintains gas transit through Ukraine at levels consistent with the volumes set forth in the Ukraine-Russian Federation gas transit agreement of December 2019 and continues to pay the transit fees specified in that agreement;

(3) an assessment of the status of negotiations between the Russian Federation and Ukraine to secure an agreement to extend gas transit through Ukraine beyond the expiration of the agreement described in paragraph (2); and

(4) an assessment of whether the United States and Germany have agreed on a common definition for energy ''weaponization'' and the associated triggers for sanctions and other enforcement actions, pursuant to the Joint Statement of the United States and Germany on support for Ukraine, European energy security, and our climate goals, dated July 21, 2021; and

(5) a description of the consultations with United States allies and partners in Europe, including Ukraine, Poland, and the countries in Central and Eastern Europe most impacted by the Nord Stream 2 pipeline concerning the matters agreed to as described in paragraph (4).

SA 4795. Mr. SHELBY (for himself, Mr. INHOFE, Mr. WICKER, Mr. BLUNT, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. COTTON, Mr. BOOZMAN, Ms. COLLINS, Mr. KENNEDY, Ms. MURKOWSKI, Mr. CRAMER, Mr. TILLIS, and Mr. HOEVEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—AUTHORIZATION OF AMOUNTS FOR DEPARTMENT OF DEFENSE INFRASTRUCTURE

SEC. _____1. ESTABLISHMENT OF DEFENSE INFRASTRUCTURE FUND.

There is established in the general fund of the Treasury an account to be known as the ''Defense Infrastructure Fund'' for the deposit of amounts to be used for improvement of the infrastructure of the Department of Defense.

SEC. _____2. AUTHORIZATION OF AMOUNTS FOR REDUCTION OF BACKLOG FOR FACILITY INFRASTRUCTURE PROJECTS.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $4,000,000,000 for the Defense Infrastructure Fund, of which $1,300,000,000 shall be available for each of the Departments of the Army, the Navy, and the Air Force, and $100,000,000 shall be for the Defense Health Agency, to reduce the backlog of facility infrastructure maintenance projects of the Department of Defense.

(b) COMPLIANCE WITH REPAIR REQUIREMENTS.—Any project carried out with amounts authorized under subsection (a) shall comply with the requirements under section 2811 of title 10, United States Code.

(c) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____3. AUTHORIZATION OF AMOUNTS FOR MODERNIZATION OF TEST AND TRAINING RANGES OF DEPARTMENT OF DEFENSE.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $2,800,000,000 for the Defense Infrastructure Fund to modernize the test and training ranges of the Department of Defense, including projects included in the report required under section 2806 of the Military Construction Authorization Act for Fiscal Year 2018

(Division B of Public Law 115–91; 10 U.S.C. 222a note) for test and evaluation activities.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2032.

SEC. _____4. AUTHORIZATION OF AMOUNTS FOR REMEDIATION OF PERFLUORALKYL SUBSTANCES AND POLYFLUOROALKYL SUBSTANCES.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $700,000,000 for the Defense Infrastructure Fund to remediate perfluoralkyl substances and polyfluoroalkyl substances at installations owned by the Department of Defense.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____5. AUTHORIZATION OF AMOUNTS FOR DEPOT MODERNIZATION.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $4,325,000,000 for the Defense Infrastructure Fund for depot modernization.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2032.

SEC. _____6. AUTHORIZATION OF AMOUNTS FOR AMMUNITION PLANT MODERNIZATION.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $2,350,000,000 for the Defense Infrastructure Fund to modernize ammunition plants.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____7. AUTHORIZATION OF AMOUNTS FOR FIFTH-GENERATION WIRELESS NETWORKING TECHNOLOGIES.

(a) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $2,500,000,000 for the Defense Infrastructure Fund to provide fifth-generation wireless networking technologies to installations owned by the Department of Defense.

(b) AVAILABILITY OF AMOUNTS.—Amounts authorized under subsection (a) shall be available for obligation until September 30, 2026.

SEC. _____8. AUTHORIZATION OF AMOUNTS FOR NAVY SHIPYARD AND INFRASTRUCTURE IMPROVEMENT.

(a) AUTHORIZATION.—

(1) IN GENERAL.—There is authorized to be appropriated to the Department of Defense $10,325,000,000 for the Defense Infrastructure Fund to improve, in accordance with subsection (b), the Navy shipyard infrastructure of the United States.

(2) AVAILABILITY OF AMOUNTS.—Amounts authorized under paragraph (1) shall be available until expended.

(3) SUPPLEMENT NOT SUPPLANT.—Amounts authorized under paragraph (1) shall supplement and not supplant other amounts appropriated or otherwise made available for the purpose described in paragraph (1).

(b) USE OF FUNDS.—

(1) IN GENERAL.—As soon as practicable after the date of the enactment of this Act, the Secretary of Defense shall make amounts appropriated pursuant to the authorization under subsection (a)(1) directly available to the Secretary of the Navy for obligation and expenditure for Navy public shipyard facilities, dock, dry dock, capital equipment improvements, and dredging efforts needed by such shipyards.

(2) PROJECTS IN ADDITION TO OTHER CONSTRUCTION PROJECTS.—Construction projects undertaken using amounts appropriated pursuant to the authorization under subsection (a)(1) shall be in addition to and separate from any military construction program authorized by any Act to authorize appropriations for a fiscal year for military activities of the Department of Defense and for military construction.

(c) NAVY PUBLIC SHIPYARD DEFINED.—In this section, the term ''Navy public shipyard'' means the following:

(1) The Norfolk Naval Shipyard, Virginia.

(2) The Pearl Harbor Naval Shipyard, Hawaii.

(3) The Portsmouth Naval Shipyard, Maine.

(4) The Puget Sound Naval Shipyard, Washington.

SA 4796. Mr. PAUL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle C of title VII, add the following:

SEC. 744. PROHIBITION ON DISHONORABLE DISCHARGE OF MEMBERS OF THE ARMED FORCES FOR REFUSING TO COMPLY WITH COVID–19 VACCINE MANDATE.

The Secretary of Defense may not give a dishonorable discharge to a member of the Armed Forces solely on the basis of the refusal of the member, for religious, medical, or personal reasons, to comply with any requirement that the member receive a vaccination for coronavirus disease 2019 (commonly known as ''COVID–19'').

SA 4797. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle D of title XXVIII, add the following:

SEC. 2836. PAYMENT TO ENVIRONMENTAL PROTECTION AGENCY FOR CERTAIN COSTS IN CONNECTION WITH FORMER ROCKY MOUNTAIN ARSENAL, COLORADO.

(a) AUTHORITY FOR PAYMENT.—

(1) TRANSFER AMOUNT.—

(A) IN GENERAL.—Notwithstanding section 2215 of title 10, United States Code, chapter 160 of such title, section 1367 of the National Defense Authorization Act for Fiscal Year 1987 (Public Law 99–661; 100 Stat. 4003), or any other provision of law, using funds described in subsection (b), the Secretary of Defense may transfer to the Administrator of the Environmental Protection Agency for use at the former Rocky Mountain Arsenal, Colorado—

(i) in fiscal year 2022, $4,805,000 for costs associated with the involvement of the Environmental Protection Agency with the cleanup by the Department of the Army of the former Rocky Mountain Arsenal from fiscal years 2015 through 2020, after a specific accounting is provided in accordance with subparagraph (B); and

(ii) in each of fiscal years 2022, 2023, and 2024, to account for costs incurred by the Environmental Protection Agency for such cleanup in fiscal years 2021, 2022, and 2023, an amount not to exceed $600,000, after a specific accounting is provided in accordance with subparagraph (B).

(B) ACCOUNTING.—Prior to the payment of amounts under subparagraph (A), the Administrator of the Environmental Protection Agency shall furnish to the Secretary of Defense a specific accounting of costs for which payment is requested.

(C) AUTHORIZED COSTS.—Payment of amounts under subparagraph (A) may be made only for those costs incurred by the Environmental Protection Agency for fiscal years 2015 through 2023—

(i) for providing technical assistance in accordance with the document entitled ''Settlement Agreement Between the United States and Shell Oil Company Concerning the Rocky Mountain Arsenal'', effective February 17, 1989, as incorporated into the consent decree entered by the United States District Court for the District of Colorado in United States v. Shell Oil Co., Civil Action No. 83-C-2379, dated February 12, 1992 (referred to in this section as the ''Settlement Agreement''); and

(ii) that are not inconsistent with the National Oil and Hazardous Substances Pollution Contingency Plan described in part 300 of title 40, Code of Federal Regulations (or successor regulations).

(2) PURPOSE OF PAYMENT.—The amounts authorized to be transferred under paragraph (1)(A) are—

(A) for payment to the Environmental Protection Agency for all costs that may be owed by the Department of the Army to the Environmental Protection Agency pursuant to the Settlement Agreement; and

(B) for use at the former Rocky Mountain Arsenal to allow the Environmental Protection Agency to proceed with review of cleanup documents that the Agency had suspended.

(b) SOURCE OF FUNDS.—The transfer authorized under subsection (a)(1)(A) shall be made using funds authorized to be appropriated for fiscal years 2022, 2023, and 2024 for Operation and Maintenance, Army for Environmental Restoration.

(c) FINALITY OF PAYMENTS.—The transfer authorized under subsection (a)(1)(A) constitutes final and complete payment for all costs borne by the Environmental Protection Agency arising from the Settlement Agreement for fiscal years 2015 through 2023.

SA 4798. Mr. CASSIDY (for himself, Mr. WHITEHOUSE, and Ms. WARREN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. _____. POSTSECONDARY STUDENT DATA SYSTEM.

(a) SHORT TITLE.—This section may be cited as the ''College Transparency Act''.

(b) POSTSECONDARY STUDENT DATA SYSTEM.—Section 132 of the Higher Education Act of 1965 (20 U.S.C. 1015a) is amended—

(1) by redesignating subsection (l) as subsection (m); and

(2) by inserting after subsection (k) the following:

''(l) POSTSECONDARY STUDENT DATA SYSTEM.—

''(1) IN GENERAL.—

''(A) ESTABLISHMENT OF SYSTEM.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner of the National Center for Education Statistics (referred to in this subsection as the 'Commissioner') shall develop and maintain a secure, privacy-protected postsecondary student-level data system in order to—

''(i) accurately evaluate student enrollment patterns, progression, completion, and postcollegiate outcomes, and higher education costs and financial aid;

''(ii) assist with transparency, institutional improvement, and analysis of Federal aid programs;

''(iii) provide accurate, complete, and customizable information for students and families making decisions about postsecondary education; and

''(iv) reduce the reporting burden on institutions of higher education, in accordance with section 5(b) of the College Transparency Act.

''(B) AVOIDING DUPLICATED REPORTING.—Notwithstanding any other provision of this section, to the extent that another provision of this section requires the same reporting or collection of data that is required under this subsection, an institution of higher education, or the Secretary or Commissioner, may use the reporting or data required for the postsecondary student data system under this subsection to satisfy both requirements.

''(C) DEVELOPMENT PROCESS.—In developing the postsecondary student data system described in this subsection, the Commissioner shall—

''(i) focus on the needs of—

''(I) users of the data system; and

''(II) entities, including institutions of higher education, reporting to the data system;

''(ii) take into consideration, to the extent practicable—

''(I) the guidelines outlined in the U.S. Web Design Standards maintained by the General Services Administration and the Digital Services Playbook and TechFAR Handbook for Procuring Digital Services Using Agile Processes of the U.S. Digital Service; and

''(II) the relevant successor documents or recommendations of such guidelines;

''(iii) use modern, relevant privacy- and security-enhancing technology, and enhance and update the data system as necessary to carry out the purpose of this subsection;

''(iv) ensure data privacy and security is consistent with any Federal law relating to privacy or data security, including—

''(I) the requirements of subchapter II of chapter 35 of title 44, United States Code, specifying security categorization under the Federal Information Processing Standards or any relevant successor of such standards;

''(II) security requirements that are consistent with the Federal agency responsibilities in section 3554 of title 44, United States Code, or any relevant successor of such responsibilities; and

''(III) security requirements, guidelines, and controls consistent with cybersecurity standards and best practices developed by the National Institute of Standards and Technology, including frameworks, consistent with section 2(c) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)), or any relevant successor of such frameworks;

''(v) follow Federal data minimization practices to ensure only the minimum amount of data is collected to meet the system's goals, in accordance with Federal data minimization standards and guidelines developed by the National Institute of Standards and Technology; and

''(vi) provide notice to students outlining the data included in the system and how the data are used.

''(2) DATA ELEMENTS.—

''(A) IN GENERAL.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner, in consultation with the Postsecondary Student Data System Advisory Committee established under subparagraph (B), shall determine—

''(i) the data elements to be included in the postsecondary student data system, in accordance with subparagraphs (C) and (D); and

''(ii) how to include the data elements required under subparagraph (C), and any additional data elements selected under subparagraph (D), in the postsecondary student data system.

''(B) POSTSECONDARY STUDENT DATA SYSTEM ADVISORY COMMITTEE.—

''(i) ESTABLISHMENT.—Not later than 2 years after the date of enactment of the College Transparency Act, the Commissioner shall establish a Postsecondary Student Data System Advisory Committee (referred to in this subsection as the 'Advisory Committee'), whose members shall include—

''(I) the Chief Privacy Officer of the Department or an official of the Department delegated the duties of overseeing data privacy at the Department;

''(II) the Chief Security Officer of the Department or an official of the Department delegated the duties of overseeing data security at the Department;

''(III) representatives of diverse institutions of higher education, which shall include equal representation between 2-year and 4-year institutions of higher education, and from public, nonprofit, and proprietary institutions of higher education, including minority-serving institutions;

''(IV) representatives from State higher education agencies, entities, bodies, or boards;

''(V) representatives of postsecondary students;

''(VI) representatives from relevant Federal agencies; and

''(VII) other stakeholders (including individuals with expertise in data privacy and security, consumer protection, and postsecondary education research).

''(ii) REQUIREMENTS.—The Commissioner shall ensure that the Advisory Committee—

''(I) adheres to all requirements under the Federal Advisory Committee Act (5 U.S.C. App.);

''(II) establishes operating and meeting procedures and guidelines necessary to execute its advisory duties; and

''(III) is provided with appropriate staffing and resources to execute its advisory duties.

''(C) REQUIRED DATA ELEMENTS.—The data elements in the postsecondary student data system shall include, at a minimum, the following:

''(i) Student-level data elements necessary to calculate the information within the surveys designated by the Commissioner as 'student-related surveys' in the Integrated Postsecondary Education Data System (IPEDS), as such surveys are in effect on the day before the date of enactment of the College Transparency Act, except that in the case that collection of such elements would conflict with subparagraph (F), such elements in conflict with subparagraph (F) shall be included in the aggregate instead of at the student level.

''(ii) Student-level data elements necessary to allow for reporting student enrollment, persistence, retention, transfer, and completion measures for all credential levels separately (including certificate, associate, baccalaureate, and advanced degree levels), within and across institutions of higher education (including across all categories of institution level, control, and predominant degree awarded). The data elements shall allow for reporting about all such data disaggregated by the following categories:

''(I) Enrollment status as a first-time student, recent transfer student, or other non-first-time student.

''(II) Attendance intensity, whether full-time or part-time.

''(III) Credential-seeking status, by credential level.

''(IV) Race or ethnicity, in a manner that captures all the racial groups specified in the most recent American Community Survey of the Bureau of the Census.

''(V) Age intervals.

''(VI) Gender.

''(VII) Program of study (as applicable).

''(VIII) Military or veteran benefit status (as determined based on receipt of veteran's education benefits, as defined in section 480(c)).

''(IX) Status as a distance education student, whether exclusively or partially enrolled in distance education.

''(X) Federal Pell Grant recipient status under section 401 and Federal loan recipient status under title IV, provided that the collection of such information complies with paragraph (1)(B).

''(D) OTHER DATA ELEMENTS.—

''(i) IN GENERAL.—The Commissioner may, after consultation with the Advisory Committee and provision of a public comment period, include additional data elements in the postsecondary student data system, such as those described in clause (ii), if those data elements—

''(I) are necessary to ensure that the postsecondary data system fulfills the purposes described in paragraph (1)(A); and

''(II) are consistent with data minimization principles, including the collection of only those additional elements that are necessary to ensure such purposes.

''(ii) DATA ELEMENTS.—The data elements described in clause (i) may include—

''(I) status as a first generation college student, as defined in section 402A(h);

''(II) economic status;

''(III) participation in postsecondary remedial coursework or gateway course completion; or

''(IV) other data elements that are necessary in accordance with clause (i).

''(E) REEVALUATION.—Not less than once every 3 years after the implementation of the postsecondary student data system described in this subsection, the Commissioner, in consultation with the Advisory Committee described in subparagraph (B), shall review the data elements included in the postsecondary student data system and may revise the data elements to be included in such system.

''(F) PROHIBITIONS.—The Commissioner shall not include individual health data (including data relating to physical health or mental health), student discipline records or data, elementary and secondary education data, an exact address, citizenship status, migrant status, or national origin status for students or their families, course grades, postsecondary entrance examination results, political affiliation, or religion in the postsecondary student data system under this subsection.

''(3) PERIODIC MATCHING WITH OTHER FEDERAL DATA SYSTEMS.—

''(A) DATA SHARING AGREEMENTS.—

''(i) The Commissioner shall ensure secure, periodic data matches by entering into data

sharing agreements with each of the following Federal agencies and offices:

''(I) The Secretary of the Treasury and the Commissioner of the Internal Revenue Service, in order to calculate aggregate program- and institution-level earnings of postsecondary students.

''(II) The Secretary of Defense, in order to assess the use of postsecondary educational benefits and the outcomes of servicemembers.

''(III) The Secretary of Veterans Affairs, in order to assess the use of postsecondary educational benefits and outcomes of veterans.

''(IV) The Director of the Bureau of the Census, in order to assess the earnings outcomes of former postsecondary education students.

''(V) The Chief Operating Officer of the Office of Federal Student Aid, in order to analyze the use of postsecondary educational benefits provided under this Act.

''(VI) The Commissioner of the Social Security Administration, in order to evaluate labor market outcomes of former postsecondary education students.

''(VII) The Commissioner of the Bureau of Labor Statistics, in order to assess the wages of former postsecondary education students.

''(ii) The heads of Federal agencies and offices described under clause (i) shall enter into data sharing agreements with the Commissioner to ensure secure, periodic data matches as described in this paragraph.

''(B) CATEGORIES OF DATA.—The Commissioner shall, at a minimum, seek to ensure that the secure periodic data system matches described in subparagraph (A) permit consistent reporting of the following categories of data for all postsecondary students:

''(i) Enrollment, retention, transfer, and completion outcomes for all postsecondary students.

''(ii) Financial indicators for postsecondary students receiving Federal grants and loans, including grant and loan aid by source, cumulative student debt, loan repayment status, and repayment plan.

''(iii) Post-completion outcomes for all postsecondary students, including earnings, employment, and further education, by program of study and credential level and as measured—

''(I) immediately after leaving postsecondary education; and

''(II) at time intervals appropriate to the credential sought and earned.

''(C) PERIODIC DATA MATCH STREAMLINING AND CONFIDENTIALITY.—

''(i) STREAMLINING.—In carrying out the secure periodic data system matches under this paragraph, the Commissioner shall—

''(I) ensure that such matches are not continuous, but occur only periodically at appropriate intervals, as determined by the Commissioner to meet the goals of subparagraph (A); and

''(II) seek to—

''(aa) streamline the data collection and reporting requirements for institutions of higher education;

''(bb) minimize duplicative reporting across or within Federal agencies or departments, including reporting requirements applicable to institutions of higher education under the Workforce Innovation and Opportunity Act (29 U.S.C. 3101 et seq.) and the Carl D. Perkins Career and Technical Education Act of 2006;

''(cc) protect student privacy; and

''(dd) streamline the application process for student loan benefit programs available to borrowers based on data available from different Federal data systems.

''(ii) REVIEW.—Not less often than once every 3 years after the establishment of the postsecondary student data system under this subsection, the Commissioner, in consultation with the Advisory Committee, shall review methods for streamlining data collection from institutions of higher education and minimizing duplicative reporting within the Department and across Federal agencies that provide data for the postsecondary student data system.

''(iii) CONFIDENTIALITY.—The Commissioner shall ensure that any periodic matching or sharing of data through periodic data system matches established in accordance with this paragraph—

''(I) complies with the security and privacy protections described in paragraph (1)(C)(iv) and other Federal data protection protocols;

''(II) follows industry best practices commensurate with the sensitivity of specific data elements or metrics;

''(III) does not result in the creation of a single standing, linked Federal database at the Department that maintains the information reported across other Federal agencies; and

''(IV) discloses to postsecondary students what data are included in the data system and periodically matched and how the data are used.

''(iv) CORRECTION.—The Commissioner, in consultation with the Advisory Committee, shall establish a process for students to request access to only their personal information for inspection and request corrections to inaccuracies in a manner that protects the student's personally identifiable information. The Commissioner shall respond in writing to every request for a correction from a student.

''(4) PUBLICLY AVAILABLE INFORMATION.—

''(A) IN GENERAL.—The Commissioner shall make the summary aggregate information described in subparagraph (C), at a minimum, publicly available through a user-friendly consumer information website and analytic tool that—

''(i) provides appropriate mechanisms for users to customize and filter information by institutional and student characteristics;

''(ii) allows users to build summary aggregate reports of information, including reports that allow comparisons across multiple institutions and programs, subject to subparagraph (B);

''(iii) uses appropriate statistical disclosure limitation techniques necessary to ensure that the data released to the public cannot be used to identify specific individuals; and

''(iv) provides users with appropriate contextual factors to make comparisons, which may include national median figures of the summary aggregate information described in subparagraph (C).

''(B) NO PERSONALLY IDENTIFIABLE INFORMATION AVAILABLE.—The summary aggregate information described in this paragraph shall not include personally identifiable information.

''(C) SUMMARY AGGREGATE INFORMATION AVAILABLE.—The summary aggregate information described in this paragraph shall, at a minimum, include each of the following for each institution of higher education:

''(i) Measures of student access, including—

''(I) admissions selectivity and yield; and

''(II) enrollment, disaggregated by each category described in paragraph (2)(C)(ii).

''(ii) Measures of student progression, including retention rates and persistence rates, disaggregated by each category described in paragraph (2)(C)(ii).

''(iii) Measures of student completion, including—

''(I) transfer rates and completion rates, disaggregated by each category described in paragraph (2)(C)(ii); and

''(II) number of completions, disaggregated by each category described in paragraph (2)(C)(ii).

''(iv) Measures of student costs, including—

''(I) tuition, required fees, total cost of attendance, and net price after total grant aid, disaggregated by in-State tuition or in-district tuition status (if applicable), program of study (if applicable), and credential level; and

''(II) typical grant amounts and loan amounts received by students reported separately from Federal, State, local, and institutional sources, and cumulative debt, disaggregated by each category described in paragraph (2)(C)(ii) and completion status.

''(v) Measures of postcollegiate student outcomes, including employment rates, mean and median earnings, loan repayment and default rates, and further education rates. These measures shall—

''(I) be disaggregated by each category described in paragraph (2)(C)(ii) and completion status; and

''(II) be measured immediately after leaving postsecondary education and at time intervals appropriate to the credential sought or earned.

''(D) DEVELOPMENT CRITERIA.—In developing the method and format of making the information described in this paragraph publicly available, the Commissioner shall—

''(i) focus on the needs of the users of the information, which will include students, families of students, potential students, researchers, and other consumers of education data;

''(ii) take into consideration, to the extent practicable, the guidelines described in paragraph (1)(C)(ii)(I), and relevant successor documents or recommendations of such guidelines;

''(iii) use modern, relevant technology and enhance and update the postsecondary student data system with information, as necessary to carry out the purpose of this paragraph;

''(iv) ensure data privacy and security in accordance with standards and guidelines developed by the National Institute of Standards and Technology, and in accordance with any other Federal law relating to privacy or security, including complying with the requirements of subchapter II of chapter 35 of title 44, United States Code, specifying security categorization under the Federal Information Processing Standards, and security requirements, and setting of National Institute of Standards and Technology security baseline controls at the appropriate level; and

''(v) conduct consumer testing to determine how to make the information as meaningful to users as possible.

''(5) PERMISSIBLE DISCLOSURES OF DATA.—

''(A) DATA REPORTS AND QUERIES.—

''(i) IN GENERAL.—Not later than 4 years after the date of enactment of the College Transparency Act, the Commissioner shall develop and implement a secure process for making student-level, non-personally identifiable information, with direct identifiers removed, from the postsecondary student data system available for vetted research and evaluation purposes approved by the Commissioner in a manner compatible with practices for disclosing National Center for Education Statistics restricted-use survey data as in effect on the day before the date of enactment of the College Transparency Act, or by applying other research and disclosure restrictions to ensure data privacy and security. Such process shall be approved by the National Center for Education Statistics' Disclosure Review Board (or successor body).

''(ii) PROVIDING DATA REPORTS AND QUERIES TO INSTITUTIONS AND STATES.—

''(I) IN GENERAL.—The Commissioner shall provide feedback reports, at least annually, to each institution of higher education, each postsecondary education system that fully participates in the postsecondary student data system, and each State higher education body as designated by the governor.

''(II) FEEDBACK REPORTS.—The feedback reports provided under this clause shall include program-level and institution-level information from the postsecondary student data system regarding students who are associated with the institution or, for State representatives, the institutions within that State, on or before the date of the report, on measures including student mobility and workforce outcomes, provided that the feedback aggregate summary reports protect the privacy of individuals.

''(III) DETERMINATION OF CONTENT.—The content of the feedback reports shall be determined by the Commissioner in consultation with the Advisory Committee.

''(iii) PERMITTING STATE DATA QUERIES.—The Commissioner shall, in consultation with the Advisory Committee and as soon as practicable, create a process through which States may submit lists of secondary school graduates within the State to receive summary aggregate outcomes for those students who enrolled at an institution of higher education, including postsecondary enrollment and college completion, provided that those data protect the privacy of individuals and that the State data submitted to the Commissioner are not stored in the postsecondary education system.

''(iv) REGULATIONS.—The Commissioner shall promulgate regulations to ensure fair, secure, and equitable access to data reports and queries under this paragraph.

''(B) DISCLOSURE LIMITATIONS.—In carrying out the public reporting and disclosure requirements of this subsection, the Commissioner shall use appropriate statistical disclosure limitation techniques necessary to ensure that the data released to the public cannot include personally identifiable information or be used to identify specific individuals.

''(C) SALE OF DATA PROHIBITED.—Data collected under this subsection, including the public-use data set and data comprising the summary aggregate information available under paragraph (4), shall not be sold to any third party by the Commissioner, including any institution of higher education or any other entity.

''(D) LIMITATION ON USE BY OTHER FEDERAL AGENCIES.—

''(i) IN GENERAL.—The Commissioner shall not allow any other Federal agency to use data collected under this subsection for any purpose except—

''(I) for vetted research and evaluation conducted by the other Federal agency, as described in subparagraph (A)(i); or

''(II) for a purpose explicitly authorized by this Act.

''(ii) PROHIBITION ON LIMITATION OF SERVICES.—The Secretary, or the head of any other Federal agency, shall not use data collected under this subsection to limit services to students.

''(E) LAW ENFORCEMENT.—Personally identifiable information collected under this subsection shall not be used for any Federal, State, or local law enforcement activity or any other activity that would result in adverse action against any student or a student's family, including debt collection activity or enforcement of immigration laws.

''(F) LIMITATION OF USE FOR FEDERAL RANKINGS OR SUMMATIVE RATING SYSTEM.—The comprehensive data collection and analysis necessary for the postsecondary student data system under this subsection shall not be used by the Secretary or any Federal entity to establish any Federal ranking system of institutions of higher education or a system that results in a summative Federal rating of institutions of higher education.

''(G) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to prevent the use of individual categories of aggregate information to be used for accountability purposes.

''(H) RULE OF CONSTRUCTION REGARDING COMMERCIAL USE OF DATA.—Nothing in this paragraph shall be construed to prohibit third-party entities from using publicly available information in this data system for commercial use.

''(6) SUBMISSION OF DATA.—

''(A) REQUIRED SUBMISSION.—Each institution of higher education participating in a program under title IV, or the assigned agent of such institution, shall, for each eligible program, in accordance with section 487(a)(17), collect, and submit to the Commissioner, the data requested by the Commissioner to carry out this subsection.

''(B) VOLUNTARY SUBMISSION.—Any institution of higher education not participating in a program under title IV may voluntarily participate in the postsecondary student data system under this subsection by collecting and submitting data to the Commissioner, as the Commissioner may request to carry out this subsection.

''(C) PERSONALLY IDENTIFIABLE INFORMATION.—In accordance with paragraph (2)(C)(i), if the submission of an element of student-level data is prohibited under paragraph (2)(F) (or otherwise prohibited by law), the institution of higher education shall submit that data to the Commissioner in the aggregate.

''(7) UNLAWFUL WILLFUL DISCLOSURE.—

''(A) IN GENERAL.—It shall be unlawful for any person who obtains or has access to personally identifiable information in connection with the postsecondary student data system described in this subsection to willfully disclose to any person (except as authorized in this Act or by any Federal law) such personally identifiable information.

''(B) PENALTY.—Any person who violates subparagraph (A) shall be subject to a penalty described under section 3572(f) of title 44, United States Code, and section 183(d)(6) of the Education Sciences Reform Act of 2002 (20 U.S.C. 9573(d)(6)).

''(C) EMPLOYEE OR OFFICER OF THE UNITED STATES.—If a violation of subparagraph (A) is committed by any officer or employee of the United States, the officer or employee shall be dismissed from office or discharged from employment upon conviction for the violation.

''(8) DATA SECURITY.—The Commissioner shall produce and update as needed guidance and regulations relating to privacy, security, and access which shall govern the use and disclosure of data collected in connection with the activities authorized in this subsection. The guidance and regulations developed and reviewed shall protect data from unauthorized access, use, and disclosure, and shall include—

''(A) an audit capability, including mandatory and regularly conducted audits;

''(B) access controls;

''(C) requirements to ensure sufficient data security, quality, validity, and reliability;

''(D) confidentiality protection in accordance with the applicable provisions of subchapter III of chapter 35 of title 44, United States Code;

''(E) appropriate and applicable privacy and security protection, including data retention and destruction protocols and data minimization, in accordance with the most recent Federal standards developed by the National Institute of Standards and Technology; and

''(F) protocols for managing a breach, including breach notifications, in accordance with the standards of National Center for Education Statistics.

''(9) DATA COLLECTION.—The Commissioner shall ensure that data collection, maintenance, and use under this subsection complies with section 552a of title 5, United States Code.

''(10) DEFINITIONS.—In this subsection:

''(A) INSTITUTION OF HIGHER EDUCATION.—The term 'institution of higher education' has the meaning given the term in section 102.

''(B) MINORITY-SERVING INSTITUTION.—The term 'minority-serving institution' means an institution of higher education listed in section 371(a).

''(C) PERSONALLY IDENTIFIABLE INFORMATION.—The term 'personally identifiable information' means personally identifiable information within the meaning of section 444 of the General Education Provisions Act.''.

(c) REPEAL OF PROHIBITION ON STUDENT DATA SYSTEM.—Section 134 of the Higher Education Act of 1965 (20 U.S.C. 1015c) is repealed.

(d) INSTITUTIONAL REQUIREMENTS.—

(1) IN GENERAL.—Paragraph (17) of section 487(a) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)) is amended to read as follows:

''(17) The institution or the assigned agent of the institution will collect and submit data to the Commissioner for Education Statistics in accordance with section 132(l), the nonstudent related surveys within the Integrated Postsecondary Education Data System (IPEDS), or any other Federal institution of higher education data collection effort (as designated by the Secretary), in a timely manner and to the satisfaction of the Secretary.''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect on the date that is 4 years after the date of enactment of this Act.

(e) TRANSITION PROVISIONS.—The Secretary of Education and the Commissioner for Education Statistics shall take such steps as are necessary to ensure that the development and maintenance of the postsecondary student data system required under section 132(l) of the Higher Education Act of 1965, as added by subsection (b) of this section, occurs in a manner that reduces the reporting burden for entities that reported into the Integrated Postsecondary Education Data System (IPEDS).

SA 4799. Mr. PETERS (for himself, Mr. PORTMAN, Mr. WARNER, Ms. COLLINS, Mr. KING, Mr. RUBIO, Mr. RISCH, Ms. ROSEN, Mr. CORNYN, and Mr. BURR) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

SEC. 5101. SHORT TITLE.

This division may be cited as the ''Federal Information Security Modernization Act of 2021''.

SEC. 5102. DEFINITIONS.

In this division, unless otherwise specified:

(1) ADDITIONAL CYBERSECURITY PROCEDURE.—The term ''additional cybersecurity procedure'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this division.

(2) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

(B) the Committee on Oversight and Reform of the House of Representatives; and

(C) the Committee on Homeland Security of the House of Representatives.

(4) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(5) INCIDENT.—The term ''incident'' has the meaning given the term in section 3552(b) of title 44, United States Code.

(6) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given the term in section 3552(b) of title 44, United States Code.

(7) PENETRATION TEST.—The term ''penetration test'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this division.

(8) THREAT HUNTING.—The term ''threat hunting'' means proactively and iteratively searching for threats to systems that evade detection by automated threat detection systems.

TITLE LI—UPDATES TO FISMA

SEC. 5121. TITLE 44 AMENDMENTS.

(a) SUBCHAPTER I AMENDMENTS.—Subchapter I of chapter 35 of title 44, United States Code, is amended—

(1) in section 3504—

(A) in subsection (a)(1)(B)—

(i) by striking clause (v) and inserting the following:

''(v) confidentiality, privacy, disclosure, and sharing of information;'';

(ii) by redesignating clause (vi) as clause (vii); and

(iii) by inserting after clause (v) the following:

''(vi) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, security of information; and''; and

(B) in subsection (g), by striking paragraph (1) and inserting the following:

''(1) develop, and in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and'';

(2) in section 3505—

(A) in paragraph (3) of the first subsection designated as subsection (c)—

(i) in subparagraph (B)—

(I) by inserting ''the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and'' before ''the Comptroller General''; and

(II) by striking ''and'' at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(D) maintained on a continual basis through the use of automation, machine-readable data, and scanning.''; and

(B) by striking the second subsection designated as subsection (c);

(3) in section 3506—

(A) in subsection (b)(1)(C), by inserting '', availability'' after ''integrity''; and

(B) in subsection (h)(3), by inserting ''security,'' after ''efficiency,''; and

(4) in section 3513—

(A) by redesignating subsection (c) as subsection (d); and

(B) by inserting after subsection (b) the following:

''(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.''.

(b) SUBCHAPTER II DEFINITIONS.—

(1) IN GENERAL.—Section 3552(b) of title 44, United States Code, is amended—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), (6), and (7) as paragraphs (2), (3), (4), (5), (6), (9), and (11), respectively;

(B) by inserting before paragraph (2), as so redesignated, the following:

''(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.'';

(C) by inserting after paragraph (6), as so redesignated, the following:

''(7) The term 'high value asset' means information or an information system that the head of an agency determines so critical to the agency that the loss or corruption of the information or the loss of access to the information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

''(8) The term 'major incident' has the meaning given the term in guidance issued by the Director under section 3598(a).'';

(D) by inserting after paragraph (9), as so redesignated, the following:

''(10) The term 'penetration test' means a specialized type of assessment that—

''(A) is conducted on an information system or a component of an information system; and

''(B) emulates an attack or other exploitation capability of a potential adversary, typically under specific constraints, in order to identify any vulnerabilities of an information system or a component of an information system that could be exploited.''; and

(E) by inserting after paragraph (11), as so redesignated, the following:

''(12) The term 'shared service' means a centralized business or mission capability that is provided to multiple organizations within an agency or to multiple agencies.''.

(2) CONFORMING AMENDMENTS.—

(A) HOMELAND SECURITY ACT OF 2002.—Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''.

(B) TITLE 10.—

(i) SECTION 2222.—Section 2222(i)(8) of title 10, United States Code, is amended by striking ''section 3552(b)(6)(A)'' and inserting ''section 3552(b)(9)(A)''.

(ii) SECTION 2223.—Section 2223(c)(3) of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(iii) SECTION 2315.—Section 2315 of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(iv) SECTION 2339A.—Section 2339a(e)(5) of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(C) HIGH-PERFORMANCE COMPUTING ACT OF 1991.—Section 207(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5527(a)) is amended by striking ''section 3552(b)(6)(A)(i)'' and inserting ''section 3552(b)(9)(A)(i)''.

(D) INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 3(5) of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a) is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(E) NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013.—Section 933(e)(1)(B) of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(F) IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011.—The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) is amended—

(i) in section 806(e)(5) (10 U.S.C. 2304 note), by striking ''section 3542(b)'' and inserting ''section 3552(b)'';

(ii) in section 931(b)(3) (10 U.S.C. 2223 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''; and

(iii) in section 932(b)(2) (10 U.S.C. 2224 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(G) E-GOVERNMENT ACT OF 2002.—Section 301(c)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(H) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''; and

(ii) in subsection (f)—

(I) in paragraph (3), by striking ''section 3532(1)'' and inserting ''section 3552(b)''; and

(II) in paragraph (5), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)''.

(c) SUBCHAPTER II AMENDMENTS.—Subchapter II of chapter 35 of title 44, United States Code, is amended—

(1) in section 3551—

(A) in paragraph (4), by striking ''diagnose and improve'' and inserting ''integrate, deliver, diagnose, and improve'';

(B) in paragraph (5), by striking ''and'' at the end;

(C) in paragraph (6), by striking the period at the end and inserting a semi colon; and

(D) by adding at the end the following:

''(7) recognize that each agency has specific mission requirements and, at times, unique cybersecurity requirements to meet the mission of the agency;

''(8) recognize that each agency does not have the same resources to secure agency systems, and an agency should not be expected to have the capability to secure the systems of the agency from advanced adversaries alone; and

''(9) recognize that a holistic Federal cybersecurity model is necessary to account for differences between the missions and capabilities of agencies.'';

(2) in section 3553—

(A) by striking the section heading and inserting ''**Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency**''.

(B) in subsection (a)—

(i) in paragraph (1), by inserting '', in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director,'' before ''overseeing'';

(ii) in paragraph (5), by striking ''and'' at the end; and

(iii) by adding at the end the following:

''(8) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology—

''(A) the use of automation to improve Federal cybersecurity and visibility with respect to the implementation of Federal cybersecurity; and

''(B) the use of presumption of compromise and least privilege principles to improve resiliency and timely response actions to incidents on Federal systems.'';

(C) in subsection (b)—

(i) by striking the subsection heading and inserting ''CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'';

(ii) in the matter preceding paragraph (1), by striking ''The Secretary, in consultation with the Director'' and inserting ''The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and the National Cyber Director'';

(iii) in paragraph (2)—

(I) in subparagraph (A), by inserting ''and reporting requirements under subchapter IV of this title'' after ''section 3556''; and

(II) in subparagraph (D), by striking ''the Director or Secretary'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(iv) in paragraph (5), by striking ''coordinating'' and inserting ''leading the coordination of'';

(v) in paragraph (8), by striking ''the Secretary's discretion'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency's discretion''; and

(vi) in paragraph (9), by striking ''as the Director or the Secretary, in consultation with the Director,'' and inserting ''as the Director of the Cybersecurity and Infrastructure Security Agency'';

(D) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking ''each year'' and inserting ''each year during which agencies are required to submit reports under section 3554(c)'';

(ii) by striking paragraph (1);

(iii) by redesignating paragraphs (2), (3), and (4) as paragraphs (1), (2), and (3), respectively;

(iv) in paragraph (3), as so redesignated, by striking ''and'' at the end;

(v) by inserting after paragraph (3), as so redesignated the following:

''(4) a summary of each assessment of Federal risk posture performed under subsection (i);''; and

(vi) in paragraph (5), by striking the period at the end and inserting ''; and'';

(E) by redesignating subsections (i), (j), (k), and (l) as subsections (j), (k), (l), and (m) respectively;

(F) by inserting after subsection (h) the following:

''(i) FEDERAL RISK ASSESSMENTS.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall perform assessments of Federal risk posture using any available information on the cybersecurity posture of agencies, and brief the Director and National Cyber Director on the findings of those assessments including—

''(1) the status of agency cybersecurity remedial actions described in section 3554(b)(7);

''(2) any vulnerability information relating to the systems of an agency that is known by the agency;

''(3) analysis of incident information under section 3597;

''(4) evaluation of penetration testing performed under section 3559A;

''(5) evaluation of vulnerability disclosure program information under section 3559B;

''(6) evaluation of agency threat hunting results;

''(7) evaluation of Federal and non-Federal cyber threat intelligence;

''(8) data on agency compliance with standards issued under section 11331 of title 40;

''(9) agency system risk assessments performed under section 3554(a)(1)(A); and

''(10) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant.''; and

(G) in subsection (j), as so redesignated—

(i) by striking ''regarding the specific'' and inserting ''that includes a summary of—

''(1) the specific'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and'' and

(iii) by adding at the end the following:

''(2) the trends identified in the Federal risk assessment performed under subsection (i).''; and

(H) by adding at the end the following:

''(n) BINDING OPERATIONAL DIRECTIVES.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emergency directive under this section, not later than 2 days after the date on which the binding operational directive requires an agency to take an action, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate reporting entities the status of the implementation of the binding operational directive at the agency.'';

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by redesignating subparagraphs (A), (B), and (C) as subparagraphs (B), (C), and (D), respectively;

(II) by inserting before subparagraph (B), as so redesignated, the following:

''(A) on an ongoing and continuous basis, performing agency system risk assessments that—

''(i) identify and document the high value assets of the agency using guidance from the Director;

''(ii) evaluate the data assets inventoried under section 3511 for sensitivity to compromises in confidentiality, integrity, and availability;

''(iii) identify agency systems that have access to or hold the data assets inventoried under section 3511;

''(iv) evaluate the threats facing agency systems and data, including high value assets, based on Federal and non-Federal cyber threat intelligence products, where available;

''(v) evaluate the vulnerability of agency systems and data, including high value assets, including by analyzing—

''(I) the results of penetration testing performed by the Department of Homeland Security under section 3553(b)(9);

''(II) the results of penetration testing performed under section 3559A;

''(III) information provided to the agency through the vulnerability disclosure program of the agency under section 3559B;

''(IV) incidents; and

''(V) any other vulnerability information relating to agency systems that is known to the agency;

''(vi) assess the impacts of potential agency incidents to agency systems, data, and operations based on the evaluations described in clauses (ii) and (iv) and the agency systems identified under clause (iii); and

''(vii) assess the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or operational reliance on the operations of the system or data in the system;'';

(III) in subparagraph (B), as so redesignated, in the matter preceding clause (i), by striking ''providing information'' and inserting ''using information from the assessment conducted under subparagraph (A), providing, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, information'';

(IV) in subparagraph (C), as so redesignated—

(aa) in clause (ii) by inserting ''binding'' before ''operational''; and

(bb) in clause (vi), by striking ''and'' at the end; and

(V) by adding at the end the following:

''(E) providing an update on the ongoing and continuous assessment performed under subparagraph (A)—

''(i) upon request, to the inspector general of the agency or the Comptroller General of the United States; and

''(ii) on a periodic basis, as determined by guidance issued by the Director but not less frequently than annually, to—

''(I) the Director;

''(II) the Director of the Cybersecurity and Infrastructure Security Agency; and

''(III) the National Cyber Director;

''(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than once every 3 years, performing an evaluation of whether additional cybersecurity procedures are appropriate for securing a system of, or under the supervision of, the agency, which shall—

''(i) be completed considering the agency system risk assessment performed under subparagraph (A); and

''(ii) include a specific evaluation for high value assets;

''(G) not later than 30 days after completing the evaluation performed under subparagraph (F), providing the evaluation and an implementation plan, if applicable, for using additional cybersecurity procedures determined to be appropriate to—

''(i) the Director of the Cybersecurity and Infrastructure Security Agency;

''(ii) the Director; and

''(iii) the National Cyber Director; and

''(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency in accordance with the risk-based cyber budget model developed pursuant to section 3553(a)(7);'';

(ii) in paragraph (2)—

(I) in subparagraph (A), by inserting ''in accordance with the agency system risk assessment performed under paragraph (1)(A)'' after ''information systems'';

(II) in subparagraph (B)—

(aa) by striking ''in accordance with standards'' and inserting ''in accordance with—

''(i) standards''; and

(bb) by adding at the end the following:

''(ii) the evaluation performed under paragraph (1)(F); and

''(iii) the implementation plan described in paragraph (1)(G);''; and

(III) in subparagraph (D), by inserting '', through the use of penetration testing, the vulnerability disclosure program established under section 3559B, and other means,'' after ''periodically'';

(iii) in paragraph (3)—

(I) in subparagraph (A)—

(aa) in clause (iii), by striking ''and'' at the end;

(bb) in clause (iv), by adding ''and'' at the end; and

(cc) by adding at the end the following:

''(v) ensure that—

''(I) senior agency information security officers of component agencies carry out responsibilities under this subchapter, as directed by the senior agency information security officer of the agency or an equivalent official; and

''(II) senior agency information security officers of component agencies report to—

''(aa) the senior information security officer of the agency or an equivalent official; and

''(bb) the Chief Information Officer of the component agency or an equivalent official;''; and

(iv) in paragraph (5), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' before ''on the effectiveness'';

(B) in subsection (b)—

(i) by striking paragraph (1) and inserting the following:

''(1) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk assessments, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11331 of title 40, as applicable;'';

(ii) in paragraph (2)—

(I) by striking subparagraph (B) and inserting the following:

''(B) comply with the risk-based cyber budget model developed pursuant to section 3553(a)(7);''; and

(II) in subparagraph (D)—

(aa) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively;

(bb) by inserting after clause (ii) the following:

''(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under section 3553;''; and

(cc) in clause (iv), as so redesignated, by striking ''as determined by the agency; and'' and inserting ''as determined by the agency, considering—

''(I) the agency risk assessment performed under subsection (a)(1)(A); and

''(II) the determinations of applying more stringent standards and additional cybersecurity procedures pursuant to section 11331(c)(1) of title 40; and'';

(iii) in paragraph (5)(A), by inserting '', including penetration testing, as appropriate,'' after ''shall include testing'';

(iv) in paragraph (6), by striking ''planning, implementing, evaluating, and documenting'' and inserting ''planning and implementing and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, evaluating and documenting'';

(v) by redesignating paragraphs (7) and (8) as paragraphs (8) and (9), respectively;

(vi) by inserting after paragraph (6) the following:

''(7) a process for providing the status of every remedial action and known system vulnerability to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;''; and

(vii) in paragraph (8)(C), as so redesignated—

(I) by striking clause (ii) and inserting the following:

''(ii) notifying and consulting with the Federal information security incident center established under section 3556 pursuant to the requirements of section 3594;'';

(II) by redesignating clause (iii) as clause (iv);

(III) by inserting after clause (ii) the following:

''(iii) performing the notifications and other activities required under subchapter IV of this title; and''; and

(IV) in clause (iv), as so redesignated—

(aa) in subclause (I), by striking ''and relevant offices of inspectors general'';

(bb) in subclause (II), by adding ''and'' at the end;

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III);

(C) in subsection (c)—

(i) by redesignating paragraph (2) as paragraph (5);

(ii) by striking paragraph (1) and inserting the following:

''(1) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment under subsection (a)(1)(A), the head of each agency shall submit to the Director, the Director of the Cybersecurity and Infrastructure Security Agency, the majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

''(A) summarizes the agency system risk assessment performed under subsection (a)(1)(A);

''(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the agency system risk assessment performed under subsection (a)(1)(A), including an analysis of the agency's cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

''(C) summarizes the evaluation and implementation plans described in subparagraphs (F) and (G) of subsection (a)(1) and whether those evaluation and implementation plans call for the use of additional cybersecurity procedures determined to be appropriate by the agency; and

''(D) summarizes the status of remedial actions identified by inspector general of the agency, the Comptroller General of the United States, and any other source determined appropriate by the head of the agency.

''(2) UNCLASSIFIED REPORTS.—Each report submitted under paragraph (1)—

''(A) shall be, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

''(B) may include a classified annex.

''(3) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified form of the report submitted by the agency under paragraph (2)(A).

''(4) BRIEFINGS.—During each year during which a report is not required to be submitted under paragraph (1), the Director shall provide to the congressional committees described in paragraph (1) a briefing summarizing current agency and Federal risk postures.''; and

(iii) in paragraph (5), as so redesignated, by striking the period at the end and inserting '', including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section.''; and

(D) in subsection (d)(1), in the matter preceding subparagraph (A), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' after ''the Director''; and

(4) in section 3555—

(A) in the section heading, by striking ''**ANNUAL INDEPENDENT**'' and inserting ''**INDEPENDENT**'';

(B) in subsection (a)—

(i) in paragraph (1), by inserting ''during which a report is required to be submitted under section 3553(c),'' after ''Each year'';

(ii) in paragraph (2)(A), by inserting '', including by penetration testing and analyzing the vulnerability disclosure program of the agency'' after ''information systems''; and

(iii) by adding at the end the following:

''(3) An evaluation under this section may include recommendations for improving the cybersecurity posture of the agency.'';

(C) in subsection (b)(1), by striking ''annual'';

(D) in subsection (e)(1), by inserting ''during which a report is required to be submitted under section 3553(c)'' after ''Each year'';

(E) by striking subsection (f) and inserting the following:

''(f) PROTECTION OF INFORMATION.—(1) Agencies, evaluators, and other recipients of information that, if disclosed, may cause grave harm to the efforts of Federal information security officers shall take appropriate steps to ensure the protection of that information, including safeguarding the information from public disclosure.

''(2) The protections required under paragraph (1) shall be commensurate with the risk and comply with all applicable laws and regulations.

''(3) With respect to information that is not related to national security systems, agencies and evaluators shall make a summary of the information unclassified and publicly available, including information that does not identify—

''(A) specific information system incidents; or

''(B) specific information system vulnerabilities.'';

(F) in subsection (g)(2)—

(i) by striking ''this subsection shall'' and inserting ''this subsection—

''(A) shall'';

(ii) in subparagraph (A), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(B) identify any entity that performs an independent evaluation under subsection (b).''; and

(G) by striking subsection (j) and inserting the following:

''(j) GUIDANCE.—

''(1) IN GENERAL.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices

''(2) PRIORITIES.—The guidance developed under paragraph (1) shall prioritize the identification of—

''(A) the most common threat patterns experienced by each agency;

''(B) the security controls that address the threat patterns described in subparagraph (A); and

''(C) any other security risks unique to the networks of each agency.''; and

(5) in section 3556(a)—

(A) in the matter preceding paragraph (1), by inserting ''within the Cybersecurity and Infrastructure Security Agency'' after ''incident center''; and

(B) in paragraph (4), by striking ''3554(b)'' and inserting ''3554(a)(1)(A)''.

(d) CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended—

(A) by striking the item relating to section 3553 and inserting the following:

''3553. Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency.''; and

(B) by striking the item relating to section 3555 and inserting the following:

''3555. Independent evaluation.''.

(2) OMB REPORTS.—Section 226(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1524(c)) is amended—

(A) in paragraph (1)(B), in the matter preceding clause (i), by striking ''annually thereafter'' and inserting ''thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code''; and

(B) in paragraph (2)(B), in the matter preceding clause (i)—

(i) by striking ''annually thereafter'' and inserting ''thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code''; and

(ii) by striking ''the report required under section 3553(c) of title 44, United States Code'' and inserting ''that report''.

(3) NIST RESPONSIBILITIES.—Section 20(d)(3)(B) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is amended by striking ''annual''.

(e) FEDERAL SYSTEM INCIDENT RESPONSE.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

''§ 3591. Definitions

''(a) IN GENERAL.—Except as provided in subsection (b), the definitions under sections 3502 and 3552 shall apply to this subchapter.

''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

''(1) APPROPRIATE REPORTING ENTITIES.—The term 'appropriate reporting entities' means—

''(A) the majority and minority leaders of the Senate;

''(B) the Speaker and minority leader of the House of Representatives;

''(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(D) the Committee on Oversight and Reform of the House of Representatives;

''(E) the Committee on Homeland Security of the House of Representatives;

''(F) the appropriate authorization and appropriations committees of Congress;

''(G) the Director;

''(H) the Director of the Cybersecurity and Infrastructure Security Agency;

''(I) the National Cyber Director;

''(J) the Comptroller General of the United States; and

''(K) the inspector general of any impacted agency.

''(2) AWARDEE.—The term 'awardee'—

''(A) means a person, business, or other entity that receives a grant from, or is a party to a cooperative agreement or an other transaction agreement with, an agency; and

''(B) includes any subgrantee of a person, business, or other entity described in subparagraph (A).

''(3) BREACH.—The term 'breach' means—

''(A) a compromise of the security, confidentiality, or integrity of data in electronic form that results in unauthorized access to, or an acquisition of, personal information; or

''(B) a loss of data in electronic form that results in unauthorized access to, or an acquisition of, personal information.

''(4) CONTRACTOR.—The term 'contractor' means—

''(A) a prime contractor of an agency or a subcontractor of a prime contractor of an agency; and

''(B) any person or business that collects or maintains information, including personally identifiable information, on behalf of an agency.

''(5) FEDERAL INFORMATION.—The term 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government in any medium or form.

''(6) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an agency, a contractor, an awardee, or another organization on behalf of an agency.

''(7) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(8) NATIONWIDE CONSUMER REPORTING AGENCY.—The term 'nationwide consumer reporting agency' means a consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

''(9) VULNERABILITY DISCLOSURE.—The term 'vulnerability disclosure' means a vulnerability identified under section 3559B.

''§ 3592. Notification of breach

''(a) NOTIFICATION.—As expeditiously as practicable and without unreasonable delay, and in any case not later than 45 days after an agency has a reasonable basis to conclude that a breach has occurred, the head of the agency, in consultation with a senior privacy officer of the agency, shall—

''(1) determine whether notice to any individual potentially affected by the breach is appropriate based on an assessment of the risk of harm to the individual that considers—

''(A) the nature and sensitivity of the personally identifiable information affected by the breach;

''(B) the likelihood of access to and use of the personally identifiable information affected by the breach;

''(C) the type of breach; and

''(D) any other factors determined by the Director; and

''(2) as appropriate, provide written notice in accordance with subsection (b) to each individual potentially affected by the breach—

''(A) to the last known mailing address of the individual; or

''(B) through an appropriate alternative method of notification that the head of the agency or a designated senior-level individual of the agency selects based on factors determined by the Director.

''(b) CONTENTS OF NOTICE.—Each notice of a breach provided to an individual under subsection (a)(2) shall include—

''(1) a brief description of the rationale for the determination that notice should be provided under subsection (a);

''(2) if possible, a description of the types of personally identifiable information affected by the breach;

''(3) contact information of the agency that may be used to ask questions of the agency, which—

''(A) shall include an e-mail address or another digital contact mechanism; and

''(B) may include a telephone number or a website;

''(4) information on any remedy being offered by the agency;

''(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affects their personally identifiable information, including relevant contact information for Federal law enforcement agencies and each nationwide consumer reporting agency; and

''(6) any other appropriate information, as determined by the head of the agency or established in guidance by the Director.

''(c) DELAY OF NOTIFICATION.—

''(1) IN GENERAL.—The Attorney General, the Director of National Intelligence, or the Secretary of Homeland Security may delay a notification required under subsection (a) if the notification would—

''(A) impede a criminal investigation or a national security activity;

''(B) reveal sensitive sources and methods;

''(C) cause damage to national security; or

''(D) hamper security remediation actions.

''(2) DOCUMENTATION.—

''(A) IN GENERAL.—Any delay under paragraph (1) shall be reported in writing to the Director, the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

''(B) CONTENTS.—A report required under subparagraph (A) shall include a written statement from the entity that delayed the notification explaining the need for the delay.

''(C) FORM.—The report required under subparagraph (A) shall be unclassified but may include a classified annex.

''(3) RENEWAL.—A delay under paragraph (1) shall be for a period of 60 days and may be renewed.

''(d) UPDATE NOTIFICATION.—If an agency determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination made under subsection (a)(1), or that it is necessary to update the details of the information provided to impacted individuals as described in subsection (b), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

''(e) EXEMPTION FROM NOTIFICATION.—

''(1) IN GENERAL.—The head of an agency, in consultation with the inspector general of the agency, may request an exemption from the Director from complying with the notification requirements under subsection (a) if the information affected by the breach is determined by an independent evaluation to be unreadable, including, as appropriate, instances in which the information is—

''(A) encrypted; and

''(B) determined by the Director of the Cybersecurity and Infrastructure Security Agency to be of sufficiently low risk of exposure.

''(2) APPROVAL.—The Director shall determine whether to grant an exemption requested under paragraph (1) in consultation with—

''(A) the Director of the Cybersecurity and Infrastructure Security Agency; and

''(B) the Attorney General.

''(3) DOCUMENTATION.—Any exemption granted by the Director under paragraph (1) shall be reported in writing to the head of the agency and the inspector general of the agency that experienced the breach and the Director of the Cybersecurity and Infrastructure Security Agency.

''(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

''(1) the Director from issuing guidance relating to notifications or the head of an agency from notifying individuals potentially affected by breaches that are not determined to be major incidents; or

''(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when notifying individuals potentially affected by breaches.

''§ 3593. Congressional and Executive Branch reports

''(a) INITIAL REPORT.—

''(1) IN GENERAL.—Not later than 72 hours after an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency impacted by the major incident shall submit to the appropriate reporting entities a written report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the appropriate authorization and appropriations committees of Congress, taking into account—

''(A) the information known at the time of the report;

''(B) the sensitivity of the details associated with the major incident; and

''(C) the classification level of the information contained in the report.

''(2) CONTENTS.—A report required under paragraph (1) shall include, in a manner that excludes or otherwise reasonably protects personally identifiable information and to the extent permitted by applicable law, including privacy and statistical laws—

''(A) a summary of the information available about the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

''(B) if applicable, a description and any associated documentation of any circumstances necessitating a delay in or exemption to notification to individuals potentially affected by the major incident under subsection (c) or (e) of section 3592; and

''(C) if applicable, an assessment of the impacts to the agency, the Federal Government, or the security of the United States, based on information available to agency officials on the date on which the agency submits the report.

''(b) SUPPLEMENTAL REPORT.—Within a reasonable amount of time, but not later than 30 days after the date on which an agency submits a written report under subsection (a), the head of the agency shall provide to the appropriate reporting entities written updates on the major incident and, to the extent practicable, provide a briefing to the congressional committees described in subsection (a)(1), including summaries of—

''(1) vulnerabilities, means by which the major incident occurred, and impacts to the agency relating to the major incident;

''(2) any risk assessment and subsequent risk-based security implementation of the affected information system before the date on which the major incident occurred;

''(3) the status of compliance of the affected information system with applicable security requirements at the time of the major incident;

''(4) an estimate of the number of individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

''(5) an assessment of the risk of harm to individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

''(6) an update to the assessment of the risk to agency operations, or to impacts on other agency or non-Federal entity operations, affected by the major incident based on information available to agency officials as of the date on which the agency provides the update; and

''(7) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d) and status updates on the notification process described in section 3592(a), including any delay or exemption described in subsection (c) or (e), respectively, of section 3592, if applicable.

''(c) UPDATE REPORT.—If the agency determines that there is any significant change in the understanding of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities that includes information relating to the change in understanding.

''(d) ANNUAL REPORT.—Each agency shall submit as part of the annual report required under section 3554(c)(1) of this title a description of each major incident that occurred during the 1-year period preceding the date on which the report is submitted.

''(e) DELAY AND EXEMPTION REPORT.—

''(1) IN GENERAL.—The Director shall submit to the appropriate notification entities an annual report on all notification delays and exemptions granted pursuant to subsections (c) and (d) of section 3592.

''(2) COMPONENT OF OTHER REPORT.—The Director may submit the report required under paragraph (1) as a component of the annual report submitted under section 3597(b).

''(f) REPORT DELIVERY.—Any written report required to be submitted under this section may be submitted in a paper or electronic format.

''(g) THREAT BRIEFING.—

''(1) IN GENERAL.—Not later than 7 days after the date on which an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency, jointly with the National Cyber Director and any other Federal entity determined appropriate by the National Cyber Director, shall provide a briefing to the congressional committees described in subsection (a)(1) on the threat causing the major incident.

''(2) COMPONENTS.—The briefing required under paragraph (1)—

''(A) shall, to the greatest extent practicable, include an unclassified component; and

''(B) may include a classified component.

''(h) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

''(1) the ability of an agency to provide additional reports or briefings to Congress; or

''(2) Congress from requesting additional information from agencies through reports, briefings, or other means.

''§ 3594. Government information sharing and incident response

''(a) IN GENERAL.—

''(1) INCIDENT REPORTING.—The head of each agency shall provide any information relating to any incident, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget.

''(2) CONTENTS.—A provision of information relating to an incident made by the head of an agency under paragraph (1) shall—

''(A) include detailed information about the safeguards that were in place when the incident occurred;

''(B) whether the agency implemented the safeguards described in subparagraph (A) correctly;

''(C) in order to protect against a similar incident, identify—

''(i) how the safeguards described in subparagraph (A) should be implemented differently; and

''(ii) additional necessary safeguards; and

''(D) include information to aid in incident response, such as—

''(i) a description of the affected systems or networks;

''(ii) the estimated dates of when the incident occurred; and

''(iii) information that could reasonably help identify the party that conducted the incident.

''(3) INFORMATION SHARING.—To the greatest extent practicable, the Director of the Cybersecurity and Infrastructure Security Agency shall share information relating to an incident with any agencies that may be impacted by the incident.

''(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems with the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

''(b) COMPLIANCE.—The information provided under subsection (a) shall take into account the level of classification of the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director

''(c) INCIDENT RESPONSE.—Each agency that has a reasonable basis to conclude that a major incident occurred involving Federal information in electronic medium or form, as defined by the Director and not involving a national security system, regardless of delays from notification granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency regarding—

''(1) incident response and recovery; and

''(2) recommendations for mitigating future incidents.

''§ 3595. Responsibilities of contractors and awardees

''(a) NOTIFICATION.—

''(1) IN GENERAL.—Unless otherwise specified in a contract, grant, cooperative agreement, or an other transaction agreement, any contractor or awardee of an agency shall report to the agency within the same amount of time such agency is required to report an incident to the Cybersecurity and Infrastructure Security Agency, if the contractor or awardee has a reasonable basis to conclude that—

''(A) an incident or breach has occurred with respect to Federal information collected, used, or maintained by the contractor or awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee;

''(B) an incident or breach has occurred with respect to a Federal information system used or operated by the contractor or awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee; or

''(C) the contractor or awardee has received information from the agency that the contractor or awardee is not authorized to receive in connection with the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee.

''(2) PROCEDURES.—

''(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under paragraph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

''(B) INCIDENT.—Following a report of an incident by a contractor or awardee under paragraph (1), an agency, in consultation with the contractor or awardee, shall carry out the requirements under section 3594 with respect to the incident.

''(b) EFFECTIVE DATE.—This section shall apply on and after the date that is 1 year after the date of enactment of the Federal Information Security Modernization Act of 2021.

''§ 3596. Training

''(a) COVERED INDIVIDUAL DEFINED.—In this section, the term 'covered individual' means an individual who obtains access to Federal information or Federal information systems because of the status of the individual as an employee, contractor, awardee, volunteer, or intern of an agency.

''(b) REQUIREMENT.—The head of each agency shall develop training for covered individuals on how to identify and respond to an incident, including—

''(1) the internal process of the agency for reporting an incident; and

''(2) the obligation of a covered individual to report to the agency a confirmed major incident and any suspected incident involving information in any medium or form, including paper, oral, and electronic.

''(c) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (b) may be included as part of an annual privacy or security awareness training of an agency.

''§ 3597. Analysis and report on Federal incidents

''(a) ANALYSIS OF FEDERAL INCIDENTS.—

''(1) QUANTITATIVE AND QUALITATIVE ANALYSES.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop, in consultation with the Director and the National Cyber Director, and perform continuous monitoring and quantitative and qualitative analyses of incidents at agencies, including major incidents, including—

''(A) the causes of incidents, including—

''(i) attacker tactics, techniques, and procedures; and

''(ii) system vulnerabilities, including zero days, unpatched systems, and information system misconfigurations;

''(B) the scope and scale of incidents at agencies;

''(C) cross Federal Government root causes of incidents at agencies;

''(D) agency incident response, recovery, and remediation actions and the effectiveness of those actions, as applicable;

''(E) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

''(F) trends in cross-Federal Government cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

''(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the greatest extent practicable, use machine readable data, automation, and machine learning processes.

''(3) SHARING OF DATA AND ANALYSIS.—

''(A) IN GENERAL.—The Director shall share on an ongoing basis the analyses required under this subsection with agencies and the National Cyber Director to—

''(i) improve the understanding of cybersecurity risk of agencies; and

''(ii) support the cybersecurity improvement efforts of agencies.

''(B) FORMAT.—In carrying out subparagraph (A), the Director shall share the analyses—

''(i) in human-readable written products; and

''(ii) to the greatest extent practicable, in machine-readable formats in order to enable automated intake and use by agencies.

''(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and other Federal agencies as appropriate, shall submit to the appropriate notification entities a report that includes—

''(1) a summary of causes of incidents from across the Federal Government that categorizes those incidents as incidents or major incidents;

''(2) the quantitative and qualitative analyses of incidents developed under subsection (a)(1) on an agency-by-agency basis and comprehensively across the Federal Government, including—

''(A) a specific analysis of breaches; and

''(B) an analysis of the Federal Government's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)); and

''(3) an annex for each agency that includes—

''(A) a description of each major incident;

''(B) the total number of compromises of the agency; and

''(C) an analysis of the agency's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

''(c) PUBLICATION.—A version of each report submitted under subsection (b) shall be made publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year in which the report is submitted.

''(d) INFORMATION PROVIDED BY AGENCIES.—

''(1) IN GENERAL.—The analysis required under subsection (a) and each report submitted under subsection (b) shall use information provided by agencies under section 3594(a).

''(2) NONCOMPLIANCE REPORTS.—

''(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident to the Cybersecurity and Infrastructure Security Agency in accordance with section 3594(a), the head of the agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes—

''(i) data for the incident; and

''(ii) the information described in subsection (b) with respect to the agency.

''(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident that occurs on a national security system in any report submitted under subparagraph (A).

''(3) NATIONAL SECURITY SYSTEM REPORTS.—

''(A) IN GENERAL.—Annually, the head of an agency that operates or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the agency to the extent that the submission is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President to—

''(i) the majority and minority leaders of the Senate,

''(ii) the Speaker and minority leader of the House of Representatives;

''(iii) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(iv) the Select Committee on Intelligence of the Senate;

''(v) the Committee on Armed Services of the Senate;

''(vi) the Committee on Appropriations of the Senate;

''(vii) the Committee on Oversight and Reform of the House of Representatives;

''(viii) the Committee on Homeland Security of the House of Representatives;

''(ix) the Permanent Select Committee on Intelligence of the House of Representatives;

''(x) the Committee on Armed Services of the House of Representatives; and

''(xi) the Committee on Appropriations of the House of Representatives.

''(B) CLASSIFIED FORM.—A report required under subparagraph (A) may be submitted in a classified form.

''(e) REQUIREMENT FOR COMPILING INFORMATION.—In publishing the public report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the impacted agency.

''§ 3598. Major incident definition

''(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall develop and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

''(b) REQUIREMENTS.—With respect to the guidance issued under subsection (a), the definition of the term 'major incident' shall—

''(1) include, with respect to any information collected or maintained by or on behalf of an agency or an information system used or operated by an agency or by a contractor of an agency or another organization on behalf of an agency—

''(A) any incident the head of the agency determines is likely to have an impact on—

''(i) the national security, homeland security, or economic security of the United States; or

''(ii) the civil liberties or public health and safety of the people of the United States;

''(B) any incident the head of the agency determines likely to result in an inability for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services;

''(C) any incident that the head of an agency, in consultation with a senior privacy officer of the agency, determines is likely to have a significant privacy impact on 1 or more individual;

''(D) any incident that the head of the agency, in consultation with a senior privacy official of the agency, determines is likely to have a substantial privacy impact on a significant number of individuals;

''(E) any incident the head of the agency determines impacts the operations of a high value asset owned or operated by the agency;

''(F) any incident involving the exposure of sensitive agency information to a foreign entity, such as the communications of the head of the agency, the head of a component of the agency, or the direct reports of the head of the agency or the head of a component of the agency; and

''(G) any other type of incident determined appropriate by the Director;

''(2) stipulate that the National Cyber Director shall declare a major incident at each agency impacted by an incident if the Director of the Cybersecurity and Infrastructure Security Agency determines that an incident—

''(A) occurs at not less than 2 agencies; and

''(B) is enabled by—

''(i) a common technical root cause, such as a supply chain compromise, a common software or hardware vulnerability; or

''(ii) the related activities of a common threat actor; and

''(3) stipulate that, in determining whether an incident constitutes a major incident because that incident—

''(A) is any incident described in paragraph (1), the head of an agency shall consult with the Director of the Cybersecurity and Infrastructure Security Agency;

''(B) is an incident described in paragraph (1)(A), the head of the agency shall consult with the National Cyber Director; and

''(C) is an incident described in subparagraph (C) or (D) of paragraph (1), the head of the agency shall consult with—

''(i) the Privacy and Civil Liberties Oversight Board; and

''(ii) the Chair of the Federal Trade Commission.

''(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In determining what constitutes a significant number of individuals under subsection (b)(1)(D), the Director—

''(1) may determine a threshold for a minimum number of individuals that constitutes a significant amount; and

''(2) may not determine a threshold described in paragraph (1) that exceeds 5,000 individuals.

''(d) EVALUATION AND UPDATES.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, and not less frequently than every 2 years thereafter, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evaluation, which shall include—

''(1) an update, if necessary, to the guidance issued under subsection (a);

''(2) the definition of the term 'major incident' included in the guidance issued under subsection (a); and

''(3) an explanation of, and the analysis that led to, the definition described in paragraph (2).''.

(2) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

''3591. Definitions.
''3592. Notification of breach.
''3593. Congressional and Executive Branch reports.
''3594. Government information sharing and incident response.
''3595. Responsibilities of contractors and awardees.
''3596. Training.
''3597. Analysis and report on Federal incidents.
''3598. Major incident definition.''.

SEC. 5122. AMENDMENTS TO SUBTITLE III OF TITLE 40.

(a) MODERNIZING GOVERNMENT TECHNOLOGY.—Subtitle G of title X of Division A of the National Defense Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note) is amended—

(1) in section 1077(b)—

(A) in paragraph (5)(A), by inserting ''improving the cybersecurity of systems and'' before ''cost savings activities''; and

(B) in paragraph (7)—

(i) in the paragraph heading, by striking ''CIO'' and inserting ''CIO'';

(ii) by striking ''In evaluating projects'' and inserting the following:

''(A) CONSIDERATION OF GUIDANCE.—In evaluating projects'';

(iii) in subparagraph (A), as so designated, by striking ''under section 1094(b)(1)'' and inserting ''by the Director''; and

(iv) by adding at the end the following:

''(B) CONSULTATION.—In using funds under paragraph (3)(A), the Chief Information Officer of the covered agency shall consult with the necessary stakeholders to ensure the project appropriately addresses cybersecurity risks, including the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate.''; and

(2) in section 1078—

(A) by striking subsection (a) and inserting the following:

''(a) DEFINITIONS.—In this section:

''(1) AGENCY.—The term 'agency' has the meaning given the term in section 551 of title 5, United States Code.

''(2) HIGH VALUE ASSET.—The term 'high value asset' has the meaning given the term in section 3552 of title 44, United States Code.'';

(B) in subsection (b), by adding at the end the following:

''(8) PROPOSAL EVALUATION.—The Director shall—

''(A) give consideration for the use of amounts in the Fund to improve the security of high value assets; and

''(B) require that any proposal for the use of amounts in the Fund includes a cybersecurity plan, including a supply chain risk management plan, to be reviewed by the member of the Technology Modernization Board described in subsection (c)(5)(C).''; and

(C) in subsection (c)—

(i) in paragraph (2)(A)(i), by inserting '', including a consideration of the impact on high value assets'' after ''operational risks'';

(ii) in paragraph (5)—

(I) in subparagraph (A), by striking ''and'' at the end;

(II) in subparagraph (B), by striking the period at the end and inserting ''and''; and

(III) by adding at the end the following:

''(C) a senior official from the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, appointed by the Director.''; and

(iii) in paragraph (6)(A), by striking ''shall be—'' and all that follows through ''4 employees'' and inserting ''shall be 4 employees''.

(b) SUBCHAPTER I.—Subchapter I of subtitle III of title 40, United States Code, is amended—

(1) in section 11302—

(A) in subsection (b), by striking ''use, security, and disposal of'' and inserting ''use, and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, promote and improve the security of,'';

(B) in subsection (c)—

(i) in paragraph (3)—

(I) in subparagraph (A)—

(aa) by striking ''including data'' and inserting ''which shall—

''(i) include data'';

(bb) in clause (i), as so designated, by striking '', and performance'' and inserting ''security, and performance; and''; and

(cc) by adding at the end the following:

''(ii) specifically denote cybersecurity funding under the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44.''; and

(II) in subparagraph (B), adding at the end the following:

''(iii) The Director shall provide to the National Cyber Director any cybersecurity funding information described in subparagraph (A)(ii) that is provided to the Director under clause (ii) of this subparagraph.''; and

(ii) in paragraph (4)(B), in the matter preceding clause (i), by inserting ''not later than 30 days after the date on which the review under subparagraph (A) is completed,'' before ''the Administrator'';

(C) in subsection (f)—

(i) by striking ''heads of executive agencies to develop'' and inserting ''heads of executive agencies to—

''(1) develop'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(2) consult with the Director of the Cybersecurity and Infrastructure Security Agency for the development and use of supply chain security best practices.''; and

(D) in subsection (h), by inserting '', including cybersecurity performances,'' after ''the performances''; and

(2) in section 11303(b)—

(A) in paragraph (2)(B)—

(i) in clause (i), by striking ''or'' at the end;

(ii) in clause (ii), by adding ''or'' at the end; and

(iii) by adding at the end the following:

''(iii) whether the function should be performed by a shared service offered by another executive agency;''; and

(B) in paragraph (5)(B)(i), by inserting '', while taking into account the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44'' after ''title 31''.

(c) SUBCHAPTER II.—Subchapter II of subtitle III of title 40, United States Code, is amended—

(1) in section 11312(a), by inserting '', including security risks'' after ''managing the risks'';

(2) in section 11313(1), by striking ''efficiency and effectiveness'' and inserting ''efficiency, security, and effectiveness'';

(3) in section 11315, by adding at the end the following:

''(d) COMPONENT AGENCY CHIEF INFORMATION OFFICERS.—The Chief Information Officer or an equivalent official of a component agency shall report to—

''(1) the Chief Information Officer designated under section 3506(a)(2) of title 44 or an equivalent official of the agency of which the component agency is a component; and

''(2) the head of the component agency.'';

(4) in section 11317, by inserting ''security,'' before ''or schedule''; and

(5) in section 11319(b)(1), in the paragraph heading, by striking ''CIOS'' and inserting ''CHIEF INFORMATION OFFICERS''.

(d) SUBCHAPTER III.—Section 11331 of title 40, United States Code, is amended—

(1) in subsection (a), by striking ''section 3532(b)(1)'' and inserting ''section 3552(b)'';

(2) in subsection (b)(1)(A), by striking ''the Secretary of Homeland Security'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(3) by striking subsection (c) and inserting the following:

''(c) APPLICATION OF MORE STRINGENT STANDARDS.—

''(1) IN GENERAL.—The head of an agency shall—

''(A) evaluate, in consultation with the senior agency information security officers, the need to employ standards for cost-effective, risk-based information security for all systems, operations, and assets within or under the supervision of the agency that are more stringent than the standards promulgated by the Director under this section, if such standards contain, at a minimum, the

provisions of those applicable standards made compulsory and binding by the Director; and

''(B) to the greatest extent practicable and if the head of the agency determines that the standards described in subparagraph (A) are necessary, employ those standards.

''(2) EVALUATION OF MORE STRINGENT STANDARDS.—In evaluating the need to employ more stringent standards under paragraph (1), the head of an agency shall consider available risk information, such as—

''(A) the status of cybersecurity remedial actions of the agency;

''(B) any vulnerability information relating to agency systems that is known to the agency;

''(C) incident information of the agency;

''(D) information from—

''(i) penetration testing performed under section 3559A of title 44; and

''(ii) information from the vulnerability disclosure program established under section 3559B of title 44;

''(E) agency threat hunting results under section 5145 of the Federal Information Security Modernization Act of 2021;

''(F) Federal and non-Federal cyber threat intelligence;

''(G) data on compliance with standards issued under this section;

''(H) agency system risk assessments performed under section 3554(a)(1)(A) of title 44; and

''(I) any other information determined relevant by the head of the agency.'';

(4) in subsection (d)(2)—

(A) in the paragraph heading, by striking ''NOTICE AND COMMENT'' and inserting ''CONSULTATION, NOTICE, AND COMMENT'';

(B) by inserting ''promulgate,'' before ''significantly modify''; and

(C) by striking ''shall be made after the public is given an opportunity to comment on the Director's proposed decision.'' and inserting ''shall be made—

''(A) for a decision to significantly modify or not promulgate such a proposed standard, after the public is given an opportunity to comment on the Director's proposed decision;

''(B) in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency;

''(C) considering the Federal risk assessments performed under section 3553(i) of title 44; and

''(D) considering the extent to which the proposed standard reduces risk relative to the cost of implementation of the standard.''; and

(5) by adding at the end the following:

''(e) REVIEW OF OFFICE OF MANAGEMENT AND BUDGET GUIDANCE AND POLICY.—

''(1) CONDUCT OF REVIEW.—

''(A) IN GENERAL.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget, in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency shall review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including an assessment of the requirements for agencies to report information to the Director, and determine whether any changes to that guidance or policy is appropriate.

''(B) FEDERAL RISK ASSESSMENTS.—In conducting the review described in subparagraph (A), the Director shall consider the Federal risk assessments performed under section 3553(i) of title 44.

''(2) UPDATED GUIDANCE.—Not later than 90 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall issue updated guidance or policy to agencies determined appropriate by the Director, based on the results of the review.

''(3) PUBLIC REPORT.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall make publicly available a report that includes—

''(A) an overview of the guidance and policy promulgated under this section that is currently in effect;

''(B) the cybersecurity risk mitigation, or other cybersecurity benefit, offered by each guidance or policy document described in subparagraph (A); and

''(C) a summary of the guidance or policy to which changes were determined appropriate during the review and what the changes are anticipated to include.

''(4) CONGRESSIONAL BRIEFING.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the review.

''(f) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, specifications to enable the automated verification of the implementation of the controls within the standard.''.

SEC. 5123. ACTIONS TO ENHANCE FEDERAL INCIDENT RESPONSE.

(a) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(A) develop a plan for the development of the analysis required under section 3597(a) of title 44, United States Code, as added by this division, and the report required under subsection (b) of that section that includes—

(i) a description of any challenges the Director anticipates encountering; and

(ii) the use of automation and machine-readable formats for collecting, compiling, monitoring, and analyzing data; and

(B) provide to the appropriate congressional committees a briefing on the plan developed under subparagraph (A).

(2) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate congressional committees a briefing on—

(A) the execution of the plan required under paragraph (1)(A); and

(B) the development of the report required under section 3597(b) of title 44, United States Code, as added by this division.

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET.—

(1) FISMA.—Section 2 of the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554 note) is amended—

(A) by striking subsection (b); and

(B) by redesignating subsections (c) through (f) as subsections (b) through (e), respectively.

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director shall develop guidance, to be updated not less frequently than once every 2 years, on the content, timeliness, and format of the information provided by agencies under section 3594(a) of title 44, United States Code, as added by this division.

(B) REQUIREMENTS.—The guidance developed under subparagraph (A) shall—

(i) prioritize the availability of data necessary to understand and analyze—

(I) the causes of incidents;

(II) the scope and scale of incidents within the environments and systems of an agency;

(III) a root cause analysis of incidents that—

(aa) are common across the Federal Government; or

(bb) have a Government-wide impact;

(IV) agency response, recovery, and remediation actions and the effectiveness of those actions; and

(V) the impact of incidents;

(ii) enable the efficient development of—

(I) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

(II) the report on Federal incidents required under section 3597(b) of title 44, United States Code, as added by this division;

(iii) include requirements for the timeliness of data production; and

(iv) include requirements for using automation and machine-readable data for data sharing and availability.

(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall develop guidance for agencies to implement the requirement under section 3594(c) of title 44, United States Code, as added by this division, to provide information to other agencies experiencing incidents.

(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this division.

(5) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to Federal agencies on how to deconflict, to the greatest extent practicable, existing regulations, policies, and procedures relating to the responsibilities of contractors and awardees established under section 3595 of title 44, United States Code, as added by this division.

(B) EXISTING PROCESSES.—To the greatest extent practicable, the guidance issued under subparagraph (A) shall allow contractors and awardees to use existing processes for notifying Federal agencies of incidents involving information of the Federal Government.

(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and templates developed under paragraphs (2) through (4).

(c) UPDATE TO THE PRIVACY ACT OF 1974.—Section 552a(b) of title 5, United States Code (commonly known as the ''Privacy Act of 1974'') is amended—

(1) in paragraph (11), by striking ''or'' at the end;

(2) in paragraph (12), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following:

''(13) to another agency in furtherance of a response to an incident (as defined in section 3552 of title 44) and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.''.

SEC. 5124. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance for agencies on—

(1) performing the ongoing and continuous agency system risk assessment required under section 3554(a)(1)(A) of title 44, United States Code, as amended by this division;

(2) implementing additional cybersecurity procedures, which shall include resources for shared services;

(3) establishing a process for providing the status of each remedial action under section 3554(b)(7) of title 44, United States Code, as amended by this division, to the Director and the Cybersecurity and Infrastructure Security Agency using automation and machine-readable data, as practicable, which shall include—

(A) specific guidance for the use of automation and machine-readable data; and

(B) templates for providing the status of the remedial action;

(4) interpreting the definition of ''high value asset'' under section 3552 of title 44, United States Code, as amended by this division; and

(5) a requirement to coordinate with inspectors general of agencies to ensure consistent understanding and application of agency policies for the purpose of evaluations by inspectors general.

SEC. 5125. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SECTOR ENTITIES IMPACTED BY INCIDENTS.

(a) DEFINITIONS.—In this section:

(1) REPORTING ENTITY.—The term ''reporting entity'' means private organization or governmental unit that is required by statute or regulation to submit sensitive information to an agency.

(2) SENSITIVE INFORMATION.—The term ''sensitive information'' has the meaning given the term by the Director in guidance issued under subsection (b).

(b) GUIDANCE ON NOTIFICATION OF REPORTING ENTITIES.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance requiring the head of each agency to notify a reporting entity of an incident that is likely to substantially affect—

(1) the confidentiality or integrity of sensitive information submitted by the reporting entity to the agency pursuant to a statutory or regulatory requirement; or

(2) the agency information system or systems used in the transmission or storage of the sensitive information described in paragraph (1).

TITLE LII—IMPROVING FEDERAL CYBERSECURITY

SEC. 5141. MOBILE SECURITY STANDARDS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall—

(1) evaluate mobile application security guidance promulgated by the Director; and

(2) issue guidance to secure mobile devices, including for mobile applications, for every agency.

(b) CONTENTS.—The guidance issued under subsection (a)(2) shall include—

(1) a requirement, pursuant to section 3506(b)(4) of title 44, United States Code, for every agency to maintain a continuous inventory of every—

(A) mobile device operated by or on behalf of the agency; and

(B) vulnerability identified by the agency associated with a mobile device; and

(2) a requirement for every agency to perform continuous evaluation of the vulnerabilities described in paragraph (1)(B) and other risks associated with the use of applications on mobile devices.

(c) INFORMATION SHARING.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies for sharing the inventory of the agency required under subsection (b)(1) with the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable.

(d) BRIEFING.—Not later than 60 days after the date on which the Director issues guidance under subsection (a)(2), the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall provide to the appropriate congressional committees a briefing on the guidance.

SEC. 5142. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) RECOMMENDATIONS.—Not later than 2 years after the date of enactment of this Act, and not less frequently than every 2 years thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Attorney General, shall submit to the Director recommendations on requirements for logging events on agency systems and retaining other relevant data within the systems and networks of an agency.

(b) CONTENTS.—The recommendations provided under subsection (a) shall include—

(1) the types of logs to be maintained;

(2) the time periods to retain the logs and other relevant data;

(3) the time periods for agencies to enable recommended logging and security requirements;

(4) how to ensure the confidentiality, integrity, and availability of logs;

(5) requirements to ensure that, upon request, in a manner that excludes or otherwise reasonably protects personally identifiable information, and to the extent permitted by applicable law (including privacy and statistical laws), agencies provide logs to—

(A) the Director of the Cybersecurity and Infrastructure Security Agency for a cybersecurity purpose; and

(B) the Federal Bureau of Investigation to investigate potential criminal activity; and

(6) requirements to ensure that, subject to compliance with statistical laws and other relevant data protection requirements, the highest level security operations center of each agency has visibility into all agency logs.

(c) GUIDANCE.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall, as determined to be appropriate by the Director, update guidance to agencies regarding requirements for logging, log retention, log management, sharing of log data with other appropriate agencies, or any other logging activity determined to be appropriate by the Director.

SEC. 5143. CISA AGENCY ADVISORS.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall assign not less than 1 cybersecurity professional employed by the Cybersecurity and Infrastructure Security Agency to be the Cybersecurity and Infrastructure Security Agency advisor to the senior agency information security officer of each agency.

(b) QUALIFICATIONS.—Each advisor assigned under subsection (a) shall have knowledge of—

(1) cybersecurity threats facing agencies, including any specific threats to the assigned agency;

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

(c) DUTIES.—The duties of each advisor assigned under subsection (a) shall include—

(1) providing ongoing assistance and advice, as requested, to the agency Chief Information Officer;

(2) serving as an incident response point of contact between the assigned agency and the Cybersecurity and Infrastructure Security Agency; and

(3) familiarizing themselves with agency systems, processes, and procedures to better facilitate support to the agency in responding to incidents.

(d) LIMITATION.—An advisor assigned under subsection (a) shall not be a contractor.

(e) MULTIPLE ASSIGNMENTS.—One individual advisor may be assigned to multiple agency Chief Information Officers under subsection (a).

SEC. 5144. FEDERAL PENETRATION TESTING POLICY.

(a) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''§ 3559A. Federal penetration testing

''(a) DEFINITIONS.—In this section:

''(1) AGENCY OPERATIONAL PLAN.—The term 'agency operational plan' means a plan of an agency for the use of penetration testing.

''(2) RULES OF ENGAGEMENT.—The term 'rules of engagement' means a set of rules established by an agency for the use of penetration testing.

''(b) GUIDANCE.—

''(1) IN GENERAL.—The Director shall issue guidance that—

''(A) requires agencies to use, when and where appropriate, penetration testing on agency systems; and

''(B) requires agencies to develop an agency operational plan and rules of engagement that meet the requirements under subsection (c).

''(2) PENETRATION TESTING GUIDANCE.—The guidance issued under this section shall—

''(A) permit an agency to use, for the purpose of performing penetration testing—

''(i) a shared service of the agency or another agency; or

''(ii) an external entity, such as a vendor; and

''(B) require agencies to provide the rules of engagement and results of penetration testing to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, without regard to the status of the entity that performs the penetration testing.

''(c) AGENCY PLANS AND RULES OF ENGAGEMENT.—The agency operational plan and rules of engagement of an agency shall—

''(1) require the agency to—

''(A) perform penetration testing on the high value assets of the agency; or

''(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed;

''(2) establish guidelines for avoiding, as a result of penetration testing—

''(A) adverse impacts to the operations of the agency;

''(B) adverse impacts to operational environments and systems of the agency; and

''(C) inappropriate access to data;

''(3) require the results of penetration testing to include feedback to improve the cybersecurity of the agency; and

''(4) include mechanisms for providing consistently formatted, and, if applicable, automated and machine-readable, data to the Director and the Director of the Cybersecurity and Infrastructure Security Agency.

''(d) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

''(1) establish a process to assess the performance of penetration testing by both Federal and non-Federal entities that establishes minimum quality controls for penetration testing;

''(2) develop operational guidance for instituting penetration testing programs at agencies;

''(3) develop and maintain a centralized capability to offer penetration testing as a service to Federal and non-Federal entities; and

''(4) provide guidance to agencies on the best use of penetration testing resources.

''(e) RESPONSIBILITIES OF OMB.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

''(1) not less frequently than annually, inventory all Federal penetration testing assets; and

''(2) develop and maintain a standardized process for the use of penetration testing.

''(f) PRIORITIZATION OF PENETRATION TESTING RESOURCES.—

''(1) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop a framework for prioritizing Federal penetration testing resources among agencies.

''(2) CONSIDERATIONS.—In developing the framework under this subsection, the Director shall consider—

''(A) agency system risk assessments performed under section 3554(a)(1)(A);

''(B) the Federal risk assessment performed under section 3553(i);

''(C) the analysis of Federal incident data performed under section 3597; and

''(D) any other information determined appropriate by the Director or the Director of the Cybersecurity and Infrastructure Security Agency.

''(g) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The guidance issued under subsection (b) shall not apply to national security systems.

''(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director described in subsection (b) shall be delegated—

''(1) to the Secretary of Defense in the case of systems described in section 3553(e)(2); and

''(2) to the Director of National Intelligence in the case of systems described in 3553(e)(3).''.

(b) DEADLINE FOR GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director shall issue the guidance required under section 3559A(b) of title 44, United States Code, as added by subsection (a).

(c) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559 the following:

''3559A. Federal penetration testing.''.

(d) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by section 5121, is further amended—

(1) in paragraph (8)(B), by striking ''and'' at the end;

(2) by redesignating paragraph (9) as paragraph (10); and

(3) by inserting after paragraph (8) the following:

''(9) performing penetration testing with or without advance notice to, or authorization from, agencies, to identify vulnerabilities within Federal information systems; and''.

SEC. 5145. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall establish a program to provide ongoing, hypothesis-driven threat-hunting services on the network of each agency.

(2) PLAN.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish the program required under paragraph (1) that describes how the Director of the Cybersecurity and Infrastructure Security Agency plans to—

(A) determine the method for collecting, storing, accessing, and analyzing appropriate agency data;

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

(D) allocate available human and financial resources to implement the plan; and

(E) provide input to the heads of agencies on the use of—

(i) more stringent standards under section 11331(c)(1) of title 40, United States Code; and

(ii) additional cybersecurity procedures under section 3554 of title 44, United States Code.

(b) REPORTS.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees—

(1) not later than 30 days after the date on which the Director of the Cybersecurity and Infrastructure Security Agency completes the plan required under subsection (a)(2), a report on the plan to provide threat hunting services to agencies;

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program under subsection (a)(1), a report providing any updates to the plan developed under subsection (a)(2); and

(3) not later than 1 year after the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services to agencies other than the Cybersecurity and Infrastructure Security Agency, a report describing lessons learned from providing those services.

SEC. 5146. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by inserting after section 3559A, as added by section 5144 of this division, the following:

''§ 3559B. Federal vulnerability disclosure programs

''(a) DEFINITIONS.—In this section:

''(1) REPORT.—The term 'report' means a vulnerability disclosure made to an agency by a reporter.

''(2) REPORTER.—The term 'reporter' means an individual that submits a vulnerability report pursuant to the vulnerability disclosure process of an agency.

''(b) RESPONSIBILITIES OF OMB.—

''(1) LIMITATION ON LEGAL ACTION.—The Director, in consultation with the Attorney General, shall issue guidance to agencies to not recommend or pursue legal action against a reporter or an individual that conducts a security research activity that the head of the agency determines—

''(A) represents a good faith effort to follow the vulnerability disclosure policy of the agency developed under subsection (d)(2); and

''(B) is authorized under the vulnerability disclosure policy of the agency developed under subsection (d)(2).

''(2) SHARING INFORMATION WITH CISA.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine readable manner with the Cybersecurity and Infrastructure Security Agency, including—

''(A) any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on Federal information systems that use commercial software or services;

''(B) information relating to vulnerability disclosure, coordination, or remediation activities of an agency, particularly as those activities relate to outside organizations—

''(i) with which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency can assist; or

''(ii) about which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency should know; and

''(C) any other information with respect to which the head of the agency determines helpful or necessary to involve the Cybersecurity and Infrastructure Security Agency.

''(3) AGENCY VULNERABILITY DISCLOSURE POLICIES.—The Director shall issue guidance to agencies on the required minimum scope of agency systems covered by the vulnerability disclosure policy of an agency required under subsection (d)(2).

''(c) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

''(1) provide support to agencies with respect to the implementation of the requirements of this section;

''(2) develop tools, processes, and other mechanisms determined appropriate to offer agencies capabilities to implement the requirements of this section; and

''(3) upon a request by an agency, assist the agency in the disclosure to vendors of newly identified vulnerabilities in vendor products and services.

''(d) RESPONSIBILITIES OF AGENCIES.—

''(1) PUBLIC INFORMATION.—The head of each agency shall make publicly available, with respect to each internet domain under the control of the agency that is not a national security system—

''(A) an appropriate security contact; and

''(B) the component of the agency that is responsible for the internet accessible services offered at the domain.

''(2) VULNERABILITY DISCLOSURE POLICY.—The head of each agency shall develop and make publicly available a vulnerability disclosure policy for the agency, which shall—

''(A) describe—

''(i) the scope of the systems of the agency included in the vulnerability disclosure policy;

''(ii) the type of information system testing that is authorized by the agency;

''(iii) the type of information system testing that is not authorized by the agency; and

''(iv) the disclosure policy of the agency for sensitive information;

''(B) with respect to a report to an agency, describe—

''(i) how the reporter should submit the report; and

''(ii) if the report is not anonymous, when the reporter should anticipate an acknowledgment of receipt of the report by the agency;

''(C) include any other relevant information; and

''(D) be mature in scope, to cover all Federal information systems used or operated by that agency or on behalf of that agency.

''(3) IDENTIFIED VULNERABILITIES.—The head of each agency shall incorporate any vulnerabilities reported under paragraph (2) into the vulnerability management process of the agency in order to track and remediate the vulnerability.

''(e) PAPERWORK REDUCTION ACT EXEMPTION.—The requirements of subchapter I (commonly known as the 'Paperwork Reduction Act') shall not apply to a vulnerability disclosure program established under this section.

''(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, and annually thereafter for a 3-year period, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (b)(3), an identification of the agencies that are compliant and not compliant.

''(g) EXEMPTIONS.—The authorities and functions of the Director and Director of the Cybersecurity and Infrastructure Security Agency under this section shall not apply to national security systems.

''(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director and the Director of the Cybersecurity and Infrastructure Security Agency described in this section shall be delegated—

''(1) to the Secretary of Defense in the case of systems described in section 3553(e)(2); and

''(2) to the Director of National Intelligence in the case of systems described in section 3553(e)(3).''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559A, as added by section 204, the following:

''3559B. Federal vulnerability disclosure programs.''.

SEC. 5147. IMPLEMENTING PRESUMPTION OF COMPROMISE AND LEAST PRIVILEGE PRINCIPLES.

(a) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from ''trusted networks'' to implement security controls based on a presumption of compromise;

(2) implementing principles of least privilege in administering information security programs;

(3) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(4) identifying incidents quickly;

(5) isolating and removing unauthorized entities from agency systems quickly;

(6) otherwise increasing the resource costs for entities that cause incidents to be successful; and

(7) a summary of the agency progress reports required under subsection (b).

(b) AGENCY PROGRESS REPORTS.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director;

(2) an identification of activities that have not yet been completed and that would have the most immediate security impact; and

(3) a schedule to implement any planned activities.

SEC. 5148. AUTOMATION REPORTS.

(a) OMB REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the use of automation under paragraphs (1), (5)(C) and (8)(B) of section 3554(b) of title 44, United States Code.

(b) GAO REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall perform a study on the use of automation and machine readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes by agencies.

SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

Section 1328 of title 41, United States Code, is amended by striking ''the date that'' and all that follows and inserting ''December 31, 2026.''.

SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 11(e)(2) of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(1) in subparagraph (A), by striking ''and'' at the end;

(2) by redesignating subparagraph (B) as subparagraph (C); and

(3) by inserting after subparagraph (A) the following:

''(B) that shall include a dashboard of open information security recommendations identified in the independent evaluations required by section 3555(a) of title 44, United States Code; and''.

SEC. 5151. QUANTITATIVE CYBERSECURITY METRICS.

(a) DEFINITION OF COVERED METRICS.—In this section, the term ''covered metrics'' means the metrics established, reviewed, and updated under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

(b) UPDATING AND ESTABLISHING METRICS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall—

(1) evaluate any covered metrics established as of the date of enactment of this Act; and

(2) as appropriate and pursuant to section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c))—

(A) update the covered metrics; and

(B) establish new covered metrics.

(c) IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promulgate guidance that requires each agency to use covered metrics to track trends in the cybersecurity and incident response capabilities of the agency.

(2) PERFORMANCE DEMONSTRATION.—The guidance issued under paragraph (1) and any subsequent guidance shall require agencies to share with the Director of the Cybersecurity and Infrastructure Security Agency data demonstrating the performance of the agency using the covered metrics included in the guidance.

(3) PENETRATION TESTS.—On not less than 2 occasions during the 2-year period following the date on which guidance is promulgated under paragraph (1), the Director shall ensure that not less than 3 agencies are subjected to substantially similar penetration tests, as determined by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, in order to validate the utility of the covered metrics.

(4) ANALYSIS CAPACITY.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop a capability that allows for the analysis of the covered metrics, including cross-agency performance of agency cybersecurity and incident response capability trends.

(d) CONGRESSIONAL REPORTS.—

(1) UTILITY OF METRICS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees a report on the utility of the covered metrics.

(2) USE OF METRICS.—Not later than 180 days after the date on which the Director promulgates guidance under subsection (c)(1), the Director shall submit to the appropriate congressional committees a report on the results of the use of the covered metrics by agencies.

(e) CYBERSECURITY ACT OF 2015 UPDATES.—Section 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522) is amended—

(1) by striking subsection (c) and inserting the following:

''(c) IMPROVED METRICS.—

''(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall establish, review, and update metrics to measure the cybersecurity and incident response capabilities of agencies in accordance with the responsibilities of agencies under section 3554 of title 44, United States Code.

''(2) QUALITIES.—With respect to the metrics established, reviewed, and updated under paragraph (1)—

''(A) not less than 2 of the metrics shall be time-based, such as a metric of—

''(i) the amount of time it takes for an agency to detect an incident; and

''(ii) the amount of time that passes between—

''(I) the detection of an incident and the remediation of the incident; and

''(II) the remediation of an incident and the recovery from the incident; and

''(B) the metrics may include other measurable outcomes.'';

(2) by striking subsection (e); and

(3) by redesignating subsection (f) as subsection (e).

TITLE LIII—RISK-BASED BUDGET MODEL

SEC. 5161. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and

(B) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COVERED AGENCY.—The term ''covered agency'' has the meaning given the term ''executive agency'' in section 133 of title 41, United States Code.

(3) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(4) INFORMATION TECHNOLOGY.—The term ''information technology''—

(A) has the meaning given the term in section 11101 of title 40, United States Code; and

(B) includes the hardware and software systems of a Federal agency that monitor and control physical equipment and processes of the Federal agency.

(5) RISK-BASED BUDGET.—The term ''risk-based budget'' means a budget—

(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of cyber threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) IN GENERAL.—

(1) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director and in coordination with the Director of the National Institute of Standards and Technology, shall develop a standard model for creating a risk-based budget for cybersecurity spending.

(2) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, as amended by section 5121 of this division, is further amended by inserting after paragraph (6) the following:

''(7) developing a standard risk-based budget model to inform Federal agency cybersecurity budget development; and''.

(3) CONTENTS OF MODEL.—The model required to be developed under paragraph (1) shall—

(A) consider Federal and non-Federal cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;

(B) consider the impact of agency operations of compromise of systems, including the interconnectivity to other agency systems and the operations of other agencies;

(C) indicate where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities;

(D) be used to inform acquisition and sustainment of—

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

(iv) cybersecurity and information technology concepts of operations; and

(E) be used to evaluate and inform Government-wide cybersecurity programs of the Department of Homeland Security.

(4) REQUIRED UPDATES.—Not less frequently than once every 3 years, the Director shall review, and update as necessary, the model required to be developed under this subsection.

(5) PUBLICATION.—The Director shall publish the model required to be developed under this subsection, and any updates necessary under paragraph (4), on the public website of the Office of Management and Budget.

(6) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under this subsection is completed, whichever is sooner, the Director shall submit a report to Congress on the development of the model.

(b) REQUIRED USE OF RISK-BASED BUDGET MODEL.—

(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

(2) AGENCY PERFORMANCE PLANS.—Section 3554(d)(2) of title 44, United States Code, is amended by inserting ''and the risk-based budget model required under section 3553(a)(7)'' after ''paragraph (1)''.

(c) VERIFICATION.—

(1) IN GENERAL.—Section 1105(a)(35)(A)(i) of title 31, United States Code, is amended—

(A) in the matter preceding subclause (I), by striking ''by agency, and by initiative area (as determined by the administration)'' and inserting ''and by agency'';

(B) in subclause (III), by striking ''and'' at the end; and

(C) by adding at the end the following:

''(V) a validation that the budgets submitted were developed using a risk-based methodology; and

''(VI) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) of title 44.''.

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(d) REPORTS.—

(1) INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—

(A) in subparagraph (B), by striking ''and'' at the end;

(B) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(D) an assessment of how the agency implemented the risk-based budget model required under section 3553(a)(7) and an evaluation of whether the model mitigates agency cyber vulnerabilities.''.

(2) ASSESSMENT.—Section 3553(c) of title 44, United States Code, as amended by section 5121, is further amended by inserting after paragraph (5) the following:

''(6) an assessment of—

''(A) Federal agency implementation of the model required under subsection (a)(7);

''(B) how cyber vulnerabilities of Federal agencies changed from the previous year; and

''(C) whether the model mitigates the cyber vulnerabilities of the Federal Government.''.

(e) GAO REPORT.—Not later than 3 years after the date on which the first budget of the President is submitted to Congress containing the validation required under section 1105(a)(35)(A)(i)(V) of title 31, United States Code, as amended by subsection (c), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(1) an evaluation of the success of covered agencies in developing risk-based budgets;

(2) an evaluation of the success of covered agencies in implementing risk-based budgets;

(3) an evaluation of whether the risk-based budgets developed by covered agencies mitigate cyber vulnerability, including the extent to which the risk-based budgets inform Federal Government-wide cybersecurity programs; and

(4) any other information relating to risk-based budgets the Comptroller General determines appropriate.

TITLE LIV—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term ''active defense technique''—

(1) means an action taken on the systems of an entity to increase the security of information on the network of an agency by misleading an adversary; and

(2) includes a honeypot, deception, or purposefully feeding false or misleading data to an adversary when the adversary is on the systems of the entity.

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A);

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

(4) the development of a framework for the use of different active defense techniques by agencies.

SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

(b) PLAN.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations center shared service offering within the Cybersecurity and Infrastructure Security Agency.

(c) CONTENTS.—The plan required under subsection (b) shall include considerations for—

(1) collecting, organizing, and analyzing agency information system data in real time;

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required

under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

(2) ADDITIONAL AGREEMENTS.—After the date on which the briefing required under subsection (e)(1) is provided, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, may enter into additional 1-year agreements described in paragraph (1) with agencies.

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 260 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

(2) REPORT.—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—

(A) the agreement; and

(B) any additional agreements entered into with agencies under subsection (d).

DIVISION F—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

TITLE LXI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 6101. SHORT TITLE.

This title may be cited as the ''Cyber Incident Reporting Act of 2021''.

SEC. 6102. DEFINITIONS.

In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms ''covered cyber incident'', ''covered entity'', and ''cyber incident'' have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 6103 of this title.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 6203 of this division.

SEC. 6103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 6203(b) of this division—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

''Subtitle C—Cyber Incident Reporting

''SEC. 2230. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

''(3) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

''(4) COVERED ENTITY.—The term 'covered entity' means—

''(A) any Federal contractor; or

''(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

''(5) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2200.

''(6) CYBER THREAT.—The term 'cyber threat'—

''(A) has the meaning given the term 'cybersecurity threat' in section 2200; and

''(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

''(7) FEDERAL CONTRACTOR.—The term 'Federal contractor' means a business, nonprofit organization, or other private sector entity that holds a Federal Government contract or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity is a party only to—

''(A) a service contract to provide housekeeping or custodial services; or

''(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

''(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The terms 'Federal entity', 'information system', and 'security control' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(10) SMALL ORGANIZATION.—The term 'small organization'—

''(A) means—

''(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

''(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

''(B) does not include—

''(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

''(ii) a Federal contractor.

''SEC. 2231. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

''(2) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetuate cyber incidents and ransomware attacks;

''(3) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(4) leverage information gathered about cybersecurity incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and incident response firms, and security researchers; and

''(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2235;

''(5) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

''(6) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the briefings required under subsection (c);

''(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

''(11) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

''(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and

''(13) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2233, or information received pursuant to a request for information or subpoena under section 2234, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

''(b) INTERAGENCY SHARING.—The National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

''(1) may establish a specific time requirement for sharing information under subsection (a)(13); and

''(2) shall determine the appropriate Federal agencies under subsection (a)(13).

''(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

''(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

''(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

''(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

''(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

''(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

''(4) be unclassified, but may include a classified annex.

''SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

''(a) IN GENERAL.—

''(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

''(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

''(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

''(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(5) EXCEPTIONS.—

''(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

''(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to an entity or the functions of an entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

''(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

''(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

''(b) RULEMAKING.—

''(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

''(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

''(3) SUBSEQUENT RULEMAKINGS.—

''(A) IN GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

''(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

''(1) A clear description of the types of entities that constitute covered entities, based on—

''(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

''(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

''(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

''(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

''(A) at a minimum, require the occurrence of—

''(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

''(ii) a disruption of business or industrial operations due to a cyber incident; or

''(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

''(B) consider—

''(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

''(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

''(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

''(C) exclude—

''(i) any event where the cyber incident is perpetuated by good faith security research or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and

''(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

''(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

''(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

''(A) A description of the covered cyber incident, including—

''(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

''(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

''(iii) the estimated date range of such incident; and

''(iv) the impact to the operations of the covered entity.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

''(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

''(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

''(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

''(F) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.

''(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

''(A) A description of the ransomware attack, including the estimated date range of the attack.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

''(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

''(D) The name and other information that clearly identifies the entity that made the ransom payment.

''(E) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

''(F) The date of the ransom payment.

''(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

''(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

''(I) The amount of the ransom payment.

''(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

''(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

''(A) be established by the Director in consultation with the Council;

''(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

''(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

''(8) Procedures for—

''(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

''(B) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

''(C) implementing the exceptions provided in subsection (a)(5); and

''(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

''(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

''(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under subsection (a).

''(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

''(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

''(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding reporting ransom payments under this section.

''(e) OUTREACH TO COVERED ENTITIES.—

''(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

''(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

''(A) An overview of the final rule issued pursuant to subsection (b).

''(B) An overview of mechanisms to submit to the Center covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

''(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

''(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

''(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

''(F) An overview of the privacy and civil liberties requirements in this subtitle.

''(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

''(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

''(B) information sharing and analysis organizations;

''(C) trade associations;

''(D) information sharing and analysis centers;

''(E) sector coordinating councils; and

''(F) any other entity as determined appropriate by the Director.

''(f) ORGANIZATION OF REPORTS.—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), the Director may request information within the scope of the final rule issued under subsection (b) by the alteration of existing questions or response fields and the reorganization and reformatting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.

''SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

''(a) IN GENERAL.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

''(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

''(c) APPLICATION OF PROTECTIONS.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

''SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

''(a) PURPOSE.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a

covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

''(b) INITIAL REQUEST FOR INFORMATION.—

''(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(a), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Center within 72 hours in accordance with section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

''(2) TREATMENT.—Information provided to the Center in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

''(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

''(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

''(2) CIVIL ACTION.—

''(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

''(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

''(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

''(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

''(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity that is a Federal contractor fails to comply with a subpoena issued under this subsection—

''(A) the Director may refer the matter to the Administrator of General Services; and

''(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

''(5) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

''(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

''(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency determines, based on information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may use that information for a regulatory enforcement action or criminal prosecution.

''(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

''(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

''(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

''(1) the size and complexity of the entity;

''(2) the complexity in determining if a covered cyber incident has occurred; and

''(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

''(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

''(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b);

''(2) issued a subpoena pursuant to subsection (c); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) DISCLOSURE, RETENTION, AND USE.—

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Center or Agency pursuant to section 2232 or 2233 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

''(A) a cybersecurity purpose;

''(B) the purpose of identifying—

''(i) a cyber threat, including the source of the cyber threat; or

''(ii) a security vulnerability;

''(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

''(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

''(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2232 or 2233 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

''(2) AGENCY ACTIONS AFTER RECEIPT.—

''(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the center shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

''(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

''(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Center or the Agency pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

''(A) personal information of a specific individual; or

''(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(4) DIGITAL SECURITY.—The Center and the Agency shall ensure that reports submitted to the Center or the Agency pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

''(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment.

''(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

''(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt

from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

''(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

''(e) LIABILITY PROTECTIONS.—

''(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rule promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

''(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Center or the Agency.

''(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

''(f) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

''(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.

''(h) STORED COMMUNICATIONS ACT.—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the items relating to subtitle B of title XXII the following:

''Subtitle C—Cyber Incident Reporting

''Sec. 2230. Definitions.
''Sec. 2231. Cyber Incident Review.
''Sec. 2232. Required reporting of certain cyber incidents.
''Sec. 2233. Voluntary reporting of other cyber incidents.
''Sec. 2234. Noncompliance with required reporting.
''Sec. 2235. Information shared with or provided to the Federal Government.''.

SEC. 6104. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Director as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 6103 of this title.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this Act or the amendments made by this Act.

(4) FOIA EXEMPTION.—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ''Freedom of Information Act'').

(b) CREATION OF COUNCIL.—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is amended—

(1) in paragraph (1)—

(A) in subparagraph (G), by striking ''and'' at the end;

(B) by redesignating subparagraph (H) as subparagraph (I); and

(C) by inserting after subparagraph (G) the following:

''(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget, the Attorney General, and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and''; and

(2) by adding at the end the following:

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any Federal entity.''.

(c) HARMONIZING REPORTING REQUIREMENTS.—The National Cyber Director shall, in consultation with the Director, the Attorney General, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director, the Attorney General, and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 6105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).

(c) ENTITY NOTIFICATION.—

(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.

SEC. 6106. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) JOINT RANSOMWARE TASK FORCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in consultation with the Attorney General and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware

Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) CLARIFYING PRIVATE SECTOR LAWFUL DEFENSIVE MEASURES.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 6107. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103(b) of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 6103(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 6105, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 6105(c) in mitigating security vulnerabilities and the threat of ransomware.

(2) Identification of the most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the National Cyber Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) GAO REPORTS.—

(1) IMPLEMENTATION OF THIS ACT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this Act and the amendments made by this Act.

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (2) and (5) of section 2232(a) of the Homeland Security Act of 2002, as added by section 6103 of this title, which shall include—

(A) to the extent practicable, an evaluation of the quantity of incidents not reported to the Federal Government;

(B) an evaluation of the impact on impacted entities, homeland security, and the national economy of the ransomware criminal ecosystem of incidents and ransom payments, including a discussion on the scope of impact of incidents that were not reported to the Federal Government;

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this Act, including an analysis of entities that meet the definition of a small organization and would be exempt from ransom payment reporting but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2234 of the Homeland Security Act of 2002, as added by section 6103 of this title.

TITLE LXII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 6201. SHORT TITLE.

This title may be cited as the ''CISA Technical Corrections and Improvements Act of 2021''.

SEC. 6202. REDESIGNATIONS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217; and

(5) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (11), by striking ''and'' at the end;

(2) in the first paragraph (12)—

(A) by striking ''section 2215'' and inserting ''section 2217''; and

(B) by striking ''and'' at the end; and

(3) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) ADDITIONAL TECHNICAL AMENDMENT.—

(1) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

SEC. 6203. CONSOLIDATION OF DEFINITIONS.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitle A heading the following:

"SEC. 2200. DEFINITIONS.

''Except as otherwise specifically provided, in this title:

''(1) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(2) AGENCY INFORMATION.—The term 'agency information' means information collected or maintained by or on behalf of an agency.

''(3) AGENCY INFORMATION SYSTEM.—The term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency.

''(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(B) the Committee on Homeland Security of the House of Representatives.

''(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(6) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

''(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

''(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

''(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

''(7) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' means information that is necessary to describe or identify—

''(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

''(B) a method of defeating a security control or exploitation of a security vulnerability;

''(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

''(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

''(E) malicious cyber command and control;

''(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

''(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

''(H) any combination thereof.

''(8) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

''(9) CYBERSECURITY RISK.—The term 'cybersecurity risk'—

''(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

''(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

''(10) CYBERSECURITY THREAT.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'cybersecurity threat' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

''(B) EXCLUSION.—The term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

''(11) DEFENSIVE MEASURE.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

''(B) EXCLUSION.—The term 'defensive measure' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

''(i) the entity operating the measure; or

''(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

''(12) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

''(13) INCIDENT.—The term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

''(14) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

''(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

''(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

''(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

''(15) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(16) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(17) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

''(18) MONITOR.—The term 'monitor' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

''(19) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

''(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

''(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

''(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

''(D) facilitating information sharing and operational coordination with threat response; and

''(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

''(20) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(21) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(22) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means a cyber incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital

mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

''(B) does not include any such event where the demand for payment is made by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

''(23) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

''(24) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

''(25) SECURITY VULNERABILITY.—The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

''(26) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

''(27) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize the confidentiality, integrity, or availability of the information technology system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

''(28) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

''(29) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

''SEC. 2201. DEFINITION.

''In this subtitle, the term 'Cybersecurity Advisory Committee' means the advisory committee established under section 2219(a).'';

(2) in section 2202—

(A) in subsection (a)(1), by striking ''(in this subtitle referred to as the Agency)'';

(B) in subsection (f)—

(i) in paragraph (1), by inserting ''Executive'' before ''Assistant Director''; and

(ii) in paragraph (2), by inserting ''Executive'' before ''Assistant Director'';

(3) in section 2203(a)(2), by striking ''as the 'Assistant Director' '' and inserting ''as the 'Executive Assistant Director' '';

(4) in section 2204(a)(2), by striking ''as the 'Assistant Director' '' and inserting ''as the 'Executive Assistant Director' '';

(5) in section 2209—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)—

(i) in subparagraph (A)(iii), as so redesignated, by striking '', as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))''; and

(ii) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(ii) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(E) in subsection (j), as so redesignated, by striking ''subsection (c)(8)'' and inserting ''subsection (b)(8)''; and

(F) in subsection (n), as so redesignated—

(i) in paragraph (2)(A), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)''; and

(ii) in paragraph (3)(B)(i), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)'';

(6) in section 2210—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(C) in subsection (b), as so redesignated—

(i) by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations''; and

(ii) by striking ''(as defined in section 2209)''; and

(D) in subsection (c), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (b)'';

(7) in section 2211, by striking subsection (h);

(8) in section 2212, by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations'';

(9) in section 2213—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (f) as subsections (a) through (e); respectively;

(C) in subsection (b), as so redesignated, by striking ''subsection (b)'' each place it appears and inserting ''subsection (a)'';

(D) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking ''subsection (b)'' and inserting ''subsection (a)''; and

(E) in subsection (d), as so redesignated—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(II) in subparagraph (A), by striking ''subsection (c)(1)'' and inserting ''subsection (b)(1)''; and

(III) in subparagraph (B), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)''; and

(ii) in paragraph (2), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(10) in section 2216, as so redesignated—

(A) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(B) by striking subsection (f) and inserting the following:

''(f) CYBER DEFENSE OPERATION DEFINED.—In this section, the term 'cyber defense operation' means the use of a defensive measure.'';

(11) in section 2218(c)(4)(A), as so redesignated, by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(12) in section 2222—

(A) by striking paragraphs (3), (5), and (8);

(B) by redesignating paragraph (4) as paragraph (3); and

(C) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXII the following:

''Sec. 2200. Definitions.'';

(2) by striking the item relating to section 2201 and inserting the following:

''Sec. 2201. Definition.''; and

(3) by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.''.

(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

''(4) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(6) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(7) DEFENSIVE MEASURE.—The term 'defensive measure' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) by striking paragraph (13) and inserting the following:

''(13) MONITOR.— The term 'monitor' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''; and

(3) by striking paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''.

SEC. 6204. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking ''section 2210'' and inserting ''section 2200''; and

(B) in paragraph (4), by striking ''section 2209'' and inserting ''section 2200'';

(2) in section 223(b) (6 U.S.C. 151 note), by striking ''section 2213(b)(1)'' each place it appears and inserting ''section 2213(a)(1)'';

(3) in section 226 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

(iii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iv) in paragraph (5), by striking ''section 2213(b)'' and inserting ''section 2213(a)''; and

(B) in subsection (c)(1)(A)(vi), by striking ''section 2213(c)(5)'' and inserting ''section 2213(b)(5)''; and

(4) in section 227(b) (6 U.S.C. 1525(b)), by striking ''section 2213(d)(2)'' and inserting ''section 2213(c)(2)''.

(b) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking ''section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))'' and inserting ''section 2210(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

(c) WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))'' and inserting ''section 2200 of the Homeland Security Act of 2002''; and

(B) by amending paragraph (7) to read as follows:

''(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) in subsection (c)(3)(B), by striking ''section 2201(5)'' and inserting ''section 2200''; and

(3) in subsection (d)—

(A) by striking ''section 2215'' and inserting ''section 2218''; and

(B) by striking '', as added by this section''.

(d) NATIONAL SECURITY ACT OF 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking ''section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147)'' and inserting ''section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(e) IOT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking ''section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(l))''.

(f) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of the Small Business Act (15 U.S.C. 648(a)(8)(B)) is amended by striking ''section 2209(a)'' and inserting ''section 2200''.

(g) TITLE 46.—Section 70101(2) of title 46, United States Code, is amended by striking ''section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)'' and inserting ''section 2200 of the Homeland Security Act of 2002''.

TITLE LXIII—FEDERAL CYBERSECURITY REQUIREMENTS

SEC. 6301. EXEMPTION FROM FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IN GENERAL.—Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) is amended to read as follows:

''(2) EXCEPTION.—

''(A) IN GENERAL.—A particular requirement under paragraph (1) shall not apply to an agency information system of an agency if—

''(i) with respect to the agency information system, the head of the agency submits to the Director an application for an exemption from the particular requirement, in which the head of the agency personally certifies to the Director with particularity that—

''(I) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the particular requirement;

''(II) the particular requirement is not necessary to secure the agency information system or agency information stored on or transiting the agency information system; and

''(III) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting the agency information system;

''(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and any other congressional committee with jurisdiction over the agency; and

''(iii) the Director grants the exemption from the particular requirement.

''(B) DURATION OF EXEMPTION.—

''(i) IN GENERAL.—An exemption granted under subparagraph (A) shall expire on the date that is 1 year after the date on which the Director grants the exemption.

''(ii) RENEWAL.—Upon the expiration of an exemption granted to an agency under subparagraph (A), the head of the agency may apply for an additional exemption.''.

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by section 5121 of this Act, is further amended—

(1) in subparagraph (C), by striking ''and'' at the end;

(2) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(E) with respect to any exemptions the agency is granted by the Director of the Office of Management and Budget under section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) that is effective on the date of submission of the report, includes—

''(i) an identification of the particular requirements from which any agency information system (as defined in section 2210 of the Homeland Security Act of 2002 (6 U.S.C. 660)) is exempted; and

''(ii) for each requirement identified under subclause (I)—

''(I) an identification of the agency information system described in subclause (I) exempted from the requirement; and

''(II) an estimate of the date on which the agency will to be able to comply with the requirement.''.

(c) EFFECTIVE DATE.—This section and the amendments made by this section shall take effect on the date that is 1 year after the date of enactment of this Act.

SA 4800. Ms. KLOBUCHAR (for herself and Mr. BLUNT) submitted an amendment intended to be proposed by her to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle A of title X, add the following:

SEC. 1004. AVAILABILITY OF TRAVEL PROMOTION FUND FOR BRAND USA.

(a) SHORT TITLE.—This section may be cited as the ''Restoring Brand USA Act''.

(b) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Secretary of the Treasury, subject to subsections (c) and (d), and notwithstanding any other provision of law, shall make available, from unobligated balances remaining available from fees collected before October 1, 2020, and credited to Travel Promotion Fund established under subsection (d) of the Travel Promotion Act of 2009 (22 U.S.C. 2131(d)), $250,000,000 for the Corporation for Travel Promotion (commonly known as ''Brand USA'').

(c) INAPPLICABILITY OF CERTAIN REQUIREMENTS AND LIMITATIONS.—The limitations in subsection (d)(2)(B) of the Travel Promotion Act of 2009 shall not apply to amounts made available under subsection (b), and the requirements in subsection (d)(3) of such Act shall not apply to more than $50,000,000 of the amounts so available.

(d) USE OF FUNDS.—Brand USA may only use funds provided under subsection (b) to promote travel from countries whose citizens and nationals are permitted to enter the United States.

(e) REPORT REQUIRED.—Not later than 60 days after the date of the enactment of this Act, Brand USA shall submit to Congress a plan for obligating and expending the amounts described in subsection (b).

SA 4801. Mr. KENNEDY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ____. SBIR AND STTR PILOT PROGRAM FOR UNDERPERFORMING STATES.

Section 9 of the Small Business Act (15 U.S.C. 638) is amended by adding at the end the following:

''(vv) DEPARTMENT OF DEFENSE PILOT PROGRAM FOR UNDERPERFORMING STATES.—

''(1) DEFINITIONS.—In this section:

''(A) DEPARTMENT.—The term 'Department' means the Department of Defense.

''(B) UNDERPERFORMING STATE.—The term 'underperforming State' means any State participating in the SBIR or STTR program that is in the bottom 68 percent of all States historically receiving SBIR or STTR program funding.

''(2) ESTABLISHMENT.—The Secretary of Defense shall establish a pilot program to provide small business concerns located in underperforming States an increased level of assistance under the SBIR and STTR programs of the Department.

''(3) ACTIVITIES.—Under the pilot program, the Department, and any component agency thereof, may—

''(A) in any case in which the Department seeks to make a Phase II SBIR or STTR award to a small business concern based on the results of a Phase I award made to the small business concern by another agency, establish a streamlined transfer and fast track approval process for that Phase II award;

''(B) provide an additional Phase II SBIR or STTR award to a small business concern

located in an underperforming State that received a Phase I SBIR or STTR award, subject to an increase in the allocation percentage;

''(C) establish a program to make Phase 1.5 SBIR or STTR awards to small business concerns located in underperforming States in order to provide funding for 12 to 24 months to continue the development of technology; and

''(D) carry out subparagraph (C) along with other mentorship programs.

''(4) DURATION.—The pilot program established under this subsection shall terminate 5 years after the date on which the pilot program is established.

''(5) REPORT.—The Department shall submit to Congress an annual report on the status of the pilot program established under this subsection, including the improvement in funding under the SBIR and STTR programs of the Department provided to small business concerns located in underperforming States.''.

SA 4802. Mr. OSSOFF (for himself, Mr. TILLIS, Mr. KING, Ms. CORTEZ MASTO, Mr. ROUNDS, Mr. SCOTT of South Carolina, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. DR. DAVID SATCHER CYBERSECURITY EDUCATION GRANT PROGRAM.

(a) SHORT TITLE.—This section may be cited as the ''Cybersecurity Opportunity Act''.

(b) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(2) ENROLLMENT OF NEEDY STUDENTS.—The term ''enrollment of needy students'' has the meaning given the term in section 312(d) of the Higher Education Act of 1965 (20 U.S.C. 1058(d)).

(3) HISTORICALLY BLACK COLLEGE OR UNIVERSITY.—The term ''historically Black college or university'' has the meaning given the term ''part B institution'' as defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061).

(4) INSTITUTION OF HIGHER EDUCATION.—The term ''institution of higher education'' has the meaning given the term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

(5) MINORITY-SERVING INSTITUTION.—The term ''minority-serving institution'' means an institution listed in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)).

(c) AUTHORIZATION OF GRANTS.—

(1) IN GENERAL.—Subject to the availability of appropriations, the Director shall carry out the Dr. David Satcher Cybersecurity Education Grant Program by—

(A) awarding grants to assist institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to establish or expand cybersecurity programs, to build and upgrade institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities, and to support such institutions on the path to producing qualified entrants in the cybersecurity workforce or becoming a National Center of Academic Excellence in Cybersecurity; and

(B) awarding grants to build capacity at institutions of higher education that have an enrollment of needy students, historically Black colleges and universities, and minority-serving institutions, to expand cybersecurity education opportunities, cybersecurity programs, cybersecurity research, and cybersecurity partnerships with public and private entities.

(2) RESERVATION.—The Director shall award not less than 50 percent of the amount available for grants under this section to historically Black colleges and universities and minority-serving institutions.

(3) COORDINATION.—The Director shall carry out this section in coordination with appropriate Federal agencies, including the Department of Homeland Security.

(4) SUNSET.—The Director's authority to award grants under paragraph (1) shall terminate on the date that is 5 years after the date the Director first awards a grant under paragraph (1).

(d) APPLICATIONS.—An eligible institution seeking a grant under subsection (a) shall submit an application to the Director at such time, in such manner, and containing such information as the Director may reasonably require, including a statement of how the institution will use the funds awarded through the grant to expand cybersecurity education opportunities at the eligible institution.

(e) ACTIVITIES.—An eligible institution that receives a grant under this section may use the funds awarded through such grant for increasing research, education, technical, partnership, and innovation capacity, including for—

(1) building and upgrading institutional capacity to better support new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities;

(2) building and upgrading institutional capacity to provide hands-on research and training experiences for undergraduate and graduate students; and

(3) outreach and recruitment to ensure students are aware of such new or existing cybersecurity programs, including cybersecurity partnerships with public and private entities.

(f) REPORTING REQUIREMENTS.—Not later than—

(1) 1 year after the effective date of this section, as provided in subsection (h), and annually thereafter until the Director submits the report under paragraph (2), the Director shall prepare and submit to Congress a report on the status and progress of implementation of the grant program under this section, including on the number and nature of institutions participating, the number and nature of students served by institutions receiving grants, the level of funding provided to grant recipients, the types of activities being funded by the grants program, and plans for future implementation and development; and

(2) 5 years after the effective date of this section, as provided in subsection (h), the Director shall prepare and submit to Congress a report on the status of cybersecurity education programming and capacity-building at institutions receiving grants under this section, including changes in the scale and scope of these programs, associated facilities, or in accreditation status, and on the educational and employment outcomes of students participating in cybersecurity programs that have received support under this section.

(g) PERFORMANCE METRICS.—The Director shall establish performance metrics for grants awarded under this section.

(h) EFFECTIVE DATE.—This section shall take effect 1 year after the date of enactment of this Act.

SA 4803. Ms. DUCKWORTH (for herself, Mr. KELLY, Ms. HIRONO, Ms. ROSEN, Mr. BENNET, Mr. HEINRICH, Mr. MORAN, Mr. YOUNG, Mrs. FEINSTEIN, Mrs. GILLIBRAND, Mr. KING, Mrs. SHAHEEN, Ms. KLOBUCHAR, Mr. DURBIN, Mr. PETERS, and Mr. BLUMENTHAL) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XII, add the following:

SEC. 1216. AFGHANISTAN WAR COMMISSION ACT OF 2021.

(a) SHORT TITLE.—This section may be cited as the ''Afghanistan War Commission Act of 2021''.

(b) DEFINITIONS.—In this section:

(1) APPLICABLE PERIOD.—The term ''applicable period'' means the period beginning June 1, 2001, and ending August 30, 2021.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Foreign Relations of the Senate;

(C) the Select Committee on Intelligence of the Senate;

(D) the Committee on Appropriations of the Senate;

(E) the Committee on Armed Services of the House of Representatives;

(F) the Committee on Foreign Affairs of the House of Representatives;

(G) the Permanent Select Committee on Intelligence of the House of Representatives; and

(H) the Committee on Appropriations of the House of Representatives.

(3) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given that term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(c) ESTABLISHMENT OF COMMISSION.—

(1) ESTABLISHMENT.—There is established in the legislative branch an independent commission to be known as the Afghanistan War Commission (in this section referred to as the ''Commission'').

(2) MEMBERSHIP.—

(A) COMPOSITION.—The Commission shall be composed of 16 members of whom—

(i) 1 shall be appointed by the Chairman of the Committee on Armed Services of the Senate;

(ii) 1 shall be appointed by the ranking member of the Committee on Armed Services of the Senate;

(iii) 1 shall be appointed by the Chairman of the Committee on Armed Services of the House of Representatives;

(iv) 1 shall be appointed by the ranking member of the Committee on Armed Services of the House of Representatives;

(v) 1 shall be appointed by the Chairman of the Committee on Foreign Relations of the Senate;

(vi) 1 shall be appointed by the ranking member of the Committee on Foreign Relations of the Senate;

(vii) 1 shall be appointed by the Chairman of the Committee on Foreign Affairs of the House of Representatives;

(viii) 1 shall be appointed by the ranking member of the Committee on Foreign Affairs of the House of Representatives;

(ix) 1 shall be appointed by the Chairman of the Select Committee on Intelligence of the Senate;

(x) 1 shall be appointed by the ranking member of the Select Committee on Intelligence of the Senate.

(xi) 1 shall be appointed by the Chairman of the Permanent Select Committee on Intelligence of the House of Representatives;

(xii) 1 shall be appointed by the ranking member of the Permanent Select Committee on Intelligence of the House of Representatives;

(xiii) 1 shall be appointed by the majority leader of the Senate;

(xiv) 1 shall be appointed by the minority leader of the Senate;

(xv) 1 shall be appointed by the Speaker of the House of Representatives; and

(xvi) 1 shall be appointed by the Minority Leader of the House of Representatives.

(B) QUALIFICATIONS.—It is the sense of Congress that each member of the Commission appointed under subparagraph (A) should have significant professional experience in national security, such as a position in—

(i) the Department of Defense;

(ii) the Department of State;

(iii) the intelligence community;

(iv) the United States Agency for International Development; or

(v) an academic or scholarly institution.

(C) PROHIBITIONS.—A member of the Commission appointed under subparagraph (A) may not—

(i) be a current member of Congress;

(ii) be a former member of Congress who served in Congress after January 3, 2001;

(iii) be a current or former registrant under the Foreign Agents Registration Act of 1938 (22 U.S.C. 611 et seq.);

(iv) have previously investigated Afghanistan policy or the war in Afghanistan through employment in the office of a relevant inspector general;

(v) have been the sole owner or had a majority stake in a company that held any United States or coalition defense contract providing goods or services to activities by the United States Government or coalition in Afghanistan during the applicable period; or

(vi) have served, with direct involvement in actions by the United States Government in Afghanistan during the time the relevant official served, as—

(I) a cabinet secretary or national security adviser to the President; or

(II) a four-star flag officer, Under Secretary, or more senior official in the Department of Defense or the Department of State.

(D) DATE.—

(i) IN GENERAL.—The appointments of the members of the Commission shall be made not later than 60 days after the date of enactment of this Act.

(ii) FAILURE TO MAKE APPOINTMENT.—If an appointment under subparagraph (A) is not made by the appointment date specified in clause (i)—

(I) the authority to make such appointment shall expire; and

(II) the number of members of the Commission shall be reduced by the number equal to the number of appointments not made.

(3) PERIOD OF APPOINTMENT; VACANCIES.—

(A) IN GENERAL.—A member of the Commission shall be appointed for the life of the Commission.

(B) VACANCIES.—A vacancy in the Commission—

(i) shall not affect the powers of the Commission; and

(ii) shall be filled in the same manner as the original appointment.

(4) MEETINGS.—

(A) INITIAL MEETING.—Not later than 30 days after the date on which all members of the Commission have been appointed, the Commission shall hold the first meeting of the Commission.

(B) FREQUENCY.—The Commission shall meet at the call of the Co-Chairpersons.

(C) QUORUM.—A majority of the members of the Commission shall constitute a quorum, but a lesser number of members may hold hearings.

(5) CO-CHAIRPERSONS.—The Commission shall select, by a simple majority vote—

(A) 1 Co-Chairperson from the members of the Commission appointed by chairpersons of the appropriate congressional committees; and

(B) 1 Co-Chairperson from the members of the Commission appointed by the ranking members of the appropriate congressional committees.

(d) PURPOSE OF COMMISSION.— The purpose of the Commission is—

(1) to examine the key strategic, diplomatic, and operational decisions that pertain to the war in Afghanistan during the relevant period, including decisions, assessments, and events that preceded the war in Afghanistan; and

(2) to develop a series of lessons learned and recommendations for the way forward that will inform future decisions by Congress and policymakers throughout the United States Government.

(e) DUTIES OF COMMISSION.—

(1) STUDY.—

(A) IN GENERAL.—The Commission shall conduct a thorough study of all matters relating to combat operations, reconstruction and security force assistance activities, intelligence operations, and diplomatic activities of the United States pertaining to the Afghanistan during the period beginning September 1, 1996, and ending August 30, 2021.

(B) MATTERS STUDIED.—The matters studied by the Commission shall include—

(i) for the time period specified under subparagraph (A)—

(I) the policy objectives of the United States Government, including—

(aa) military objectives;

(bb) diplomatic objectives;

(cc) development objectives; and

(dd) intelligence objectives;

(II) significant decisions made by the United States, including the development of options presented to policymakers;

(III) the efficacy of efforts by the United States Government in meeting the objectives described in clause (i), including an analysis of —

(aa) military efforts;

(bb) diplomatic efforts;

(cc) development efforts; and

(dd) intelligence efforts; and

(IV) the efficacy of counterterrorism efforts against al Qaeda, the Islamic State Khorasan Province, and other foreign terrorist organizations in degrading the will and capabilities of such organizations—

(aa) to mount external attacks against the United States mainland or its allies and partners; or

(bb) to threaten regional stability in Afghanistan and neighboring countries.

(ii) the efficacy of metrics, measures of effectiveness, and milestones used to assess progress of diplomatic, military, and intelligence efforts;

(iii) the efficacy of interagency planning and execution process by the United States Government;

(iv) factors that led to the collapse of the Afghan National Defense Security Forces in 2021, including—

(I) training;

(II) assessment methodologies;

(III) building indigenous forces on western models;

(IV) reliance on technology and logistics support; and

(V) reliance on warfighting enablers provided by the United States;

(v) the efficacy of counter-corruption efforts to include linkages to diplomatic lines of effort, linkages to foreign and security assistance, and assessment methodologies;

(vi) the efficacy of counter-narcotic efforts to include alternative livelihoods, eradication, interdiction, and education efforts;

(vii) the role of countries neighboring Afghanistan in contributing to the instability of Afghanistan;

(viii) varying diplomatic approaches between Presidential administrations;

(ix) the extent to which the intelligence community did or did not fail to provide sufficient warning about the probable outcomes of a withdrawal of coalition military support from Afghanistan, including as it relates to—

(I) the capability and sustainability of the Afghanistan National Defense Security Forces;

(II) the sustainability of the Afghan central government, absent coalition support;

(III) the extent of Taliban control over Afghanistan over time with respect to geographic territory, governance, and influence; and

(IV) the likelihood of the Taliban regaining control of Afghanistan at various levels of United States and coalition support, including the withdrawal of most or all United States or coalition support;

(x) the extent to which intelligence products related to the state of the conflict in Afghanistan and the effectiveness of the Afghanistan National Defense Security Forces complied with intelligence community-wide analytic tradecraft standards and fully reflected the divergence of analytic views across the intelligence community;

(xi) an evaluation of whether any element of the United States Government inappropriately restricted access to data from elements of the intelligence community, Congress, or the Special Inspector General for Afghanistan Reconstruction (SIGAR) or any other oversight body such as other inspectors general or the Gpvernment Accountability Office, including through the use of overclassification; and

(xii) the extent to which public representations of the situation in Afghanistan before Congress by United States Government officials were not consistent with the most recent formal assessment of the intelligence community at the time those representations were made.

(2) REPORT REQUIRED.—

(A) IN GENERAL.—

(i) ANNUAL REPORT.—

(I) IN GENERAL.—Not later than 1 year after the date of the initial meeting of the Commission, and annually thereafter, the Commission shall submit to the appropriate congressional committees a report describing the progress of the activities of the Commission as of the date of such report, including any findings, recommendations, or lessons learned endorsed by the Commission.

(II) ADDENDA.—Any member of the Commission may submit an addendum to a report required under subclause (I) setting

forth the separate views of such member with respect to any matter considered by the Commission.

(III) BRIEFING.—On the date of the submission of the first annual report, the Commission shall brief Congress.

(ii) FINAL REPORT.—

(I) SUBMISSION.—Not later than 3 years after the date of the initial meeting of the Commission, the Commission shall submit to Congress a report that contains a detailed statement of the findings, recommendations, and lessons learned endorsed by the Commission.

(II) ADDENDA.—Any member of the Commission may submit an addendum to the report required under subclause (I) setting forth the separate views of such member with respect to any matter considered by the Commission.

(III) EXTENSION.—The Commission may submit the report required under subclause (I) at a date that is not more than 1 year later than the date specified in such clause if agreed to by the chairperson and ranking member of each of the appropriate congressional committees.

(B) FORM.—The report required by paragraph (1)(B) shall be submitted and publicly released on a Government website in unclassified form but may contain a classified annex.

(C) SUBSEQUENT REPORTS ON DECLASSIFICATION.—

(i) IN GENERAL.—Not later than 4 years after the date that the report required by subparagraph (A)(ii) is submitted, each relevant agency of jurisdiction shall submit to the committee of jurisdiction a report on the efforts of such agency to declassify such annex.

(ii) CONTENTS.—Each report required by clause (i) shall include—

(I) a list of the items in the classified annex that the agency is working to declassify at the time of the report and an estimate of the timeline for declassification of such items;

(II) a broad description of items in the annex that the agency is declining to declassify at the time of the report; and

(III) any justification for withholding declassification of certain items in the annex and an estimate of the timeline for declassification of such items.

(f) POWERS OF COMMISSION.—

(1) HEARINGS.—The Commission may hold such hearings, take such testimony, and receive such evidence as the Commission considers necessary to carry out its purpose and functions under this section.

(2) ASSISTANCE FROM FEDERAL AGENCIES.—

(A) INFORMATION.—

(i) IN GENERAL.—The Commission may secure directly from a Federal department or agency such information as the Commission considers necessary to carry out this section.

(ii) FURNISHING INFORMATION.—Upon receipt of a written request by the Co-Chairpersons of the Commission, the head of the department or agency shall expeditiously furnish the information to the Commission.

(B) SPACE FOR COMMISSION.—Not later than 30 days after the date of the enactment of this Act, the Administrator of General Services, in consultation with the Commission, shall identify and make available suitable excess space within the Federal space inventory to house the operations of the Commission. If the Administrator of General Services is not able to make such suitable excess space available within such 30-day period, the Commission may lease space to the extent that funds are available for such purpose.

(3) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the Federal Government.

(4) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services, goods, and property from non-Federal entities for the purposes of aiding and facilitating the work of the Commission. The authority in this subsection does not extend to gifts of money. Gifts accepted under this authority shall be documented, and conflicts of interest or the appearance of conflicts of interest shall be avoided. Subject to the authority in this section, commissioners shall otherwise comply with rules set forth by the Select Committee on Ethics of the Senate and the Committee on Ethics of the House of Representatives governing employees of the Senate and the House of Representatives.

(5) LEGISLATIVE ADVISORY COMMITTEE.—The Commission shall operate as a legislative advisory committee and shall not be subject to the provisions of the Federal Advisory Committee Act (Public Law 92–463; 5 U.S.C. App) or section 552b, United States Code (commonly known as the Government in the Sunshine Act).

(g) COMMISSION PERSONNEL MATTERS.—

(1) COMPENSATION OF MEMBERS.—A member of the Commission who is not an officer or employee of the Federal Government shall be compensated at a rate equal to the daily equivalent of the annual rate of basic pay prescribed for level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day (including travel time) during which the member is engaged in the performance of the duties of the Commission.

(2) TRAVEL EXPENSES.—A member of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Commission.

(3) STAFF.—

(A) STATUS AS FEDERAL EMPLOYEES.—Notwithstanding the requirements of section 2105 of title 5, United States Code, including the required supervision under subsection (a)(3) of such section, the members of the commission shall be deemed to be Federal employees.

(B) EXECUTIVE DIRECTOR.—The Commission shall appoint and fix the rate of basic pay for an Executive Director in accordance with section 3161(d) of title 5, United States Code.

(C) PAY.—The Executive Director, with the approval of the Commission, may appoint and fix the rate of basic pay for additional personnel as staff of the Commission in accordance with section 3161(d) of title 5, United States Code.

(4) DETAIL OF GOVERNMENT EMPLOYEES.—A Federal Government employee may be detailed to the Commission without reimbursement, and such detail shall be without interruption or loss of civil service status or privilege.

(5) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES.—The Co-Chairpersons of the Commission may procure temporary and intermittent services under section 3109(b) of title 5, United States Code, at rates for individuals that do not exceed the daily equivalent of the annual rate of basic pay prescribed for level V of the Executive Schedule under section 5316 of that title.

(h) TERMINATION OF COMMISSION.—The Commission shall terminate 90 days after the date on which the Commission submits the report required under subsection (e)(2)(A)(ii).

(i) AUTHORIZATION OF APPROPRIATIONS.—

(1) INCREASE.—The amount authorized to be appropriated by section 4301 for Operation and Maintenance, Defense-wide, for the Office of the Secretary of Defense, is hereby increased by $3,000,000.

(2) OFFSET.—The amount authorized to be appropriated by section 4301 for Operation and Maintenance, Afghanistan Security Forces Fund, for Afghanistan Air Force, Line 090, is hereby reduced by $3,000,000.

SA 4804. Mr. YOUNG submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title XII, add the following:

SEC. 1253. REPORT ON GEOSTRATEGIC INTERESTS AND NATIONAL SECURITY IMPLICATIONS RELATED TO TRADE IN INDO-PACIFIC REGION.

(a) IN GENERAL.—Not later than 150 days after the date of the enactment of this Act, the United States Trade Representative, in coordination with the Secretary of Defense, the Secretary of State, the Secretary of Commerce, and the Secretary of Homeland Security, shall submit to Congress and make available to the public a report on geostrategic interests and national security implications related to trade in the Indo-Pacific region.

(b) ELEMENTS.—The report required by subsection (a) shall include an assessment of the following:

(1) How reductions in tariffs, revisions in government procurement rules, and other market access commitments by countries in the Indo-Pacific region could potentially affect United States producers and supply chains deemed critical for national security purposes.

(2) How agreements by those countries, including with respect to strengthening investment and intellectual property rights, could potentially affect the development by the United States of critical new technologies.

(3) How agreements by those countries relating to digital trade could potentially affect United States cybersecurity, including potential agreements entered into with the United States to promote cybersecurity and open data flows and to combat discriminatory practices and government censorship.

(4) How tariff and nontariff barriers imposed by those countries and trade agreements by those countries could broadly affect geostrategic United States interests, partnerships, and alliances.

(5) Current and predicted foreign direct investment in the Indo-Pacific region by the People's Republic of China.

(6) How agreements by those countries could counter the semiconductor policies of the Government of the People's Republic of China, particularly those policies that could lead to the transfer of intellectual property, research and development, and manufacturing to the People's Republic of China.

(c) PUBLIC HEARING.—The Trade Representative and the officials specified in subsection (a) shall jointly conduct a public hearing and invite witnesses to testify with respect to the elements described in subsection (b).

SA 4805. Ms. CORTEZ MASTO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year

2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title X, insert the following:

Subtitle ____—Veterans Matters

SEC. _____. EXTENSIONS OF CERTAIN PROVISIONS OF LAW RELATING TO BENEFITS PROVIDED UNDER DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE PROGRAMS DURING COVID–19 PANDEMIC.

(a) EXTENSION OF STUDENT VETERAN CORONAVIRUS RESPONSE ACT OF 2020.—Section 2 of the Student Veteran Coronavirus Response Act of 2020 (Public Law 116–140; 38 U.S.C. 3031 note), as amended by section 5202(a) of the Department of Veterans Affairs Expiring Authorities Act of 2020 (division E of Public Law 116–159), is further amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(b) EXTENSION OF PAYMENT OF WORK-STUDY ALLOWANCES DURING EMERGENCY SITUATION.—Section 3 of the Student Veteran Coronavirus Response Act of 2020 (38 U.S.C. 3485 note) is amended by striking ''During the covered period'' and inserting ''During the period beginning on March 1, 2020, and ending on June 1, 2022''.

(c) EXTENSION OF PERIOD FOR CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE BENEFITS FOR CERTAIN PROGRAMS OF EDUCATION CONVERTED TO DISTANCE LEARNING BY REASON OF EMERGENCIES AND HEALTH-RELATED SITUATIONS.—Section 1(b) of Public Law 116–128 (38 U.S.C. 3001 note prec.), as amended by section 5202(b) of the Department of Veterans Affairs Expiring Authorities Act of 2020 (division E of Public Law 116–159), is further amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(d) EXTENSION OF MODIFICATION OF TIME LIMITATIONS ON USE OF ENTITLEMENT TO MONTGOMERY GI BILL AND VOCATIONAL REHABILITATION AND TRAINING.—Section 1105 of the Johnny Isakson and David P. Roe, M.D. Veterans Health Care and Benefits Improvement Act of 2020 (Public Law 116–315) is amended by striking ''December 21, 2021'' each place it appears and inserting ''June 1, 2022''.

(e) EXTENSION OF CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE BENEFITS DURING COVID–19 EMERGENCY.—Section 1102(e) of the Johnny Isakson and David P. Roe, M.D. Veterans Health Care and Benefits Improvement Act of 2020 (Public Law 116–315) is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(f) EXTENSION OF PROVISIONS RELATING TO EFFECTS OF CLOSURE OF EDUCATIONAL INSTITUTION AND MODIFICATION OF COURSES BY REASON OF COVID–19 EMERGENCY.—Section 1103(h) of such Act is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(g) EXTENSION OF PROVISION RELATING TO PAYMENT OF EDUCATIONAL ASSISTANCE IN CASES OF WITHDRAWAL.—Section 1104(a) of such Act is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

(h) EXTENSION OF PROVISION RELATING TO APPRENTICESHIP OR ON-JOB TRAINING REQUIREMENTS.—Section 1106(b) of such Act is amended by striking ''December 21, 2021'' and inserting ''June 1, 2022''.

SEC. _____. MODIFICATIONS TO REQUIREMENTS FOR EDUCATIONAL INSTITUTIONS PARTICIPATING IN THE EDUCATIONAL ASSISTANCE PROGRAMS OF THE DEPARTMENT OF VETERANS AFFAIRS.

(a) WAIVER OF VERIFICATION OF ENROLLMENT FOR CERTAIN EDUCATIONAL INSTITUTIONS.—Section 3313(l) of title 38, United States Code, is amended by adding at the end the following new paragraph:

''(4) WAIVER.—The Secretary may waive the requirements of this subsection for an educational institution that the Secretary has determined uses a flat tuition and fee structure that would make the use of a second verification under this subsection unnecessary.''.

(b) LIMITATIONS ON AUTHORITY TO DISAPPROVE OF COURSES.—

(1) IN GENERAL.—Subsection (f) of section 3679 of title 38, United States Code, is amended—

(A) in paragraph (2)(B),

(i) by inserting '', except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance'' after ''assistance''; and

(ii) by adding at the end the following new subparagraph:

''(C) In determining whether a violation of subparagraph (B) has occurred, the State approving agency, or the Secretary when acting in the place of the State approving agency, shall construe the requirements of this paragraph in accordance with the regulations and guidance prescribed by the Secretary of Education under section 487(a)(20) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)(20)).'';

(B) by redesignating paragraph (7) as paragraph (8); and

(C) by inserting after paragraph (6) the following new paragraph (7):

''(7) This subsection shall not apply to an educational institution—

''(A) located in a foreign country; or

''(B) that provides to a covered individual consumer information regarding costs of the program of education (including financial aid available to such covered individual) using a form or template developed by the Secretary of Education.''.

(2) APPLICATION DATE.—The Secretary of Veterans Affairs may not carry out subsection (f) of section 3679 of title 38, United States Code, until August 1, 2022, except that, beginning on June 15, 2022, an educational institution may submit an application for a waiver under paragraph (5) of such subsection.

(3) CONFORMING AMENDMENTS.—Subsection (c) of section 3696 of such title is amended—

(A) by inserting ''(1)'' before ''An educational'';

(B) by inserting '', except for the recruitment of foreign students residing in foreign countries who are not eligible to receive Federal student assistance'' after ''assistance''; and

(C) by adding at the end the following new paragraph:

''(2) In determining whether a violation of paragraph (1) has occurred, the Under Secretary for Benefits shall construe the requirements of this paragraph in accordance with the regulations and guidance prescribed by the Secretary of Education under section 487(a)(20) of the Higher Education Act of 1965 (20 U.S.C. 1094(a)(20)).''.

(c) EXEMPTION OF FOREIGN SCHOOLS FROM CERTAIN REQUIREMENTS.—

(1) INFORMATION RELATING TO TESTS.—Section 3689(c) of title 38, United States Code, is amended by adding at the end the following new paragraph:

''(3) Subparagraph (G) of paragraph (1) shall not apply with respect to an educational institution located in a foreign country.''.

(2) EXAMINATION OF RECORDS.—Section 3690(c) of title 38, United States Code, is amended—

(A) by striking ''Notwithstanding'' and inserting ''(1) Except as provided in paragraph (2), notwithstanding''; and

(B) by adding at the end the following new paragraph:

''(2) Paragraph (1) does not apply to the records and accounts—

''(A) of an educational institution located in a foreign country; and

''(B) that pertain to an individual who is not receiving educational assistance under this chapter.''.

SEC. _____. CONTINUATION OF DEPARTMENT OF VETERANS AFFAIRS EDUCATIONAL ASSISTANCE BENEFITS FOR CERTAIN PROGRAMS OF EDUCATION CONVERTED TO DISTANCE LEARNING BY REASON OF EMERGENCIES AND HEALTH-RELATED SITUATIONS.

(a) IN GENERAL.—In the case of a program of education approved by a State approving agency, or the Secretary of Veterans Affairs when acting in the role of a State approving agency, that is converted from being offered on-site at an educational institution to being offered by distance learning by reason of an emergency or health-related situation, as determined by the Secretary, the Secretary may continue to provide educational assistance under the laws administered by the Secretary without regard to such conversion, including with respect to paying any—

(1) monthly housing stipends under chapter 33 of title 38, United States Code; or

(2) payments or subsistence allowances under chapters 30, 31, 32, and 35 of such title and chapters 1606 and 1607 of title 10, United States Code.

(b) APPLICABILITY PERIOD.—Subsection (a) shall apply during the period beginning on December 21, 2021, and ending on June 1, 2022.

(c) DEFINITIONS.—In this section:

(1) EDUCATIONAL INSTITUTION.—The term ''educational institution'' has the meaning given that term in section 3452 of title 38, United States Code, and includes an institution of higher learning (as defined in such section).

(2) PROGRAM OF EDUCATION.—The term ''program of education'' has the meaning given that term in section 3002 of title 38, United States Code.

(3) STATE APPROVING AGENCY.—The term ''State approving agency'' has the meaning given that term in section 3671 of title 38, United States Code.

SEC. _____. BUDGETARY EFFECTS.

(a) IN GENERAL.—Amounts provided to carry out the amendments made by this subtitle are designated as an emergency requirement pursuant to section 4(g) of the Statutory Pay-As-You-Go Act of 2010 (2 U.S.C. 933(g)).

(b) DESIGNATION IN SENATE.—In the Senate, amounts provided to carry out the amendments made by this subtitle are designated as an emergency requirement pursuant to section 4112(a) of H. Con. Res. 71 (115th Congress), the concurrent resolution on the budget for fiscal year 2018.

SA 4806. Ms. SMITH (for herself and Mr. YOUNG) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel

strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE ____—EMERGENCY PREPAREDNESS

SEC. __01. SHORT TITLE.

This title may be cited as the ''Advancing Emergency Preparedness Through One Health Act of 2021''.

SEC. __02. FINDINGS.

Congress finds the following:

(1) The term ''One Health'' reflects the interconnectedness of human health, animal health, and the environment. As technology and population growth facilitates increased interaction of human settlements with wildlife habitats and as international travel and trade increases, the interface between these elements will also continue to rise.

(2) When zoonotic diseases spill over to humans, there are often enormous health and economic costs. The World Bank estimates that, between 1997 and 2009, the global costs from six zoonotic outbreaks exceeded $80,000,000,000 and the Centers for Disease Control and Prevention estimates that there are annually 2,500,000,000 cases of zoonotic infections globally, resulting in 2,700,000 deaths.

(3) There are also immense effects on the agriculture sector. In 2014 and 2015, a high pathogenic avian influenza (HPAI) outbreak in the United States led to the cull of nearly 50,000,000 birds, and imposed up to approximately $3,300,000,000 in losses for poultry and egg farmers, animal feed producers, baked good production, and other related industries.

(4) Public health preparedness depends on agriculture in a variety of ways. For example, a wide range of vaccines, including those for influenza, yellow fever, rabies, and measles-mumps-rubella (MMR), are primarily cultivated in poultry eggs. Egg shortages resulting from zoonotic disease outbreaks could impose serious risks to vaccine manufacturing efforts.

(5) It is estimated that approximately 80 percent of potential pathogens likely to be used in bioterrorism or biowarfare are common zoonotic pathogens.

(6) While existing Federal Government initiatives related to One Health span multiple agencies, including the Centers for Disease Control and Prevention One Health office and the Department of Agriculture Animal and Plant Health Inspection Services' One Health Coordination Center, additional interagency coordination is necessary to help better prevent, prepare for, and respond to zoonotic disease outbreaks.

SEC. __03. INTERAGENCY ONE HEALTH PROGRAM.

(a) IN GENERAL.—The Secretary of the Interior, the Secretary of Health and Human Services, and the Secretary of Agriculture (referred to in this title as the ''Secretaries''), in coordination with the United States Agency for International Development, the Environmental Protection Agency, the Department of Homeland Security, the Department of Defense, the Department of Commerce, and other departments and agencies as appropriate, shall develop, publish, and submit to Congress a national One Health Framework (referred to in this title as the ''framework'') for coordinated Federal Activities under the One Health Program.

(b) NATIONAL ONE HEALTH FRAMEWORK.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Secretaries, in cooperation with the United States Agency for International Development, the Environmental Protection Agency, the Department of Homeland Security, the Department of Defense, the Department of Commerce, and other departments and agencies as appropriate, shall develop, publish, and submit to Congress a One Health Framework (referred to in this section as the ''framework'') for coordinated Federal activities under the One Health Program.

(2) CONTENTS OF FRAMEWORK.—The framework described in paragraph (1) shall describe existing efforts and contain recommendations for building upon and complementing the activities of the Department of the Interior, the Centers for Disease Control and Prevention, the Food and Drug Administration, the Office of the Assistant Secretary for Preparedness and Response, the Department of Agriculture, the United States Agency for International Development, the Environmental Protection Agency, the National Institutes of Health, the Department of Homeland Security, and other departments and agencies, as appropriate, and shall—

(A) assess, identify, and describe, as appropriate, existing activities of Federal agencies and departments under the One Health Program and consider whether all relevant agencies are adequately represented;

(B) for the 10-year period beginning in the year the framework is submitted, establish specific Federal goals and priorities that most effectively advance—

(i) scientific understanding of the connections between human, animal, and environmental health;

(ii) coordination and collaboration between agencies involved in the framework including sharing data and information, engaging in joint fieldwork, and engaging in joint laboratory studies related to One Health;

(iii) identification of priority zoonotic diseases and priority areas of study;

(iv) surveillance of priority zoonotic diseases and their transmission between animals and humans;

(v) prevention of priority zoonotic diseases and their transmission between animals and humans;

(vi) protocol development to improve joint outbreak response to and recovery from zoonotic disease outbreaks in animals and humans; and

(vii) workforce development to prevent and respond to zoonotic disease outbreaks in animals and humans;

(C) describe specific activities required to achieve the goals and priorities described in subparagraph (B), and propose a timeline for achieving these goals;

(D) identify and expand partnerships, as appropriate, among Federal agencies, States, Indian tribes, academic institutions, nongovernmental organizations, and private entities in order to develop new approaches for reducing hazards to human and animal health and to strengthen understanding of the value of an integrated approach under the One Health Program to addressing public health threats in a manner that prevents duplication;

(E) identify best practices related to State and local-level research coordination, field activities, and disease outbreak preparedness, response, and recovery related to One Health; and

(F) provide recommendations to Congress regarding additional action or legislation that may be required to assist in establishing the One Health Program.

(3) ADDENDUM.—Not later than 3 years after the creation of the framework, the Secretaries, in coordination with the agencies described in paragraph (1), shall submit to Congress an addendum to the framework that describes the progress made in advancing the activities described in the framework.

(c) AUTHORIZATION OF APPROPRIATIONS.—To carry out this section, there is authorized to be appropriated such sums as may be necessary.

SEC. __04. GAO REPORT.

Not later than 2 years after the date of the submission of the addendum under section __03(b)(3), the Comptroller General of the United States shall submit to Congress a report that—

(1) details existing collaborative efforts between the Department of the Interior, the Centers for Disease Control and Prevention, the Food and Drug Administration, the Department of Agriculture, the United States Agency for International Development, the Environmental Protection Agency, the National Institutes of Health, the Department of Homeland Security, and other departments and agencies to prevent and respond to zoonotic disease outbreaks in animals and humans; and

(2) contains an evaluation of the framework and the specific activities requested to achieve the framework.

SA 4807. Ms. SMITH (for herself, Mr. CASSIDY, and Ms. WARREN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1064. STUDY AND REPORT ON THE REDISTRIBUTION OF COVID–19 VACCINE DOSES THAT WOULD OTHERWISE EXPIRE TO FOREIGN COUNTRIES AND ECONOMIES.

(a) STUDY.—

(1) IN GENERAL.—The Secretary of Health and Human Services, in consultation with the Secretary of State and the Administrator of the United States Agency for International Development, shall conduct a study to identify and analyze the logistical prerequisites for the collection of unused and unexpired doses of the COVID–19 vaccine in the United States and for the distribution of such doses to foreign countries and economies.

(2) MATTERS STUDIED.—The matters studied by the Secretary of Health and Human Services under paragraph (1) shall include—

(A) options for the collection of unused and unexpired doses of the COVID–19 vaccine from entities in the United States;

(B) methods for the collection and shipment of such doses to foreign countries and economies;

(C) methods for ensuring the appropriate storage and handling of such doses during and following the distribution and delivery of the doses to such countries and economies;

(D) the capacity and capability of foreign countries and economies receiving such doses to distribute and administer the doses while assuring their safety and quality;

(E) the minimum supply of doses of the COVID–19 vaccine necessary to be retained within the United States; and

(F) other Federal agencies with which the heads of the relevant agencies should coordinate to accomplish the tasks described in subparagraphs (A) through (E) and the degree of coordination necessary between such agencies.

(b) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Health and Human Services, in consultation with the other heads of the relevant agencies, shall submit to the appropriate congressional committees a report on the results of the study conducted under subsection (a).

(c) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Health, Education, Labor, and Pensions, and the Committee on Foreign Relations of the Senate; and

(B) the Committee on Energy and Commerce, and the Committee on Foreign Affairs of the House of Representatives.

(2) RELEVANT AGENCIES.—The term ''relevant agencies'' means—

(A) the Department of Health and Human Services;

(B) the Department of State; and

(C) the United States Agency for International Development.

SA 4808. Mrs. FEINSTEIN (for herself, Ms. ERNST, Mr. DURBIN, Ms. COLLINS, Ms. HIRONO, Ms. ROSEN, Mr. PETERS, Mr. CORNYN, and Ms. DUCKWORTH) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XII, add the following:

SEC. 1216. STATUS OF WOMEN AND GIRLS IN AFGHANISTAN.

(a) FINDINGS.—Congress finds the following:

(1) Since May 2021, the escalation of violent conflict in Afghanistan has forcibly displaced an estimated 655,000 civilians, and 80 percent of those forced to flee are women and children.

(2) Since regaining control of Afghanistan in August 2021, the Taliban have taken actions reminiscent of their brutal rule in the late 1990s, including by cracking down on protesters, detaining and beating journalists, reestablishing the Ministry for the Promotion of Virtue and Prevention of Vice, and requiring women to study at universities in gender-segregated classrooms while wearing Islamic attire.

(3) Until the Taliban assumed control of the country in August 2021, the women and girls of Afghanistan had achieved much since 2001, even as insecurity, poverty, underdevelopment, and patriarchal norms continued to limit their rights and opportunities in much of Afghanistan.

(4) Through strong support from the United States and the international community—

(A) female enrollment in public schools in Afghanistan continued to increase through 2015, with an estimated high of 50 percent of school age girls attending; and

(B) by 2019—

(i) women held political leadership positions, and women served as ambassadors; and

(ii) women served as professors, judges, prosecutors, defense attorneys, police, military members, health professionals, journalists, humanitarian and developmental aid workers, and entrepreneurs.

(5) Efforts to empower women and girls in Afghanistan continue to serve the national interests of Afghanistan and the United States because women are sources of peace and economic progress.

(6) With the return of Taliban control, the United States has little ability to preserve the human rights of women and girls in Afghanistan, and those women and girls may again face the intimidation and marginalization they faced under the last Taliban regime.

(7) Women and girls in Afghanistan are again facing gender-based violence, including—

(A) forced marriage;

(B) intimate partner and domestic violence;

(C) sexual harassment;

(D) sexual violence, including rape; and

(E) emotional and psychological violence.

(8) Gender-based violence has always been a significant problem in Afghanistan and is expected to become more widespread with the Taliban in control. In 2020, even before the Taliban assumed control of the country, some studies projected that 87 percent of Afghan women and girls will experience at least one form of gender-based violence in their lifetime, with 62 percent experiencing multiple incidents of such violence.

(9) Prior to the Taliban takeover in August 2021, approximately 7,000,000 people in Afghanistan lacked or had limited access to emergency and primary health services as a result of inadequate public health coverage, weak health systems, and conflict-related interruptions in care.

(10) Women and girls faced additional challenges, as their access to prenatal, childbirth, and postpartum care was limited due to a shortage of female medical staff, cultural barriers, stigma and fears of reprisals following sexual violence, or other barriers to mobility, including security fears.

(11) Only approximately 50 percent of pregnant women and girls in Afghanistan deliver their children in a health facility with a professional attendant, which increases the risk of complications in childbirth and preventable maternal mortality.

(12) Food insecurity in Afghanistan is also posing a variety of threats to women and girls, as malnutrition weakens their immune systems and makes them more susceptible to infections, complications during pregnancy, and risks during childbirth.

(13) With the combined impacts of ongoing conflict and COVID–19, Afghan households increasingly resort to child marriage, forced marriage, and child labor to address food insecurity and other effects of extreme poverty.

(14) In Afghanistan, the high prevalence of anemia among adolescent girls reduces their ability to survive childbirth, especially when coupled with high rates of child marriage and forced marriage and barriers to accessing prenatal and childbirth services.

(b) SENSE OF CONGRESS.—It is the sense of Congress that—

(1) since 2001, organizations and networks promoting the empowerment of women and girls have been important engines of social, economic, and political development in Afghanistan;

(2) any future political order in Afghanistan should secure the political, economic, and social gains made by Afghan women and work to increase the equal treatment of women and girls;

(3) respecting the internationally recognized human rights of all people is essential to securing lasting peace and sustainable development in Afghanistan;

(4) in cooperation with international partners, the United States must endeavor to preserve the hard-won gains made in Afghanistan during the past two decades, particularly as related to the social, economic and political empowerment of women and girls in society;

(5) the continued provision of humanitarian assistance in Afghanistan should be targeted toward the most vulnerable, including for the protection, education, and well-being of women and girls;

(6) immediate and ongoing humanitarian needs in Afghanistan can only be met by a humanitarian response that includes formal agreements between local nongovernmental organizations and international partners that promotes the safe access and participation of female staff at all levels and across functional roles among all humanitarian actors; and

(7) a lack of aid would exacerbate the current humanitarian crisis and harm the well-being of women and girls in Afghanistan.

(c) POLICY OF THE UNITED STATES REGARDING THE RIGHTS OF WOMEN AND GIRLS OF AFGHANISTAN.—

(1) IN GENERAL.—It is the policy of the United States—

(A) to continue to support the internationally recognized human rights of women and girls in Afghanistan following the withdrawal of the United States Armed Forces from Afghanistan, including through mechanisms to hold all parties publicly accountable for violations of international humanitarian law and violations of such rights against women and girls;

(B) to strongly oppose any weakening of the political or economic rights of women and girls in Afghanistan;

(C) to use the voice and influence of the United States at the United Nations to promote, respect, and uphold the internationally recognized human rights of the women and girls of Afghanistan, including the right to safely work;

(D) to identify individuals who violate the internationally recognized human rights of women and girls in Afghanistan, such as by committing acts of murder, lynching, and grievous domestic violence against women, and to press for bringing those individuals to justice; and

(E) to systematically consult with Afghan women and girls on their needs and priorities in the development, implementation, and monitoring of humanitarian action, including women and girls who are part of the Afghan diaspora community.

(d) HUMANITARIAN ASSISTANCE AND AFGHAN WOMEN.—The Administrator of the United States Agency for International Development should work to ensure that Afghan women are employed and enabled to work in the delivery of humanitarian assistance in Afghanistan, to the extent practicable.

(e) REPORT ON WOMEN AND GIRLS IN AFGHANISTAN.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, and every 180 days thereafter through 2024, the Secretary of State shall submit to the appropriate committees of Congress, and make available to the public, a report that includes the following:

(A) An assessment of the status of women and girls in Afghanistan following the departure of United States and partner military forces, including with respect to access to primary and secondary education, jobs, primary and emergency health care, and legal protections and status.

(B) An assessment of the political and civic participation of women and girls in Afghanistan.

(C) An assessment of the prevalence of gender-based violence in Afghanistan.

(D) A report on funds for United States foreign assistance obligated or expended during the period covered by the report to advance

gender equality and the internationally recognized human rights of women and girls in Afghanistan, including funds directed toward local organizations promoting such rights of women and girls, that includes the following:

(i) The amounts awarded to principal recipients and sub-recipients for such purposes during the reporting period.

(ii) A description of each program for which such funds are used for such purposes.

(2) ASSESSMENT.—

(A) INPUT.—The assessment described in paragraph (1)(A) shall include the input of—

(i) Afghan women and girls;

(ii) organizations employing and working with Afghan women and girls; and

(iii) humanitarian organizations, including faith-based organizations, providing assistance in Afghanistan.

(B) SAFETY AND CONFIDENTIALITY.—In carrying out the assessment described in paragraph (1)(A), the Secretary shall, to the maximum extent practicable, ensure the safety and confidentiality of personal information of each individual who provides information from within Afghanistan.

(3) DEFINITION OF APPROPRIATE COMMITTEES OF CONGRESS.—In this subsection, the term ''appropriate committees of Congress'' means—

(A) the Committee on Foreign Relations and the Committee on Appropriations of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Appropriations of the House of Representatives.

SA 4809. Mr. WARNER submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title V, add the following:

SEC. 576. COUNTERING EXTREMISM IN THE ARMED FORCES.

(a) IN GENERAL.—The Secretary of Defense shall—

(1) promulgate policy that prohibits and defines participation in extremist activities;

(2) develop and implement programs, resources, and activities to counter extremism within the Armed Forces, including screening of publicly available information and Insider Threat Programs;

(3) collect and report data on incidents, allegations, investigations, disciplinary actions, and separations related to extremism, as well as publication of reports on these data in a regular, public, and transparent manner; and

(4) designate a senior official, to be known as the ''Senior Official for Countering Extremism'', within the Department of Defense as responsible for facilitation and coordination of the activities described in this subsection with personnel and readiness officials, law enforcement organizations, security organizations, insider threat programs, and watch lists related to extremism in the Armed Forces.

(b) TRAINING AND EDUCATION.—

(1) IN GENERAL.—The Secretary of each military department, in coordination with the Senior Official for Countering Extremism, shall develop and implement training and education programs and related materials to assist members of the Armed Forces and civilian employees of the Department of Defense in identifying, preventing, responding to, reporting, and mitigating the risk of extremist activities.

(2) CONTENT.—The training and education described in paragraph (1) shall include specific material for activities determined by the Senior Official for Countering Extremism as high risk for extremist activities, including recruitment activities and separating members of the Armed Forces.

(3) REQUIREMENTS.—The Secretary of Defense, in consultation with the Secretary of Homeland Security, shall provide the training and education described paragraph (1)—

(A) to a member of the Armed Forces, civilian employee of the Department of Defense, or an individual in a pre-commissioning program no less than once a year;

(B) to a member of the Armed Forces whose discharge (regardless of character of discharge) or release from active duty is anticipated as of a specific date within the time period specified under section 1142(a)(3) of title, United States Code;

(C) to a member of the Armed Forces performing recruitment activities within the 30 days prior to commencing such activities; and

(D) additionally as determined by the Secretary of Defense.

(c) PROGRESS REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the Committees on Armed Services of the Senate and House of Representatives a report on the status of the implementation of this section.

SA 4810. Mrs. GILLIBRAND (for herself, Mr. RUBIO, Mr. HEINRICH, Mr. BLUNT, and Mr. GRAHAM) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title XV, insert the following:

SEC. _____. ESTABLISHMENT OF STRUCTURE AND AUTHORITIES TO ADDRESS UNIDENTIFIED AERIAL PHENOMENA.

(a) ESTABLISHMENT OF ANOMALY SURVEILLANCE, TRACKING, AND RESOLUTION OFFICE.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall, in coordination with the Director of National Intelligence, establish an office within an appropriate component of the Department of Defense, or within a joint organization of the Department of Defense and the Office of the Director of National Intelligence, to assume—

(A) the duties of the Unidentified Aerial Phenomenon Task Force, as in effect on the day before the date of the enactment of this Act; and

(B) such other duties as are required by this section.

(2) DESIGNATION.—The office established under paragraph (1) shall be known as the ''Anomaly Surveillance, Tracking, and Resolution Office'' (in this section referred to as the ''Office'').

(3) TERMINATION OR SUBORDINATION OF PRIOR TASK FORCE.—Upon the establishment of the Anomaly Surveillance, Tracking, and Resolution Office, the Secretary shall terminate the Unidentified Aerial Phenomenon Task Force or subordinate it to the Office.

(b) FACILITATION OF REPORTING AND DATA SHARING.—The Director and the Secretary shall each, in coordination with each other, require that—

(1) each element of the intelligence community and the Department, with any data that may be relevant to the investigation of unidentified aerial phenomena, make such data available immediately to the Office; and

(2) military and civilian personnel employed by or under contract to the Department or an element of the intelligence community shall have access to procedures by which they shall report incidents or information, including adverse physiological effects, involving or associated with unidentified aerial phenomena directly to the Office.

(c) DUTIES.—The duties of the Office established under subsection (a) shall include the following:

(1) Developing procedures to synchronize and standardize the collection, reporting, and analysis of incidents, including adverse physiological effects, regarding unidentified aerial phenomena across the Department and in consultation with the intelligence community.

(2) Developing processes and procedures to ensure that such incidents from each component of the Department and each element of the intelligence community are reported and incorporated in a centralized repository.

(3) Establishing procedures to require the timely and consistent reporting of such incidents.

(4) Evaluating links between unidentified aerial phenomena and adversarial foreign governments, other foreign governments, or nonstate actors.

(5) Evaluating the threat that such incidents present to the United States.

(6) Consulting with other departments and agencies of the Federal Government, as appropriate, including the Federal Aviation Administration, the National Aeronautics and Space Administration, the Department of Homeland Security, the National Oceanic and Atmospheric Administration, and the Department of Energy.

(7) Consulting with allies and partners of the United States, as appropriate, to better assess the nature and extent of unidentified aerial phenomena.

(8) Preparing reports for Congress, in both classified and unclassified form, as required by subsections (h) and (i).

(d) EMPLOYMENT OF LINE ORGANIZATIONS FOR FIELD INVESTIGATIONS OF UNIDENTIFIED AERIAL PHENOMENA.—

(1) IN GENERAL.—The Secretary shall, in coordination with the Director, designate line organizations within the Department of Defense and the intelligence community that possess appropriate expertise, authorities, accesses, data, systems, platforms, and capabilities to rapidly respond to, and conduct field investigations of, incidents involving unidentified aerial phenomena under the direction of the Office.

(2) PERSONNEL, EQUIPMENT, AND RESOURCES.—The Secretary, in coordination with the Director, shall take such actions as may be necessary to ensure that the designated organization or organizations have available adequate personnel with requisite expertise, equipment, transportation, and other resources necessary to respond rapidly to incidents or patterns of observations of unidentified aerial phenomena of which the Office becomes aware.

(e) UTILIZATION OF LINE ORGANIZATIONS FOR SCIENTIFIC, TECHNOLOGICAL, AND OPERATIONAL ANALYSES OF DATA ON UNIDENTIFIED AERIAL PHENOMENA.—

(1) IN GENERAL.—The Secretary, in coordination with the Director, shall designate one or more line organizations that will be primarily responsible for scientific, technical, and operational analysis of data gathered by field investigations conducted under subsection (d), or data from other sources, including testing of materials, medical studies, and development of theoretical models to better understand and explain unidentified aerial phenomena.

(2) AUTHORITY.—The Secretary and the Director shall promulgate such directives as necessary to ensure that the designated line organizations have authority to draw on special expertise of persons outside the Federal Government with appropriate security clearances.

(f) INTELLIGENCE COLLECTION AND ANALYSIS PLAN.—

(1) IN GENERAL.—The head of the Office shall supervise the development and execution of an intelligence collection and analysis plan on behalf of the Secretary and the Director to gain as much knowledge as possible regarding the technical and operational characteristics, origins, and intentions of unidentified aerial phenomena, including the development, acquisition, deployment, and operation of technical collection capabilities necessary to detect, identify, and scientifically characterize unidentified aerial phenomena.

(2) USE OF RESOURCES AND CAPABILITIES.—In developing the plan required by paragraph (1), the head of the Office shall consider and propose, as appropriate, the use of any resource, capability, asset, or process of the Department and the intelligence community.

(g) SCIENCE PLAN.—The head of the Office shall supervise the development and execution of a science plan on behalf of the Secretary and the Director to develop and test, as practicable, scientific theories to account for characteristics and performance of unidentified aerial phenomena that exceed the known state of the art in science or technology, including in the areas of propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, and power generation, and to provide the foundation for potential future investments to replicate any such advanced characteristics and performance.

(h) ASSIGNMENT OF PRIORITY.—The Director, in consultation with, and with the recommendation of the Secretary, shall assign an appropriate level of priority within the National Intelligence Priorities Framework to the requirement to understand, characterize, and respond to unidentified aerial phenomena.

(i) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated such sums as may be necessary to carry out the work of the Office, including—

(1) general intelligence gathering and intelligence analysis; and

(2) strategic defense, space defense, defense of controlled air space, defense of ground, air, or naval assets, and related purposes.

(j) ANNUAL REPORT.—

(1) REQUIREMENT.—Not later than October 31, 2022, and annually thereafter until October 31, 2026, the Secretary in consultation with the Director, shall submit to the appropriate committees of Congress a report on unidentified aerial phenomena.

(2) ELEMENTS.—Each report under paragraph (1) shall include, with respect to the year covered by the report, the following information:

(A) An analysis of data and intelligence received through reports of unidentified aerial phenomena.

(B) An analysis of data relating to unidentified aerial phenomena collected through—

(i) geospatial intelligence

(ii) signals intelligence;

(iii) human intelligence; and

(iv) measurement and signals intelligence.

(C) The number of reported incidents of unidentified aerial phenomena over restricted air space of the United States.

(D) An analysis of such incidents identified under subparagraph (C).

(E) Identification of potential aerospace or other threats posed by unidentified aerial phenomena to the national security of the United States.

(F) An assessment of any activity regarding unidentified aerial phenomena that can be attributed to one or more adversarial foreign governments.

(G) Identification of any incidents or patterns regarding unidentified aerial phenomena that indicate a potential adversarial foreign government may have achieved a breakthrough aerospace capability.

(H) An update on the coordination by the United States with allies and partners on efforts to track, understand, and address unidentified aerial phenomena.

(I) An update on any efforts to capture or exploit discovered unidentified aerial phenomena.

(J) An assessment of any health-related effects for individuals who have encountered unidentified aerial phenomena.

(K) The number of reported incidents, and descriptions thereof, of unidentified aerial phenomena associated with military nuclear assets, including strategic nuclear weapons and nuclear-powered ships and submarines.

(L) In consultation with the Administrator of the National Nuclear Security Administration, the number of reported incidents, and descriptions thereof, of unidentified aerial phenomena associated with facilities or assets associated with the production, transportation, or storage of nuclear weapons or components thereof.

(M) In consultation with the Chairman of the Nuclear Regulatory Commission, the number of reported incidents, and descriptions thereof, of unidentified aerial phenomena or drones of unknown origin associated with nuclear power generating stations, nuclear fuel storage sites, or other sites or facilities regulated by the Nuclear Regulatory Commission.

(N) The names of the line organizations that have been designated to perform the specific functions imposed by subsections (d) and (e) of this section, and the specific functions for which each such line organization has been assigned primary responsibility.

(3) FORM.— Each report submitted under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(k) SEMIANNUAL BRIEFINGS.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act and not less frequently than semiannually thereafter until December 31, 2026, the head of the Office shall provide the classified briefings on unidentified aerial phenomena to—

(A) the Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(2) FIRST BRIEFING.—The first briefing provided under paragraph (1) shall include all incidents involving unidentified aerial phenomena that were reported to the Unidentified Aerial Phenomena Task Force or to the Office after June 24, 2021, regardless of the date of occurrence of the incident.

(3) SUBSEQUENT BRIEFINGS.—Each briefing provided subsequent to the first briefing described in paragraph (2) shall include, at a minimum, all events relating to unidentified aerial phenomena that occurred during the previous 180 days, and events relating to unidentified aerial phenomena that were not included in an earlier briefing due to delay in an incident reaching the reporting system or other such factors.

(4) INSTANCES IN WHICH DATA WAS NOT SHARED.—For each briefing period, the Chairman and Vice Chairman or Ranking Member of the Committee on Armed Services and the Select Committee on Intelligence of the Senate and the Committee on Armed Services and the Permanent Select Committee on Intelligence of the House of Representatives shall receive an enumeration of any instances in which data related to unidentified aerial phenomena was denied to the Office because of classification restrictions on that data or for any other reason.

(l) AERIAL AND TRANSMEDIUM PHENOMENA ADVISORY COMMITTEE.—

(1) ESTABLISHMENT.—(A) Not later than October 1, 2022, the Secretary and the Director shall establish an advisory committee for the purpose of—

(i) advising the Office in the execution of the duties of the Office as provided by this subsection; and

(ii) advising the Secretary and the Director regarding the gathering and analysis of data, and scientific research and development pertaining to unidentified aerial phenomena.

(B) The advisory committee established under subparagraph (A) shall be known as the ''Aerial and Transmedium Phenomena Advisory Committee'' (in this subparagraph the ''Committee'').

(2) MEMBERSHIP.—(A) Subject to subparagraph (B), the Committee shall be composed of members as follows:

(i) 20 members selected by the Secretary as follows:

(I) Three members selected from among individuals recommended by the Administrator of the National Astronautics and Space Administration.

(II) Two members selected from among individuals recommended by the Administrator of the Federal Aviation Administration.

(III) Two members selected from among individuals recommended by the President of the National Academies of Sciences.

(IV) Two members selected from among individuals recommended by the President of the National Academy of Engineering.

(V) One member selected from among individuals recommended by the President of the National Academy of Medicine.

(VI) Three members selected from among individuals recommended by the Director of the Galileo Project at Harvard University.

(VII) Two members selected from among individuals recommended by the Board of Directors of the Scientific Coalition for Unidentified Aerospace Phenomena Studies.

(VIII) Two members selected from among individuals recommended by the President of the American Institute of Astronautics and Aeronautics.

(IX) Two members selected from among individuals recommended by the Director of the Optical Technology Center at Montana State University.

(X) One member selected from among individuals recommended by the president of the American Society for Photogrammetry and Remote Sensing.

(ii) Up to five additional members, as the Secretary, in consultation with the Director, considers appropriate, selected from among individuals with requisite expertise, at least

3 of whom shall not be employees of any Federal Government agency or Federal Government contractor.

(B) No individual may be appointed to the Committee under subparagraph (A) unless the Secretary and the Directly jointly determine that the individual—

(i) qualifies for a security clearance at the secret level or higher;

(ii) possesses scientific, medical, or technical expertise pertinent to some aspect of the investigation and analysis of unidentified aerial phenomena; and

(iii) has previously conducted research or writing that demonstrates scientific, technological, or operational knowledge regarding aspects of the subject matter, including propulsion, aerodynamic control, signatures, structures, materials, sensors, countermeasures, weapons, electronics, power generation, field investigations, forensic examination of particular cases, analysis of open source and classified information regarding domestic and foreign research and commentary, and historical information pertaining to unidentified aerial phenomena.

(C) The Secretary and Director may terminate the membership of any individual on the Committee upon a finding by the Secretary and the Director jointly that the member no longer meets the criteria specified in this subsection.

(3) CHAIRPERSON.—The Secretary shall, in coordination with the Director, designate a temporary Chairperson of the Committee, but at the earliest practicable date the Committee shall elect a Chairperson from among its members, who will serve a term of 2 years, and is eligible for re-election.

(4) EXPERT ASSISTANCE, ADVICE, AND RECOMMENDATIONS.—(A) The Committee may, upon invitation of the head of the Office, provide expert assistance or advice to any line organization designated to carry out field investigations or data analysis as authorized by subsections (d) and (e).

(B) The Committee, on its own initiative, or at the request of the Director, the Secretary, or the head of the Office, may provide advice and recommendations regarding best practices with respect to the gathering and analysis of data on unidentified aerial phenomena in general, or commentary regarding specific incidents, cases, or classes of unidentified aerial phenomena.

(5) REPORT.—Not later than December 31, 2022, and not later than December 31 of each year thereafter, the Committee shall submit a report summarizing its activities and recommendations to the following:

(A) The Secretary.

(B) The Director.

(C) The head of the Office.

(D) The Committee on Armed Services, the Select Committee on Intelligence, and the Committee on Appropriations of the Senate.

(E) The Committee on Armed Services, the Permanent Select Committee on Intelligence, and the Committee on Appropriations of the House of Representatives.

(6) RELATION TO FACA.—For purposes of the Federal Advisory Committee Act (5 U.S.C. App.), the Committee shall be considered an advisory committee (as defined in section 3 of such Act, except as otherwise provided in the section or as jointly deemed warranted by the Secretary and the Director under section 4(b)(3) of such Act.

(7) TERMINATION OF COMMITTEE.—The Committee shall terminate on the date that is six years after the date of the establishment of the Committee.

(m) DEFINITIONS.—In this section:

(1) The term ''appropriate committees of Congress'' means—

(A) the Committee on Armed Services, the Select Committee on Intelligence, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Permanent Select Committee on Intelligence, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(2) The term ''intelligence community'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(3) The term ''transmedium objects or devices'' means objects or devices that are observed to transition between space and the atmosphere, or between the atmosphere and bodies of water, that are not immediately identifiable.

(4) The term ''unidentified aerial phenomena'' means—

(A) airborne objects that are not immediately identifiable;

(B) transmedium objects or devices; and

(C) submerged objects or devices that are not immediately identifiable and that display behavior or performance characteristics suggesting that they may be related to the subjects described in subparagraph (A) or (B).

SA 4811. Mr. TUBERVILLE (for himself and Mr. BRAUN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PROHIBITING THE INTERNAL REVENUE SERVICE FROM REQUIRING FINANCIAL INSTITUTIONS TO REPORT ON FINANCIAL TRANSACTIONS OF CUSTOMERS.

(a) IN GENERAL.—Subject to subsection (b), the Internal Revenue Service shall not be permitted to create or implement any new financial account information reporting program that—

(1) was not in effect as of October 1, 2021, and

(2) would require financial institutions to report data on financial accounts in an information return listing balances, transactions, transfers, or inflows or outflows of any kind.

(b) RULE OF CONSTRUCTION.—

(1) IN GENERAL.—Nothing in this section shall preempt, limit, or supersede, or be construed to preempt, limit, or supersede, any provision of, or requirement under, the Bank Secrecy Act or any regulations promulgated under such Act.

(2) DEFINITION.—For purposes of this subsection, the term ''Bank Secrecy Act'' means—

(A) section 21 of the Federal Deposit Insurance Act (12 U.S.C. 1829b),

(B) chapter 2 of title I of Public Law 91–508 (12 U.S.C. 1951 et seq.), and

(C) subchapter II of chapter 53 of title 31, United States Code.

SA 4812. Mr. TUBERVILLE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. PROHIBITING TSP INVESTMENT IN CHINA.

(a) FINDINGS.—Congress finds the following:

(1) The Thrift Savings Fund invests more than $700,000,000,000 on behalf of plan participants. As the guardian of the retirement funds of approximately 6,000,000 Federal civilian and military plan participants, it is critical that sums in the Thrift Savings Fund are not invested in securities linked to the economy of the People's Republic of China.

(2) Companies headquartered in the People's Republic of China have repeatedly committed corporate espionage, violated sanctions imposed by the United States, flouted international property laws, committed theft, and failed to comply with audit and regulatory standards designed to safeguard investors.

(3) The Thrift Savings Plan is known for its low management fees and comprehensive array of investment strategies. The provisions of this section, and the amendments made by this section, will not increase fees imposed on participants of the Thrift Savings Plan.

(4) The November 2017 selection of the MSCI ACWI Index by the Federal Retirement Thrift Investment Board, initially scheduled to be effective in 2020, would violate the terms of subsection (i) of section 8438 of title 5, United States Code, as added by subsection (b)(1) of this section.

(b) PROHIBITION ON ANY TSP FUND INVESTING IN ENTITIES BASED IN THE PEOPLE'S REPUBLIC OF CHINA.—

(1) IN GENERAL.—Section 8438 of title 5, United States Code, is amended by adding at the end the following:

''(i) Notwithstanding any other provision of this section, no fund established or overseen by the Board may include an investment in any security of—

''(1) an entity based in the People's Republic of China; or

''(2) any subsidiary that is owned or operated by an entity described in paragraph (1).''.

(2) DIVESTITURE OF ASSETS.—Not later than 30 days after the date of enactment of this Act, the Federal Retirement Thrift Investment Board established under section 8472(a) of title 5, United States Code, shall—

(A) review whether any sums in the Thrift Savings Fund are invested in violation of subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection;

(B) if any sums are invested in the manner described in subparagraph (A), divest those sums in a manner that is consistent with the legal and fiduciary duties provided under chapter 84 of that title, or any other applicable provision of law; and

(C) reinvest any sums divested under subparagraph (B) in investments that do not violate subsection (i) of section 8438 of that title, as added by paragraph (1) of this subsection.

(c) PROHIBITION ON INVESTMENT OF TSP FUNDS IN ENTITIES BASED IN THE PEOPLE'S REPUBLIC OF CHINA THROUGH THE TSP MUTUAL FUND WINDOW.—Section 8438(b)(5) of title 5, United States Code, is amended by adding at the end the following:

''(E) A mutual fund accessible through a mutual fund window authorized under this

paragraph may not include an investment in any security of—

''(i) an entity based in the People's Republic of China; or

''(ii) any subsidiary that is owned or operated by an entity described in clause (i).''.

SA 4813. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

TITLE LI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 5101. SHORT TITLE.

This title may be cited as the ''Cyber Incident Reporting Act of 2021''.

SEC. 5102. DEFINITIONS.

In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms ''covered cyber incident'', ''covered entity'', and ''cyber incident'' have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 5103 of this title.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 5203 of this division.

SEC. 5103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 5203(b) of this division—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

"Subtitle C—Cyber Incident Reporting

"SEC. 2230. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

''(3) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

''(4) COVERED ENTITY.—The term 'covered entity' means—

''(A) any Federal contractor; or

''(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

''(5) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2200.

''(6) CYBER THREAT.—The term 'cyber threat'—

''(A) has the meaning given the term 'cybersecurity threat' in section 2200; and

''(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

''(7) FEDERAL CONTRACTOR.—The term 'Federal contractor' means a business, nonprofit organization, or other private sector entity that holds a Federal Government contract or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity is a party only to—

''(A) a service contract to provide housekeeping or custodial services; or

''(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

''(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The terms 'Federal entity', 'information system', and 'security control' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(10) SMALL ORGANIZATION.—The term 'small organization'—

''(A) means—

''(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

''(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

''(B) does not include—

''(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

''(ii) a Federal contractor.

"SEC. 2231. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

''(2) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetuate cyber incidents and ransomware attacks;

''(3) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(4) leverage information gathered about cybersecurity incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and incident response firms, and security researchers; and

''(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2235;

''(5) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

''(6) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the briefings required under subsection (c);

''(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

''(11) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

''(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and

''(13) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2233, or information received pursuant to a request for information or subpoena under section 2234, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

''(b) INTERAGENCY SHARING.—The National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

''(1) may establish a specific time requirement for sharing information under subsection (a)(13); and

''(2) shall determine the appropriate Federal agencies under subsection (a)(13).

''(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

''(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

''(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

''(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

''(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

''(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

''(4) be unclassified, but may include a classified annex.

''SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

''(a) IN GENERAL.—

''(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

''(2) RANSOM PAYMENT REPORTS.—A covered entity, except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

''(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

''(4) PRESERVATION OF INFORMATION.—Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(5) EXCEPTIONS.—

''(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

''(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to an entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

''(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

''(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

''(b) RULEMAKING.—

''(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

''(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

''(3) SUBSEQUENT RULEMAKINGS.—

''(A) IN GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

''(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

''(1) A clear description of the types of entities that constitute covered entities, based on—

''(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

''(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

''(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

''(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

''(A) at a minimum, require the occurrence of—

''(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

''(ii) a disruption of business or industrial operations due to a cyber incident; or

''(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

''(B) consider—

''(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

''(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

''(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

''(C) exclude—

''(i) any event where the cyber incident is perpetuated by good faith security research or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and

''(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

''(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

''(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

''(A) A description of the covered cyber incident, including—

''(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

''(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

''(iii) the estimated date range of such incident; and

''(iv) the impact to the operations of the covered entity.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

''(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

''(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

''(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

''(F) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.

''(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

''(A) A description of the ransomware attack, including the estimated date range of the attack.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

''(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

''(D) The name and other information that clearly identifies the entity that made the ransom payment.

''(E) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

''(F) The date of the ransom payment.

''(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

''(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

''(I) The amount of the ransom payment.

''(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

''(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

''(A) be established by the Director in consultation with the Council;

''(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

''(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

''(8) Procedures for—

''(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

''(B) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

''(C) implementing the exceptions provided in subsection (a)(5); and

''(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

''(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

''(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under subsection (a).

''(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

''(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

''(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding reporting ransom payments under this section.

''(e) OUTREACH TO COVERED ENTITIES.—

''(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

''(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

''(A) An overview of the final rule issued pursuant to subsection (b).

''(B) An overview of mechanisms to submit to the Center covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

''(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

''(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

''(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

''(F) An overview of the privacy and civil liberties requirements in this subtitle.

''(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

''(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

''(B) information sharing and analysis organizations;

''(C) trade associations;

''(D) information sharing and analysis centers;

''(E) sector coordinating councils; and

''(F) any other entity as determined appropriate by the Director.

''(f) ORGANIZATION OF REPORTS.—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), the Director may request information within the scope of the final rule issued under subsection (b) by the alteration of existing questions or response fields and the reorganization and reformatting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.

''SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

''(a) IN GENERAL.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

''(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

''(c) APPLICATION OF PROTECTIONS.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

''SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

''(a) PURPOSE.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

''(b) INITIAL REQUEST FOR INFORMATION.—

''(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(a), that an entity has experienced a covered cyber incident or made a ransom payment but failed to

report such incident or payment to the Center within 72 hours in accordance with section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

''(2) TREATMENT.—Information provided to the Center in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

''(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

''(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

''(2) CIVIL ACTION.—

''(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

''(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

''(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

''(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

''(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity that is a Federal contractor fails to comply with a subpoena issued under this subsection—

''(A) the Director may refer the matter to the Administrator of General Services; and

''(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

''(5) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

''(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

''(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency determines, based on information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may use that information for a regulatory enforcement action or criminal prosecution.

''(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

''(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

''(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

''(1) the size and complexity of the entity;

''(2) the complexity in determining if a covered cyber incident has occurred; and

''(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

''(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

''(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b);

''(2) issued a subpoena pursuant to subsection (c); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) DISCLOSURE, RETENTION, AND USE.—

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Center or Agency pursuant to section 2232 or 2233 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

''(A) a cybersecurity purpose;

''(B) the purpose of identifying—

''(i) a cyber threat, including the source of the cyber threat; or

''(ii) a security vulnerability;

''(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

''(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

''(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2232 or 2233 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

''(2) AGENCY ACTIONS AFTER RECEIPT.—

''(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the center shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

''(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

''(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Center or the Agency pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

''(A) personal information of a specific individual; or

''(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(4) DIGITAL SECURITY.—The Center and the Agency shall ensure that reports submitted to the Center or the Agency pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

''(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment.

''(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

''(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

''(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

''(e) LIABILITY PROTECTIONS.—

''(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rule promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

''(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Center or the Agency.

''(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

''(f) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

''(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.

''(h) STORED COMMUNICATIONS ACT.—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the items relating to subtitle B of title XXII the following:

''Subtitle C—Cyber Incident Reporting

''Sec. 2230. Definitions.
''Sec. 2231. Cyber Incident Review.
''Sec. 2232. Required reporting of certain cyber incidents.
''Sec. 2233. Voluntary reporting of other cyber incidents.
''Sec. 2234. Noncompliance with required reporting.
''Sec. 2235. Information shared with or provided to the Federal Government.''.

SEC. 5104. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Director as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 5103 of this title.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this title or the amendments made by this title.

(4) FOIA EXEMPTION.—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ''Freedom of Information Act'').

(b) CREATION OF COUNCIL.—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is amended—

(1) in paragraph (1)—

(A) in subparagraph (G), by striking ''and'' at the end;

(B) by redesignating subparagraph (H) as subparagraph (I); and

(C) by inserting after subparagraph (G) the following:

''(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget, the Attorney General, and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and''; and

(2) by adding at the end the following:

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any Federal entity.''.

(c) HARMONIZING REPORTING REQUIREMENTS.—The National Cyber Director shall, in consultation with the Director, the Attorney General, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director, the Attorney General, and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 5105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).

(c) ENTITY NOTIFICATION.—

(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.

SEC. 5106. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) JOINT RANSOMWARE TASK FORCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in consultation with the Attorney General and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) CLARIFYING PRIVATE SECTOR LAWFUL DEFENSIVE MEASURES.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 5107. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103(b) of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 5103(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 5105, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 5105(c) in mitigating security vulnerabilities and the threat of ransomware.

(2) Identification of the most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the National Cyber Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) GAO REPORTS.—

(1) IMPLEMENTATION OF THIS TITLE.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this title and the amendments made by this title.

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (2) and (5) of section 2232(a) of the Homeland Security Act of 2002, as added by section 5103 of this title, which shall include—

(A) to the extent practicable, an evaluation of the quantity of incidents not reported to the Federal Government;

(B) an evaluation of the impact on impacted entities, homeland security, and the national economy of the ransomware criminal ecosystem of incidents and ransom payments, including a discussion on the scope of impact of incidents that were not reported to the Federal Government;

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this title, including an analysis of entities that meet the definition of a small organization and would be exempt from ransom payment reporting but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2234 of the Homeland Security Act of 2002, as added by section 5103 of this title.

TITLE LII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 5201. SHORT TITLE.

This title may be cited as the ''CISA Technical Corrections and Improvements Act of 2021''.

SEC. 5202. REDESIGNATIONS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217; and

(5) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (11), by striking ''and'' at the end;

(2) in the first paragraph (12)—

(A) by striking ''section 2215'' and inserting ''section 2217''; and

(B) by striking ''and'' at the end; and

(3) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) ADDITIONAL TECHNICAL AMENDMENT.—

(1) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

SEC. 5203. CONSOLIDATION OF DEFINITIONS.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitle A heading the following:

''SEC. 2200. DEFINITIONS.

''Except as otherwise specifically provided, in this title:

''(1) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(2) AGENCY INFORMATION.—The term 'agency information' means information collected or maintained by or on behalf of an agency.

''(3) AGENCY INFORMATION SYSTEM.—The term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency.

''(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(B) the Committee on Homeland Security of the House of Representatives.

''(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(6) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

''(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

''(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

''(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

''(7) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' means information that is necessary to describe or identify—

''(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

''(B) a method of defeating a security control or exploitation of a security vulnerability;

''(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

''(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

''(E) malicious cyber command and control;

''(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

''(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

''(H) any combination thereof.

''(8) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

''(9) CYBERSECURITY RISK.—The term 'cybersecurity risk'—

''(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

''(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

''(10) CYBERSECURITY THREAT.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'cybersecurity threat' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

''(B) EXCLUSION.—The term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

''(11) DEFENSIVE MEASURE.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

''(B) EXCLUSION.—The term 'defensive measure' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

''(i) the entity operating the measure; or

''(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

''(12) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

''(13) INCIDENT.—The term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

''(14) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

''(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

''(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

''(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

''(15) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(16) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(17) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

''(18) MONITOR.—The term 'monitor' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

''(19) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

''(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

''(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

''(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

''(D) facilitating information sharing and operational coordination with threat response; and

''(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

''(20) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(21) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(22) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means a cyber incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

''(B) does not include any such event where the demand for payment is made by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of the information

system for third parties to identify vulnerabilities in the information system.

''(23) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

''(24) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

''(25) SECURITY VULNERABILITY.—The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

''(26) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

''(27) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize the confidentiality, integrity, or availability of the information technology system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

''(28) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

''(29) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

''SEC. 2201. DEFINITION.

''In this subtitle, the term 'Cybersecurity Advisory Committee' means the advisory committee established under section 2219(a).'';

(2) in section 2202—

(A) in subsection (a)(1), by striking ''(in this subtitle referred to as the Agency)'';

(B) in subsection (f)—

(i) in paragraph (1), by inserting ''Executive'' before ''Assistant Director''; and

(ii) in paragraph (2), by inserting ''Executive'' before ''Assistant Director'';

(3) in section 2203(a)(2), by striking ''as the 'Assistant Director' '' and inserting ''as the 'Executive Assistant Director' '';

(4) in section 2204(a)(2), by striking ''as the 'Assistant Director' '' and inserting ''as the 'Executive Assistant Director' '';

(5) in section 2209—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)—

(i) in subparagraph (A)(iii), as so redesignated, by striking '', as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))''; and

(ii) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(ii) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(E) in subsection (j), as so redesignated, by striking ''subsection (c)(8)'' and inserting ''subsection (b)(8)''; and

(F) in subsection (n), as so redesignated—

(i) in paragraph (2)(A), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)''; and

(ii) in paragraph (3)(B)(i), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)'';

(6) in section 2210—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(C) in subsection (b), as so redesignated—

(i) by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations''; and

(ii) by striking ''(as defined in section 2209)''; and

(D) in subsection (c), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (b)'';

(7) in section 2211, by striking subsection (h);

(8) in section 2212, by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations'';

(9) in section 2213—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (f) as subsections (a) through (e); respectively;

(C) in subsection (b), as so redesignated, by striking ''subsection (b)'' each place it appears and inserting ''subsection (a)'';

(D) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking ''subsection (b)'' and inserting ''subsection (a)''; and

(E) in subsection (d), as so redesignated—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(II) in subparagraph (A), by striking ''subsection (c)(1)'' and inserting ''subsection (b)(1)''; and

(III) in subparagraph (B), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)''; and

(ii) in paragraph (2), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(10) in section 2216, as so redesignated—

(A) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(B) by striking subsection (f) and inserting the following:

''(f) CYBER DEFENSE OPERATION DEFINED.—In this section, the term 'cyber defense operation' means the use of a defensive measure.'';

(11) in section 2218(c)(4)(A), as so redesignated, by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(12) in section 2222—

(A) by striking paragraphs (3), (5), and (8);

(B) by redesignating paragraph (4) as paragraph (3); and

(C) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXII the following:

''Sec. 2200. Definitions.'';

(2) by striking the item relating to section 2201 and inserting the following:

''Sec. 2201. Definition.''; and

(3) by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.''.

(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

''(4) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(6) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(7) DEFENSIVE MEASURE.—The term 'defensive measure' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) by striking paragraph (13) and inserting the following:

''(13) MONITOR.— The term 'monitor' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''; and

(3) by striking paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''.

SEC. 5204. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking ''section 2210'' and inserting ''section 2200''; and

(B) in paragraph (4), by striking ''section 2209'' and inserting ''section 2200'';

(2) in section 223(b) (6 U.S.C. 151 note), by striking ''section 2213(b)(1)'' each place it appears and inserting ''section 2213(a)(1)'';

(3) in section 226 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

(iii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iv) in paragraph (5), by striking ''section 2213(b)'' and inserting ''section 2213(a)''; and

(B) in subsection (c)(1)(A)(vi), by striking ''section 2213(c)(5)'' and inserting ''section 2213(b)(5)''; and

(4) in section 227(b) (6 U.S.C. 1525(b)), by striking ''section 2213(d)(2)'' and inserting ''section 2213(c)(2)''.

(b) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking ''section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))'' and inserting ''section 2210(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

(c) WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))'' and inserting ''section 2200 of the Homeland Security Act of 2002''; and

(B) by amending paragraph (7) to read as follows:

''(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) in subsection (c)(3)(B), by striking ''section 2201(5)'' and inserting ''section 2200''; and

(3) in subsection (d)—

(A) by striking ''section 2215'' and inserting ''section 2218''; and

(B) by striking '', as added by this section''.

(d) NATIONAL SECURITY ACT OF 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking ''section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147)'' and inserting ''section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(e) IOT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking ''section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(l))''.

(f) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of the Small Business Act (15 U.S.C. 648(a)(8)(B)) is amended by striking ''section 2209(a)'' and inserting ''section 2200''.

(g) TITLE 46.—Section 70101(2) of title 46, United States Code, is amended by striking ''section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)'' and inserting ''section 2200 of the Homeland Security Act of 2002''.

SA 4814. Ms. MURKOWSKI submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. EXTENSION OF AVAILABILITY OF CORONAVIRUS RELIEF FUND PAYMENTS TO TRIBAL GOVERNMENTS.

Section 601(d)(3) of the Social Security Act (42 U.S.C. 801(d)(3)) is amended by inserting ''(or, in the case of costs incurred by a Tribal government, during the period that begins on March 1, 2020, and ends on December 31, 2022)'' before the period.

SA 4815. Mr. SANDERS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1064. REQUIREMENT OF DENTAL CLINIC OF DEPARTMENT OF VETERANS AFFAIRS IN EACH STATE.

The Secretary of Veterans Affairs shall ensure that each State has a dental clinic of the Department of Veterans Affairs to service the needs of the veterans within that State by not later than September 30, 2024.

SA 4816. Mr. COONS submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

Subtitle ____—Sudan Democracy Act

SEC. ____1. SHORT TITLE.

This subtitle may be cited as the ''Sudan Democracy Act''.

SEC. ____2. DEFINITIONS.

In this subtitle:

(1) ADMITTED; ALIEN.—The terms ''admitted'' and ''alien'' have the meanings given such terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1001).

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations of the Senate;

(B) the Committee on Appropriations of the Senate;

(C) the Committee on Foreign Affairs of the House of Representatives; and

(D) the Committee on Appropriations of the House of Representatives.

(3) FOREIGN PERSON.—The term ''foreign person'' means a person that is not a United States person.

(4) GROSS VIOLATIONS OF INTERNATIONALLY RECOGNIZED HUMAN RIGHTS.—The term ''gross violations of internationally recognized human rights'' has the meaning given such term in section 502B(d)(1) of the Foreign Assistance Act of 1961 (22 U.S.C. 2304(d)(1)).

(5) INTERNATIONAL FINANCIAL INSTITUTIONS.—The term ''international financial institutions'' means—

(A) the International Monetary Fund;

(B) the International Bank for Reconstruction and Development;

(C) the International Development Association;

(D) the International Finance Corporation;

(E) the Inter-American Development Bank;

(F) the Asian Development Bank;

(G) the Inter-American Investment Corporation;

(H) the African Development Bank;

(I) the African Development Fund;

(J) the European Bank for Reconstruction and Development; and

(K) the Multilateral Investment Guaranty Agency.

(6) KNOWINGLY.—The term ''knowingly'' means, with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(7) SECURITY AND INTELLIGENCE SERVICES.—The term ''security and intelligence services'' means—

(A) the Sudan Armed Forces;

(B) the Rapid Support Forces;

(C) the Popular Defense Forces;

(D) other Sudanese paramilitary units;

(E) Sudanese police forces; and

(F) the General Intelligence Service (previously known as the National Intelligence and Security Services).

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen, an alien lawfully admitted for permanent residence to the United States, or any other individual subject to the jurisdiction of the United States; or

(B) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such entity.

SEC. ____3. FINDINGS; STATEMENT OF POLICY.

(a) FINDINGS.—Congress makes the following findings:

(1) On November 17, 1958, Lieutenant General Ibrahim Abboud of Sudan led the country's first coup after independence, and the first successful coup in post-independence Africa.

(2) There have been more than 200 coup attempts across Africa since the 1958 coup in Sudan, including successful coups in Sudan in 1969, 1985, 1989, and 2019.

(3) On April 11, 2019, President Omar al Bashir of Sudan, who came to power in a military coup in 1989, was overthrown after months of popular protests by his own security chiefs, who established a Transitional Military Council, led by Lieutenant General Abdel Fattah al-Burhan, that ignored calls from the Sudanese people to transfer power to civilians.

(4) On August 17, 2019—

(A) the Transitional Military Council, under domestic and international pressure, signed a power-sharing agreement with the Forces for Freedom and Change, a broad coalition of political parties and civic groups representing the protest movement that had pushed for the end of the Bashir regime and a transition to civilian rule; and

(B) a transitional government was formed that allowed the junta leaders to remain in government in a partnership with new civilian authorities nominated by the Forces for Freedom and Change, including Prime Minister Abdallah Hamdok, for a transitional period to democracy.

(5) On October 25, 2021, Lieutenant General Burhan, with the support of Lieutenant Mohamed Hamdan Dagalo (also known as ''Hemedti'')—

(A) seized control of the Government of Sudan;

(B) deployed the military to the streets of Khartoum and Omdurman;

(C) shut down the internet in Sudan; and

(D) detained Prime Minister Hamdok and other civilian officials.

(6) The African Union Peace and Security Council has condemned the military takeover, rejected the unconstitutional change of

government, and on October 27, 2021, suspended Sudan from the Council until the civilian-led transitional government is restored.

(7) The Troika (the United States, United Kingdom, Norway), the European Union, and Switzerland ''continue to recognize the Prime Minister and his cabinet as the constitutional leaders of the transitional government''.

(8) The Sudanese people have condemned the military takeover and launched a campaign of peaceful civil disobedience, continuing the protests for democracy that began in late 2018 and reflecting a historic tradition of non-violence protests led by previous generations in Sudan against military regimes in 1964 and 1985.

(9) In response to public calls for civilian rule since October 25, 2021, Sudanese security forces have arbitrarily detained civilians and used excessive and lethal force against peaceful protesters that has resulted in civilian deaths across the country.

(10) The October 25, 2021 military takeover represents a threat to—

(A) Sudan's economic recovery and stability;

(B) the bilateral relationship between Sudan and the United States; and

(C) regional peace and security.

(b) STATEMENT OF POLICY.—It is the policy of the United States—

(1) to support the democratic aspirations of the people of Sudan and a political transition process that results in a civilian government that is democratic, accountable, respects the human rights of its citizens, and is at peace with itself and with its neighbors;

(2) to encourage the reform of the security sector of Sudan to one that is protects citizens under a democracy and respects civilian authority; and

(3) to deter military coups and efforts by external parties to support them.

SEC. ___4. IMPOSITION OF SANCTIONS.

(a) IN GENERAL.—The President shall impose the sanctions described in subsection (b) with respect to any person or entity that the President determines, on or after the date of enactment of this Act—

(1) is responsible for, complicit in, or directly or indirectly engaged or attempted to engage in—

(A) actions that undermine the transition to democracy in Sudan, or, after elections, undermine democratic processes or institutions;

(B) actions that threaten the peace, security, or stability of Sudan;

(C) actions that prohibit, limit, or penalize the exercise of freedom of expression or assembly by people in Sudan, or limit access to print, online, or broadcast media in Sudan;

(D) the arbitrary detention or torture of any person in Sudan or other gross violations of internationally recognized human rights in Sudan;

(E) significant efforts to impede investigations or prosecutions of alleged serious human rights abuses in Sudan;

(F) actions that result in the misappropriation of significant state assets of Sudan or manipulation of the currency, or that hinder government oversight of parastatal budgets and revenues;

(G) actions that violate medical neutrality, including blocking access to care and targeting first responders, medical personnel, or medical institutions; or

(H) disrupting access to communication technologies and information on the internet;

(2) is an entity owned or controlled by any person or entity described in paragraph (1);

(3) forms an entity for the purpose of evading sanctions that would otherwise be imposed pursuant to subsection (b);

(4) is acting for, or on behalf of, a person or entity referred to in paragraph (1), (2), or (3);

(5) is an entity that is owned or controlled (directly or indirectly) by security and intelligence services, from which 1 or more persons or entities described in paragraph (1) derive significant revenue or financial benefit; or

(6) has knowingly—

(A) provided significant financial, material, or technological support—

(i) to a foreign person or entity described in paragraph (1) in furtherance of any of the acts described in subparagraph (A) or (B) of such paragraph; or

(ii) to any entity owned or controlled by such person or entity or an immediate family member of such person; or

(B) received significant financial, material, or technological support from a foreign person or entity described in paragraph (1) or an entity owned or controlled by such person or entity or an immediate family member of such person.

(b) SANCTIONS; EXCEPTIONS.—

(1) SANCTIONS.—

(A) ASSET BLOCKING.—Notwithstanding section 202 of the International Emergency Economic Powers Act (50 U.S.C. 1701), the exercise of all powers granted to the President by such Act to the extent necessary to block and prohibit all transactions in all property and interests in property of a foreign person the President determines meets 1 or more of the criteria described in subsection (a) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(B) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(i) VISAS, ADMISSION, OR PAROLE.—An alien who the Secretary of State or the Secretary of Homeland Security (or a designee of one of such Secretaries) knows, or has reason to believe, meets any of the criteria described in subsection (a)—

(I) is inadmissible to the United States;

(II) is ineligible to receive a visa or other documentation to enter the United States; and

(III) is otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(ii) CURRENT VISAS REVOKED.—

(I) IN GENERAL.—The issuing consular officer, the Secretary of State, or a designee of the Secretary of State, in accordance with section 221(i) of the Immigration and Nationality Act (8 U.S.C. 1201(i)), shall revoke any visa or other entry documentation issued to an alien described in clause (i) regardless of when the visa or other entry documentation was issued.

(II) EFFECT OF REVOCATION.—A revocation under subclause (I) shall take effect immediately and shall automatically cancel any other valid visa or entry documentation that is in the alien's possession.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under paragraph (1)(B) shall not apply with respect to an alien if admitting or paroling the alien into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.

(3) PENALTIES.—Any person that violates, attempts to violate, conspires to violate, or causes a violation of this section or any regulation, license, or order issued to carry out subsection (b) shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of such section.

(4) IMPLEMENTATION.—The President—

(A) may exercise all authorities provided under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section; and

(B) shall issue such regulations, licenses, and orders as may be necessary to carry out this section.

(5) EXCEPTION TO COMPLY WITH NATIONAL SECURITY.—Activities subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) and any authorized intelligence or law enforcement activities of the United States shall be exempt from sanctions under this section.

(c) WAIVER.—The President may annually waive the application of sanctions imposed on a foreign person pursuant to subsection (a) if the President—

(1) determines that such waiver with respect to such foreign person is in the national interest of the United States; and

(2) not later than the date on which such waiver will take effect, submits notice of, and justification for, such waiver to—

(A) the appropriate congressional committees;

(B) the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(C) the Committee on Financial Services of the House of Representatives.

(d) SUNSET.—The requirement to impose sanctions under this section shall cease to be effective on December 31, 2026.

SA 4817. Ms. SINEMA submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. LAND TAKEN INTO TRUST FOR BENEFIT OF THE GILA RIVER INDIAN COMMUNITY.

(a) DEFINITIONS.—In this section:

(1) BLACKWATER TRADING POST LAND.—The term ''Blackwater Trading Post Land'' means the approximately 55.3 acres of land as depicted on the map that—

(A) is located in Pinal County, Arizona, and bordered by Community land to the east, west, and north and State Highway 87 to the south; and

(B) is owned by the Community.

(2) COMMUNITY.—The term ''Community'' means the Gila River Indian Community of the Reservation.

(3) MAP.—The term ''map'' means the map entitled ''Results of Survey, Ellis Property, A Portion of the West ½ of Section 12, Township 5 South, Range 7 East, Gila and Salt River Meridian, Pinal County, Arizona'' and dated October 15, 2012.

(4) RESERVATION.—The term ''Reservation'' means the land located within the exterior boundaries of the reservation created under sections 3 and 4 of the Act of February 28, 1859 (11 Stat. 401, chapter LXVI), and Executive orders of August 31, 1876, June 14, 1879,

May 5, 1882, November 15, 1883, July 31, 1911, June 2, 1913, August 27, 1914, and July 19, 1915, and any other lands placed in trust for the benefit of the Community.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of the Interior.

(b) LAND TAKEN INTO TRUST FOR BENEFIT OF THE GILA RIVER INDIAN COMMUNITY.—

(1) IN GENERAL.—The Secretary shall take the Blackwater Trading Post Land into trust for the benefit of the Community, after the Community—

(A) conveys to the Secretary all right, title, and interest of the Community in and to the Blackwater Trading Post Land;

(B) submits to the Secretary a request to take the Blackwater Trading Post Land into trust for the benefit of the Community;

(C) conducts a survey (to the satisfaction of the Secretary) to determine the exact acreage and legal description of the Blackwater Trading Post Land, if the Secretary determines a survey is necessary; and

(D) pays all costs of any survey conducted under subparagraph (C).

(2) AVAILABILITY OF MAP.—Not later than 180 days after the Blackwater Trading Post Land is taken into trust under paragraph (1), the map shall be on file and available for public inspection in the appropriate offices of the Secretary.

(3) LANDS TAKEN INTO TRUST PART OF RESERVATION.—After the date on which the Blackwater Trading Post Land is taken into trust under paragraph (1), the land shall be treated as part of the Reservation.

(4) GAMING.—Class II and class III gaming under the Indian Gaming Regulatory Act (25 U.S.C. 2701 et seq.) shall not be allowed at any time on the land taken into trust under paragraph (1).

(5) DESCRIPTION.—Not later than 180 days after the date of enactment of this Act, the Secretary shall cause the full metes-and-bounds description of the Blackwater Trading Post Land to be published in the Federal Register. The description shall, on publication, constitute the official description of the Blackwater Trading Post Land.

SA 4818. Mr. BENNET submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle H—Long Wars Commission Act of 2021

SEC. 1291. SHORT TITLE.

This subtitle may be cited as the ''Long Wars Commission Act of 2021''.

SEC. 1292. ESTABLISHMENT OF COMMISSION.

(a) ESTABLISHMENT.—There is established the Long Wars Commission (in this subtitle referred to as the ''Commission'').

(b) MEMBERSHIP.—

(1) IN GENERAL.—The Commission shall be composed of 12 members appointed as follows:

(A) One member appointed by the chair of the Committee on Armed Services of the Senate.

(B) One member appointed by the ranking minority member of the Committee on Armed Services of the Senate.

(C) One member appointed by the chair of the Committee on Foreign Relations of the Senate.

(D) One member appointed by the ranking minority member of the Committee on Foreign Relations of the Senate.

(E) One member appointed by the chair of the Committee on Armed Services of the House of Representatives.

(F) One member appointed by the ranking minority member of the Committee on Armed Services of the House of Representatives.

(G) One member appointed by the chair of the Committee on Foreign Affairs of the House of Representatives.

(H) One member appointed by the ranking minority member of the Committee on Foreign Affairs of the House of Representatives.

(I) One member appointed by the chair of the Senate Select Committee on Intelligence.

(J) One member appointed by the ranking minority member of the Senate Select Committee on Intelligence.

(K) One member appointed by the chair of the House Permanent Select Committee on Intelligence.

(L) One member appointed by the ranking minority member of the House Permanent Select Committee on Intelligence.

(2) DATE.—The appointments of the members of the Commission shall be made not later than 90 days after the date of enactment of this Act.

(3) PROHIBITIONS.—A member of the Commission appointed under subparagraph (A) may not—

(A) be a current member of Congress, or a former member of Congress, who served in Congress after January 3, 2001;

(B) have served in military or civilian positions having significant operational or strategic decisionmaking responsibilities for conducting United States Government actions in Afghanistan during the applicable period; or

(C) have been a party to any United States or coalition defense contract during the applicable period.

(c) PERIOD OF APPOINTMENT; VACANCIES.—Members shall be appointed for the life of the Commission. Any vacancy in the Commission shall be filled in the same manner as the original appointment.

(d) MEETINGS.—

(1) INITIAL MEETING.—Not later than 30 days after the date on which all members of the Commission have been appointed, the Commission shall hold the first meeting of the Commission.

(2) FREQUENCY.—The Commission shall meet at the call of the co-chairs.

(3) QUORUM.—A majority of the members of the Commission shall constitute a quorum, but a lesser number of members may hold hearings.

(e) CO-CHAIRS.—

(1) DESIGNATION BY COMMITTEE CHAIRS.—The chair of the Committee on Armed Services of the Senate, the chair of the Committee on Foreign Relations of the Senate, the chair of the Committee on Armed Services of the House of Representatives, the chair of the Committee on Foreign Affairs of the House of Representatives, the chair of the Senate Select Committee on Intelligence, and the chair of the House Permanent Select Committee on Intelligence shall jointly designate one member of the Commission to serve as co-chair of the Commission.

(2) DESIGNATION BY RANKING MINORITY MEMBERS.—The ranking minority member of the Committee on Armed Services of the Senate, the ranking minority member of the Committee on Foreign Relations of the Senate, the ranking minority member of the Committee Armed Services of the House of Representatives, and the ranking minority member of the Committee on Foreign Affairs of the House of Representatives, the ranking minority member of the Senate Select Committee on Intelligence, and the ranking minority member of the House Permanent Select Committee on Intelligence shall jointly designate one member of the Commission to serve as co-chair of the Commission.

SEC. 1293. DUTIES.

(a) REVIEW.—The Commission shall review United States involvement in the conflicts in Afghanistan and Iraq beginning during the period prior to the September 11, 2001, attacks and ending on September 1, 2022, including military engagement, diplomatic engagement, training and advising of local forces, reconstruction efforts, foreign assistance, congressional oversight, and withdrawal in such conflicts.

(b) ASSESSMENT AND RECOMMENDATIONS.—The Commission shall—

(1) conduct a comprehensive assessment of United States involvement in the conflicts in Afghanistan and Iraq, including—

(A) United States military, diplomatic, and political objectives in the conflicts, and the extent to which those objectives were achievable;

(B) an evaluation of the interagency decisionmaking processes during the campaigns;

(C) an evaluation of the United States military's conduct during the campaigns and the extent to which its operational approach compromised campaign progress;

(D) any regional and geopolitical threats to the United States resulting from the conflicts;

(E) the extent to which initial United States national objectives for the conflicts were met;

(F) long-term impact on United States relations with allied nations who participated in the Iraq and Afghanistan conflicts;

(G) the effectiveness of counterterrorism, counterinsurgency, and security force assistance strategies employed by the United States military;

(H) the effect of United States involvement in the conflicts on the readiness of the United States Armed Forces;

(I) the effect of United States involvement in the conflicts on civil-military relations in the United States;

(J) the implications of the use of funds for overseas contingency operations as a mechanism for funding United States involvement in the conflicts; and

(K) any other matters in connection with United States involvement in the conflicts the Commission considers appropriate;

(2) identify circumstances in which a conflict presents a significant likelihood of developing into an irregular or civil war; and

(3) develop recommendations based on the assessment, as well as any other information the Commission considers appropriate, for relevant questions to be asked during future deliberations by Congress of an authorization for use of military force in conflicts that have the potential to develop into an irregular or civil war.

(c) REPORT.—

(1) FINAL REPORT.—Not later than 2 years after the date of the enactment of this Act, the Commission shall submit to the President, the Secretary of Defense, the Committee on Armed Services of the Senate, the Committee on Armed Services of the House of Representatives, the Committee on Foreign Relations of the Senate, the Committee on Foreign Affairs of the House of Representatives, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence a report on the findings, conclusions, and recommendations of the Commission under this section. The report shall do each of the following:

(A) Provide an assessment of the current security, political, humanitarian, and economic situation in Afghanistan and Iraq.

(B) Provide lessons learned from United States involvement in, and withdrawal from, the conflicts in Afghanistan and Iraq.

(C) Provide recommendations on questions to be asked during future deliberations by Congress of an authorization for use of military force in a conflict that has the potential to develop into an irregular war.

(D) Address any other matters with respect to United States involvement in the conflicts in Afghanistan and Iraq that the Commission considers appropriate.

(E) Provide recommendations about United States instruments of power, including the use of military force and nation-building, in future foreign policy engagements.

(F) Provide recommendations about the need to foster any new alliances necessary to future foreign policy engagements.

(2) INTERIM BRIEFING.—Not later than one year after the date of the enactment of this Act, the Commission shall provide to the committees of Congress and the officials referred to in paragraph (1) a briefing on the status of its review and assessment under subsection (b), together with a discussion of any interim recommendations developed by the Commission as of the date of the briefing.

(3) FORM OF REPORT.—The report submitted to Congress under paragraph (1) shall be submitted in unclassified form. The report shall also include a classified annex.

SEC. 1294. POWERS OF COMMISSION.

(a) HEARINGS.—The Commission may hold such hearings, sit and act at such times and places, take such testimony, and receive such evidence as the Commission considers advisable to carry out this subtitle.

(b) ASSISTANCE FROM FEDERAL AGENCIES.—

(1) INFORMATION.—

(A) IN GENERAL.—The Commission may secure directly from a Federal department or agency such information as the Commission considers necessary to carry out this subtitle.

(B) FURNISHING INFORMATION.—On request of the co-chairs of the Commission, the head of the department or agency shall expeditiously furnish the information to the Commission.

(2) GENERAL SERVICES.—Upon the request of the Commission, the Administrator of General Services shall provide to the Commission, on a reimbursable basis, the administrative support services and office space necessary for the Commission to carry out its purposes and functions under this subtitle.

(c) POSTAL SERVICES.—The Commission may use the United States mails in the same manner and under the same conditions as other departments and agencies of the Federal Government.

(d) GIFTS.—The Commission may accept, use, and dispose of gifts or donations of services or property.

(e) COOPERATION FROM UNITED STATES GOVERNMENT.—

(1) IN GENERAL.—The Commission shall receive the full and timely cooperation of the Secretary of Defense, the Secretary of State, and the Director of National Intelligence in providing the Commission with analyses, briefings, and other information necessary for the discharge of the duties of the Commission.

(2) LIAISON.—The Secretary of Defense, the Secretary of State, and the Director of National Intelligence shall each designate at least one officer or employee of their respective organizations to serve as a liaison officer to the Commission.

SEC. 1295. COMMISSION PERSONNEL MATTERS.

(a) COMPENSATION OF MEMBERS.—A member of the Commission who is not an officer or employee of the Federal Government shall be compensated at a rate equal to the daily equivalent of the annual rate of basic pay prescribed for level IV of the Executive Schedule under section 5315 of title 5, United States Code, for each day (including travel time) during which the member is engaged in the performance of the duties of the Commission.

(b) TRAVEL EXPENSES.—A member of the Commission shall be allowed travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Commission.

(c) STAFF.—

(1) IN GENERAL.—The co-chairs of the Commission, may, without regard to the civil service laws (including regulations), appoint and terminate an executive director and such other additional personnel as may be necessary to enable the Commission to perform its duties, except that the employment of an executive director shall be subject to confirmation by the Commission.

(2) QUALIFICATIONS FOR PERSONNEL.—The co-chairs of the Commission shall give preference in such appointments to individuals with significant professional experience in national security, such as a position in the Department of Defense, the Department of State, the intelligence community, the United States Agency for International Development, or an academic or scholarly institution.

(3) COMPENSATION.—The co-chairs may fix the compensation of the executive director and other personnel without regard to chapter 51 and subchapter III of chapter 53 of title 5, United States Code, relating to classification of positions and General Schedule pay rates, except that the rate of pay for the executive director and other personnel may not exceed the rate payable for level V of the Executive Schedule under section 5316 of that title.

(d) DETAIL OF GOVERNMENT EMPLOYEES.—A Federal Government employee may be detailed to the Commission without reimbursement, and such detail shall be without interruption or loss of civil service status or privilege.

(e) PROCUREMENT OF TEMPORARY AND INTERMITTENT SERVICES.—The co-chairs of the Commission, may procure temporary and intermittent services under section 3109(b) of title 5, United States Code, at rates for individuals that do not exceed the daily equivalent of the annual rate of 3 basic pay prescribed for level V of the Executive Schedule under section 5316 of that title.

SEC. 1296. TERMINATION OF COMMISSION.

The Commission shall terminate 90 days after the date on which the Commission submits the report required under section 1293(c).

SEC. 1297. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There is authorized to be appropriated to the Commission such amounts as necessary to carry out activities under this subtitle.

(b) AVAILABILITY.—Any sums appropriated under the authorization contained in this section shall remain available, without fiscal year limitation, until the date of the termination of the Commission under section 1296.

SA 4819. Mr. SULLIVAN (for himself and Mr. WHITEHOUSE) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle F of title X, add the following:

SEC. 1054. REPORT ON EFFORTS OF COMBATANT COMMANDS TO COMBAT THREATS POSED BY ILLEGAL, UNREPORTED, AND UNREGULATED FISHING.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, in consultation with the chair and deputy chairs of the Interagency Working Group on IUU Fishing and the heads of other relevant agencies, as determined by the Secretary, shall submit to the appropriate committees of Congress a report on the maritime domain awareness efforts of the combatant commands to combat the threats posed by illegal, unreported, and unregulated fishing.

(b) ELEMENTS.—The report required by subsection (a) shall include a detailed summary of each of the following for each combatant command:

(1) Activities undertaken as of the date on which the report is submitted to combat the threats posed by illegal, unreported, and unregulated fishing in the geographic area of the combatant command, including the steps taken to build the capacity of partners to combat those threats.

(2) Coordination among the United States Armed Forces, partner countries, and public-private partnerships to combat the threats described in paragraph (1).

(3) Efforts undertaken to support unclassified data integration, analysis, and delivery with regional partners to combat the threats described in paragraph (1).

(4) Information sharing and coordination with efforts of the Interagency Working Group on IUU Fishing.

(5) Best practices and lessons learned from ongoing and previous efforts relating to the threats described in paragraph (1), including strategies for coordination and successes in public-private partnerships.

(6) Limitations related to affordability, resource constraints, or other gaps or factors that constrain the success or expansion of efforts related to the threats described in paragraph (1).

(7) Any new authorities needed to support efforts to combat the threats described in paragraph (1).

(c) FORM.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

(d) DEFINITIONS.—In this section:

(1) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Committee on Foreign Relations, and the Committee on Appropriations of the Senate; and

(B) the Committee on Armed Services, the Committee on Natural Resources, the Committee on Transportation and Infrastructure, the Committee on Foreign Affairs, and the Committee on Appropriations of the House of Representatives.

(2) INTERAGENCY WORKING GROUP ON IUU FISHING.—The term ''Interagency Working Group on IUU Fishing'' means the working group established by section 3551 of the Maritime Security and Fisheries Enforcement Act (16 U.S.C. 8031).

SA 4820. Mr. COTTON (for himself, Mr. MANCHIN, Mr. TUBERVILLE, and Mr. KELLY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XIV, add the following:

Subtitle D—Extraction and Processing of Critical Minerals in the United States

SEC. 1431. SHORT TITLE.

This subtitle may be cited as the ''Restoring Essential Energy and Security Holdings Onshore for Rare Earths and Critical Minerals Act of 2021'' or the ''REEShore Critical Minerals Act of 2021''.

SEC. 1432. DEFINITIONS.

In this subtitle:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services, the Committee on Foreign Relations, the Committee on Energy and Natural Resources, the Committee on Commerce, Science, and Transportation, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Armed Services, the Committee on Foreign Affairs, the Committee on Natural Resources, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives.

(2) CRITICAL MINERAL.—The term ''critical mineral'' has the meaning given that term in section 7002(a) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(a)).

(3) DEFENSE MINERAL PRODUCT.—The term ''defense mineral product'' means any product—

(A) formed or comprised of, or manufactured from, one or more critical minerals; and

(B) used in critical military defense technologies or other related applications of the Department of Defense.

(4) PROCESSED OR REFINED.—The term ''processed or refined'' means any process by which a defense mineral is extracted, separated, or otherwise manipulated to render the mineral usable for manufacturing a defense mineral product.

SEC. 1433. REPORT ON STRATEGIC CRITICAL MINERAL AND DEFENSE MINERAL PRODUCTS RESERVE.

(a) FINDINGS.—Congress finds that the storage of substantial quantities of critical minerals and defense mineral products will—

(1) diminish the vulnerability of the United States to the effects of a severe supply chain interruption; and

(2) provide limited protection from the short-term consequences of an interruption in supplies of defense mineral products.

(b) SENSE OF CONGRESS.—It is the sense of Congress that, in procuring critical minerals and defense mineral products, the Secretary of Defense should prioritize procurement of critical minerals and defense mineral products from sources in the United States, including that are mined, produced, separated, and manufactured within the United States.

(c) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of the Interior, acting through the United States Geologic Survey, and the Secretary of Defense, in consultation with the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, the Secretary of Commerce, and the Director of National Intelligence, shall jointly submit to the appropriate congressional committees a report—

(A) describing the existing authorities and funding levels of the Federal Government to stockpile critical minerals and defense mineral products;

(B) assessing whether those authorities and funding levels are sufficient to meet the requirements of the United States; and

(C) including recommendations to diminish the vulnerability of the United States to disruptions in the supply chains for critical minerals and defense mineral products through changes to policy, procurement regulation, or existing law, including any additional statutory authorities that may be needed.

(2) CONSIDERATIONS.—In developing the report required by paragraph (1), the Secretary of the Interior, the Secretary of Defense, the Secretary of Commerce, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the Director of National Intelligence shall take into consideration the needs of the Armed Forces of the United States, the intelligence community (as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))), the defense industrial and technology sectors, and any places, organizations, physical infrastructure, or digital infrastructure designated as critical to the national security of the United States.

SEC. 1434. REPORT ON DISCLOSURES CONCERNING CRITICAL MINERALS BY CONTRACTORS OF DEPARTMENT OF DEFENSE.

(a) REPORT REQUIRED.—Not later than December 31, 2022, the Secretary of Defense, after consultation with the Secretary of Commerce, the Secretary of State, and the Secretary of the Interior, shall submit to the appropriate congressional committees a report that includes—

(1) a review of the existing disclosure requirements with respect to the provenance of magnets used within defense mineral products;

(2) a review of the feasibility of imposing a requirement that any contractor of the Department of Defense provide a disclosure with respect to any system with a defense mineral product that is a permanent magnet, including an identification of the country or countries in which—

(A) the critical minerals used in the magnet were mined;

(B) the critical minerals were refined into oxides;

(C) the critical minerals were made into metals and alloys; and

(D) the magnet was sintered or bonded and magnetized; and

(3) recommendations to Congress for implementing such a requirement, including methods to ensure that any tracking or provenance system is independently verifiable.

SEC. 1435. REPORT ON PROHIBITION ON ACQUISITION OF DEFENSE MATERIALS FROM NON-ALLIED FOREIGN NATIONS.

The Secretary of Defense shall study and submit to the appropriate congressional committees a report on the potential impacts of imposing a restriction that, for any contract entered into or renewed on or after December 31, 2026, for the procurement of a system the export of which is restricted or controlled under the Arms Export Control Act (22 U.S.C. 2751 et seq.), no critical minerals processed or refined in the People's Republic of China may be included in the system.

SEC. 1436. PRODUCTION IN AND USES OF CRITICAL MINERALS BY UNITED STATES ALLIES.

(a) POLICY.—It shall be the policy of the United States to encourage countries that are allies of the United States to identify alternatives, to the maximum extent practicable, to the use of critical minerals from foreign entities of concern.

(b) REPORT REQUIRED.—Not later than December 31, 2022, and annually thereafter, the Secretary of Defense, in coordination with the Secretary of State, shall submit to the appropriate congressional committees a report—

(1) describing the discussions of such Secretaries with countries that are allies of the United States concerning supply chain security for critical minerals;

(2) assessing the likelihood of those countries identifying alternatives, to the maximum extent practicable, to the use of critical minerals from foreign entities of concern or countries that such Secretaries deem to be of concern; and

(3) assessing initiatives in other countries to increase critical mineral mining and production capabilities.

(c) FOREIGN ENTITY OF CONCERN DEFINED.—In this section, the term ''foreign entity of concern'' has the meaning given that term in section 9901(6) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 4651(6)).

SA 4821. Mr. BROWN (for himself and Mr. WARNER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place in title II, insert the following:

SEC. _____. MINORITY INSTITUTE FOR DEFENSE RESEARCH.

(a) PLAN TO PROMOTE DEFENSE RESEARCH AT MINORITY INSTITUTIONS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this section, the Secretary of Defense shall submit to the congressional defense committees a plan (in this section referred to as the ''Plan'')—

(A) to promote defense research activities at minority institutions to elevate the defense research capacity of minority institutions; and

(B) for the establishment of the Minority Institute for Defense Research (in this section referred to as the ''Consortium'').

(2) ELEMENTS.—The Plan shall include the following:

(A) An assessment relating to the engineering, research, and development capability, including the workforce, administrative support, and physical research infrastructure, of minority institutions and their ability to participate in defense research and engineering activities and effectively compete for defense research contracts.

(B) An assessment of the activities and investments necessary to elevate minority institutions or a consortium of minority institutions, including historically Black colleges and universities, to the level of R1 research institutions and increase their participation

in, and ability to effectively compete for, defense research and engineering activities.

(C) Recommendations relating to actions that may be taken by the Department of Defense, Congress, and minority institutions to establish the Consortium within 3 years.

(D) The specific goals, incentives, and metrics developed by the Secretary in subsection (c) to increase and measure the capacity of minority institutions to address the research and development needs of the Department.

(3) CONSULTATION.—In developing the plan under paragraph (1), the Secretary shall consult with such other public and private sector organizations as the Secretary considers appropriate.

(4) PUBLICLY AVAILABLE.—The Secretary shall post the Plan on a publicly available website of the Department.

(5) MINORITY INSTITUTION DEFINED.—In this subsection, the term ''minority institution'' means—

(A) a part B institution (as such term is defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061)); or

(B) an accredited minority institution (as such term is defined in section 365 of the Higher Education Act of 1965 (20 U.S.C. 1067k)).

(b) ACTIVITIES TO SUPPORT RESEARCH AND ENGINEERING CAPACITY OF HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY-SERVING INSTITUTIONS OF HIGHER EDUCATION.—Subsection (c) of section 2362 of title 10, United States Code, is amended—

(1) by redesignating paragraph (4) as paragraph (5); and

(2) by inserting after paragraph (3) the following new paragraph (4):

''(4) Developing the capability, including workforce, administrative support, and research infrastructure (including physical), of covered educational institutions to more effectively compete for Federal research and engineering funding opportunities.''.

(c) INCREASING INCENTIVES FOR NATIONAL SECURITY RESEARCH AND ENGINEERING ORGANIZATIONS TO COLLABORATE WITH HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY-SERVING INSTITUTIONS OF HIGHER EDUCATION.—Subsection (d) of such section is amended—

(1) by striking ''The Secretary of Defense may develop'' and inserting ''The Secretary of Defense shall—

''(1) develop'';

(2) in paragraph (1), as designated by paragraph (1), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(2) establish goals and incentives for each federally funded research and development center, science and technology reinvention laboratory, and university-affiliated research center funded by the Department of Defense to increase and measure the capacity of covered educational institutions to address the research and development needs of the Department through partnerships and collaborations.''.

(d) INCREASING PARTNERSHIPS FOR MINORITY INSTITUTIONS WITH NATIONAL SECURITY RESEARCH AND ENGINEERING ORGANIZATIONS.—Such section is amended—

(1) by redesignating subsections (e) and (f) as (f) and (g) respectively; and

(2) by inserting after subsection (d) the following new subsection (e):

''(e) PARTNERSHIPS.—The Secretary of Defense shall—

''(1) require the core capabilities of each university-affiliated research center to include partnerships with covered educational institutions;

''(2) require in each indefinite delivery indefinite quantity established or renewed with a university-affiliated research center to establish or maintain a partnership with a specific covered educational institution or consortium of covered educational institutions for the purpose of capacity building at such covered educational institution or covered educational institutions;

''(3) require each university-affiliated research center to report annually on their subcontracts and other activities with covered educational institutions; and

''(4) post on a publicly available website of the Department a list of covered educational institutions and their defense research capabilities.''.

(e) DEFINITION OF UNIVERSITY-AFFILIATED RESEARCH CENTERS.—Subsection (g) of such section, as redesignated by subsection (d)(1), is amended to read as follows:

''(f) DEFINITIONS.—In this section:

''(1) the term 'covered educational institution' means—

''(A) an institution of higher education eligible for assistance under title III or V of the Higher Education Act of 1965 (20 U.S.C. 1051 et seq.); or

''(B) an accredited postsecondary minority institution.

''(2) The term 'university-affiliated research center' means a research organization within an institution of higher education (as defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)) that—

''(A) provides or maintains Department essential engineering, research, or development capabilities; and

''(B) receives sole source contract funding from the Department pursuant to section 2304(c)(3)(B) of this title.''.

SEC. _____. FUNDING FOR APPLIED AND ADVANCED TECHNOLOGY DEVELOPMENT AT HISTORICALLY BLACK COLLEGES AND UNIVERSITIES AND MINORITY INSTITUTIONS.

(a) ADDITIONAL FUNDING.—

(1) APPLIED RESEARCH.—(A) The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with the amount of the increase to be available for Advancement of S&T Priorities (PE 0602251D8Z).

(B) The amount available under subparagraph (A) shall be available for minority institutions.

(2) ADVANCED TECHNOLOGY DEVELOPMENT.—(A) The amount authorized to be appropriated for fiscal year 2022 by section 201 for research, development, test, and evaluation is hereby increased by $10,000,000, with the amount of the increase to be available for Advanced Research (PE 0603180C).

(B) The amount available under subparagraph (A) shall be available for minority institutions.

(b) OFFSET.—The amount authorized to be appropriated for fiscal year 2022 by section 301 for operation and maintenance is hereby decreased by $20,000,000, with the amount of the decrease to be taken from amounts available as specified in the funding table in section 4301 for the Afghanistan Security Forces Fund, Afghan Air Force Sustainment.

(c) MINORITY INSTITUTION DEFINED.—In this subsection, the term ''minority institution'' means—

(1) a part B institution (as such term is defined in section 322 of the Higher Education Act of 1965 (20 U.S.C. 1061)); or

(2) an accredited minority institution (as such term is defined in section 365 of the Higher Education Act of 1965 (20 U.S.C. 1067k)).

SA 4822. Mrs. BLACKBURN submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

Strike section 853 and insert the following:

SEC. 853. DETERMINATION WITH RESPECT TO OPTICAL FIBER FOR DEPARTMENT OF DEFENSE PURPOSES.

(a) DETERMINATION.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Commerce, in consultation with the Secretary of Defense and the Director of the Cybersecurity and Infrastructure Security Agency, shall determine whether access, metro, and long-haul passive optical fiber and optical fiber cable that is manufactured or produced by an entity owned or controlled by the People's Republic of China pose an unacceptable risk to the national security of the United States or the security and safety of United States persons pursuant to section 2(b)(1) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1601(b)(1)).

(2) APPLICABILITY.—If the Secretary of Commerce makes a determination that any such optical fiber or optical fiber cable would pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, and the Commission makes the determination required under section 2(b)(2) of the Secure and Trusted Communications Networks Act (47 U.S.C. 1601(b)(2)), the inclusion of such optical fiber and optical fiber cable on the covered communications equipment and services list shall apply only to such optical fiber or optical fiber cable deployed after such determination.

(b) NOTIFICATION REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce shall notify the congressional defense committees, the Committee on Commerce, Science, and Transportation of the Senate, and the Committee on Energy and Commerce of the House of Representatives of the findings of the review and determination required under subsection (a), publish the determination in the Federal Register, and submit that determination to the relevant Federal agencies, including the Department of Defense, the Cybersecurity and Infrastructure Security Agency, and the Federal Communications Commission.

(c) SAVINGS CLAUSE.—No determination made under section (a) shall impact the current filing and reimbursement process for the Secure and Trusted Communications Networks Reimbursement Program at the Federal Communications Commission.

(d) DEFINITIONS.—In this section:

(1) The term ''access'' means optical fiber and optical fiber cable that connects subscribers (residential and business) and radio sites to a service provider.

(2) The term ''control'' means the ability to determine the outcome of decision-making for a company through the strategic policy setting exercised by boards of directors or similar organizational governance bodies and the day-to-day management and administration of business operations as overseen by principals.

(3) The term ''long haul'' means optical fiber and optical fiber cable that connects cities and metropolitan areas.

(4) The term ''metro'' means optical fiber and optical fiber cable that connects city

business districts and central city and suburban areas.

(5) The term ''passive'' means unpowered optical fiber and optical fiber cable.

SA 4823. Mr. MARKEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

Strike section 6505 and insert the following:

SEC. 6505. BRIEFING ON CONSULTATIONS WITH UNITED STATES ALLIES REGARDING NUCLEAR POSTURE REVIEW.

(a) IN GENERAL.—Not later than January 31, 2022, the Secretary of Defense, in coordination with the Secretary of State, shall brief the appropriate congressional committees on all consultations with United States allies and related matters regarding the 2021 Nuclear Posture Review.

(b) ELEMENTS.—The briefing required by subsection shall include the following:

(1) A listing of all countries consulted with respect to the 2021 Nuclear Posture Review, including the dates and circumstances of each such consultation and the countries present.

(2) An overview of the topics and concepts discussed with each such country during such consultations, including any discussion of potential changes to the nuclear declaratory policy of the United States.

(3) A summary of any feedback provided during such consultations.

(4) A description of the consultations conducted by the Department of Defense and the Department of State with experts outside such Departments and civil society organizations with respect to the 2021 Nuclear Posture Review.

(5) A listing of the consultants who participated in the 2021 Nuclear Posture Review in a formal or informal capacity.

(6) An identification of the options related to United States nuclear force structure and nuclear doctrine that were presented to the President by the Department of Defense.

SA 4824. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1064. ENSURING CONSIDERATION OF THE NATIONAL SECURITY IMPACTS OF URANIUM AS A CRITICAL MINERAL.

(a) IN GENERAL.—The Secretary of Defense, in coordination with the Secretary of Energy, the Secretary of the Interior (acting through the Director of the United States Geological Survey), and the Secretary of Commerce, shall conduct an assessment of the effect on national security that may result from uranium ceasing to be designated as a critical mineral by the Secretary of the Interior pursuant to section 7002(c) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(c)).

(b) REPORT REQUIRED.—Not later than 180 days after enactment of this Act, the Secretary of Defense shall submit to the appropriate committees of Congress a report on the findings of the assessment conducted under subsection (a), including an assessment of—

(1) any effects the change in designation described in that subsection may have on domestic uranium production;

(2) any effects of the reliance of the United States on imports of uranium from foreign sources, including from state-owned entities, to supply fuel for commercial reactors;

(3) the effects of such reliance and other factors on the domestic production, conversion, fabrication, and enrichment of uranium as it relates to national security, including energy security purposes; and

(4) any effects on Federal national security programs, including existing and future uses of unobligated, United States-origin uranium.

(c) RECOMMENDATION ON URANIUM CRITICAL MINERAL DESIGNATION.—The report required by subsection (b) shall include a recommendation to the Secretary of the Interior regarding whether it is in the interest of the United States to consider uranium for future designation as a critical mineral pursuant to section 7002(c) of the Energy Act of 2020 (division Z of Public Law 116–260; 30 U.S.C. 1606(c)).

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Armed Services, the Committee on Energy and Natural Resources, the Committee on Commerce, Science, and Transportation of the Senate; and

(2) the Committee on Armed Services, the Committee on Energy and Commerce, and the Committee on Natural Resources of the House of Representatives.

SA 4825. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. HA–LEU FOR ADVANCED NUCLEAR REACTORS.

Section 2001 of the Energy Act of 2020 (42 U.S.C. 16281) is amended—

(1) in subsection (a)—

(A) in paragraph (2)—

(i) in subparagraph (D)—

(I) in clause (v)(III), by adding ''or'' after the semicolon at the end;

(II) by striking clause (vi); and

(III) by redesignating clause (vii) as clause (vi); and

(ii) in subparagraph (E), by striking ''for domestic commercial use'' and inserting ''to meet the needs of commercial, government, academic, and international entities''; and

(B) by redesignating paragraphs (6) and (7) as paragraphs (8) and (6), respectively, and moving the paragraphs so as to appear in numerical order;

(2) in subsection (b)(2)—

(A) by striking ''subsection (a)(1)'' each place it appears and inserting ''subsection (b)(1)'';

(B) in subparagraph (B)(viii), by striking ''subsection (a)(2)(F)'' and inserting ''subsection (b)(2)(F)''; and

(C) in subparagraph (D)(vi), by striking ''subsection (a)(2)(A)'' and inserting ''subsection (b)(2)(A)'';

(3) in subsection (c)—

(A) by redesignating paragraphs (1) through (5) as subparagraphs (A) through (E), respectively, and indenting appropriately; and

(B) in the matter preceding subparagraph (A) (as so redesignated)—

(i) by striking ''There are'' and inserting the following:

''(7) AUTHORIZATION OF APPROPRIATIONS.—There are''; and

(ii) by striking ''in this section'' and inserting ''under this subsection'';

(4) in subsection (d)—

(A) by redesignating paragraphs (1) through (6) as paragraphs (2), (3), (5), (6), (7), and (8), respectively;

(B) by inserting before paragraph (2) (as so redesignated) the following:

''(1) ADVANCED NUCLEAR REACTOR.—The term 'advanced nuclear reactor' has the meaning given the term in section 951(b) of the Energy Policy Act of 2005 (42 U.S.C. 16271(b)).''; and

(C) by inserting after paragraph (3) (as so redesignated) the following:

''(4) DEPARTMENT.—The term 'Department' means the Department of Energy.'';

(5) by moving paragraph (7) of subsection (c) (as designated by paragraph (3)(B)(i)) so as to appear after paragraph (6) of subsection (a) (as redesignated by paragraph (1)(B));

(6) by striking subsection (c);

(7) by redesignating subsections (a), (b), and (d) as subsections (b), (g), and (a), respectively, and moving the subsections so as to appear in alphabetical order; and

(8) by inserting after subsection (b) (as so redesignated) the following:

''(c) HA–LEU FOR ADVANCED NUCLEAR REACTOR DEMONSTRATION PROJECTS.—

''(1) ACTIVITIES.—Not later than 30 days after the date of enactment of the National Defense Authorization Act for Fiscal Year 2022, the Secretary shall initiate activities to make available HA–LEU, produced from inventories owned by the Department, for use by advanced nuclear reactors, with priority given to the awards made pursuant to the funding opportunity announcement of the Department numbered DE–FOA–0002271 for Pathway 1, Advanced Reactor Demonstrations, with additional HA–LEU to be made available to members of the consortium established under subsection (b)(2)(F), as available.

''(2) OWNERSHIP.—HA–LEU made available under this subsection—

''(A) shall remain the property of, and title shall remain with, the Department; and

''(B) shall not be subject to the requirements of section 3112(d)(2) and 3113 of the USEC Privatization Act (42 U.S.C. 2297h–10(d)(2), 2297h–11).

''(3) QUANTITY.—In carrying out activities under this subsection, the Secretary, to the maximum extent practicable, shall make available—

''(A) by September 30, 2024, not less than 3 metric tons of HA–LEU; and

''(B) by December 31, 2025, not less than an additional 15 metric tons of HA–LEU.

''(4) FACTORS FOR CONSIDERATION.—In carrying out activities under this subsection, the Secretary shall take into consideration—

''(A) options for providing HA–LEU from a stockpile of uranium owned by the Department (including the National Nuclear Security Administration), including—

''(i) fuel that—

''(I) directly meets the needs of the end-users described in paragraph (1); but

''(II) has been previously used or fabricated for another purpose;

''(ii) fuel that can meet the needs of the end-users described in paragraph (1) after removing radioactive or other contaminants that resulted from a previous use or fabrication of the fuel for research, development, demonstration, or deployment activities of the Department (including activities of the National Nuclear Security Administration);

''(iii) fuel from a high-enriched uranium stockpile, which can be blended with lower assay uranium to become HA–LEU to meet the needs of the end-users described in paragraph (1); and

''(iv) fuel from uranium stockpiles intended for other purposes, but for which material could be swapped or replaced in time in such a manner that would not negatively impact the missions of the Department;

''(B) options for providing HA–LEU from domestically enriched HA–LEU procured by the Department through a competitive process pursuant to the HA–LEU Bank established under subsection (d)(3)(C); and

''(C) options to replenish, as needed, Department stockpiles of uranium made available pursuant to subparagraph (A) with domestically enriched HA–LEU procured by the Department through a competitive process pursuant to the HA–LEU Bank established under subsection (d)(3)(C).

''(5) LIMITATION.—The Secretary shall not barter or otherwise sell or transfer uranium in any form in exchange for services relating to—

''(A) the final disposition of radioactive waste from uranium that is the subject of a contract for sale, resale, transfer, or lease under this subsection; or

''(B) environmental cleanup activities.

''(6) APPROPRIATIONS.—In addition to amounts otherwise made available, there is appropriated to the Secretary to carry out this subsection, out of any amounts in the Treasury not otherwise appropriated, $200,000,000 for each of fiscal years 2022 through 2026.

''(7) SUNSET.—The authority of the Secretary to carry out activities under this subsection shall terminate on the earlier of—

''(A) September 30, 2027; and

''(B) the date on which the HA–LEU needs of the end-users described in paragraph (1) can be fully met by commercial enrichers in the United States.

''(d) COMMERCIAL HA–LEU AVAILABILITY.—

''(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of the National Defense Authorization Act for Fiscal Year 2022, the Secretary shall establish a program (referred to in this subsection as the 'program') to accelerate the availability of commercially produced HA–LEU in the United States in accordance with this subsection.

''(2) PURPOSES.—The purposes of the program are—

''(A) to provide for the availability of HA–LEU enriched, deconverted, and fabricated in the United States;

''(B) to address nuclear supply chain issues in the United States; and

''(C) to support strategic nuclear fuel cycle capabilities in the United States.

''(3) CONSIDERATIONS.—In carrying out the program, the Secretary shall consider and, as appropriate, execute—

''(A) options to establish, through a competitive process, a commercial HA–LEU production capability of not less than 20 metric tons of HA–LEU per year by—

''(i) December 31, 2026; or

''(ii) the earliest operationally feasible date thereafter;

''(B) options that provide for an array of HA–LEU—

''(i) enrichment levels;

''(ii) output levels to meet demand; and

''(iii) fuel forms; and

''(C) options to establish, through a competitive process, a HA–LEU Bank—

''(i) to replenish Department stockpiles of material used in carrying out activities under subsection (c); and

''(ii) after replenishing those stockpiles, to make HA–LEU available to members of the consortium established under subsection (b)(2)(F).

''(4) APPROPRIATIONS.—In addition to amounts otherwise made available, there is appropriated to the Secretary to carry out this subsection, out of any amounts in the Treasury not otherwise appropriated, $150,000,000 for each of fiscal years 2022 through 2031.

''(e) COST RECOVERY.—

''(1) IN GENERAL.—In carrying out activities under subsections (c) and (d), the Secretary shall ensure that any HA–LEU acquired, provided, or made available under those subsections for members of the consortium established under subsection (b)(2)(F) is subject to cost recovery in accordance with subsection (b)(2)(G).

''(2) AVAILABILITY OF CERTAIN FUNDS.—Notwithstanding section 3302 of title 31, United States Code, revenues received from the sale or transfer of fuel feed material and other activities related to making HA–LEU available pursuant to this section—

''(A) shall be available to the Department for carrying out the purposes of this section, to reduce the need for further appropriations for those purposes; and

''(B) shall remain available until expended.

''(f) EXCLUSION.—In carrying out activities under this section, the Secretary shall not make available, or provide funding for, uranium that is recovered, downblended, converted, or enriched by an entity that—

''(1) is owned or controlled by the Government of the Russian Federation or the Government of the People's Republic of China; or

''(2) is organized under the laws of, or otherwise subject to the jurisdiction of, the Russian Federation or the People's Republic of China.''.

SA 4826. Mr. TOOMEY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. STATE AND LOCAL LAW ENFORCEMENT ACCESS TO LIFESAVING FEDERAL EQUIPMENT.

(a) UNENFORCEABILITY OF CERTAIN REGULATIONS UNLESS ENACTED INTO LAW.—

(1) IN GENERAL.—No regulation, rule, guidance, policy, or recommendations issued on or after May 15, 2015, that limits the sale or donation of property of the Federal Government, including excess property of the Department of Defense, to State and local agencies for law enforcement activities (whether pursuant to section 2576a of title 10, United States Code, or any other provision of law, or as a condition on the use of Federal funds) shall have any force or effect after the date of the enactment of this Act unless enacted into law by Congress.

(2) PROHIBITION ON USE OF FUNDS TO ENFORCE REGULATIONS.—No agency or instrumentality of the Federal Government may use any Federal funds, fees, or resources to implement or carry out a regulation, rule, guidance, policy, or recommendation issued as described in subsection (a) that is not enacted into law by Congress.

(b) RETURN OR REISSUE OF EQUIPMENT RECALLED OR SEIZED PURSUANT TO REGULATIONS.—Any property recalled or seized on or after May 15, 2015, pursuant to a regulation, rule, guidance, policy, or recommendation issued as described in subsection (a) shall be returned, replaced, or re-issued to the agency from which recalled or seized, at no cost to such agency, as soon as practicable after the date of the enactment of this Act.

SA 4827. Mr. ROUNDS (for himself and Mr. VAN HOLLEN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title XII, add the following:

SEC. 1283. SENSE OF CONGRESS ON THE NECESSITY OF MAINTAINING THE UNITED NATIONS ARMS EMBARGO ON SOUTH SUDAN UNTIL CONDITIONS FOR PEACE, STABILITY, DEMOCRACY, AND DEVELOPMENT EXIST.

It is the sense of Congress that—

(1) the signatories to the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan, signed on September 12, 2018, have delayed implementation, leading to continued conflict and instability in South Sudan;

(2) despite years of fighting, 2 peace agreements, punitive actions by the international community, and widespread suffering among civilian populations, the leaders of South Sudan have failed to build sustainable peace;

(3) the United Nations arms embargo on South Sudan, most recently extended by 1 year to May 31, 2022, through United Nations Security Council Resolution 2577 (2021), is a necessary act by the international community to stem the illicit transfer and destabilizing accumulation and misuse of small arms and light weapons in perpetuation of the conflict in South Sudan;

(4) the United States should call on other member states of the United Nations to redouble efforts to enforce the United Nations arms embargo on South Sudan; and

(5) the United States, through the United States Mission to the United Nations, should use its voice and vote in the United Nations Security Council in favor of maintaining the United Nations arms embargo on South Sudan until—

(A) the Revitalized Agreement on the Resolution of the Conflict in the Republic of South Sudan is fully implemented; or

(B) credible, fair, and transparent democratic elections are held in South Sudan.

SA 4828. Mr. BLUMENTHAL submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year

2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle B of title XII, insert the following:

SEC. 1216. STRATEGY TO SUPPORT NATIONALS OF AFGHANISTAN WHO ARE APPLICANTS FOR SPECIAL IMMIGRANT VISAS OR FOR REFERRAL TO THE UNITED STATES REFUGEE ADMISSIONS PROGRAM.

(a) SENSE OF CONGRESS.—It is the sense of Congress that the United States should increase support for nationals of Afghanistan who aided the United States mission in Afghanistan during the past 20 years and are now under threat from the Taliban, specifically such nationals of Afghanistan, in Afghanistan or third countries, who are applicants for—

(1) special immigrant visas under the Afghan Allies Protection Act of 2009 (8 U.S.C. 1101 note; Public Law 111–8) or section 1059 of the National Defense Authorization Act for Fiscal Year 2006 (8 U.S.C. 1101 note; Public Law 109–163); or

(2) referral to the United States Refugee Admissions Program as refugees (as defined in section 101(a)(42) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(42))), including as Priority 2 refugees.

(b) STRATEGY.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of State, in coordination with the Secretary of Homeland Security and the heads of other relevant Federal departments and agencies, shall submit to the appropriate committees of Congress a strategy for the safe processing abroad of nationals of Afghanistan described in subsection (a).

(2) ELEMENTS.—The strategy required by paragraph (1) shall include a detailed plan—

(A) to prioritize for evacuation from Afghanistan nationals of Afghanistan described in subsection (a);

(B) to provide for expedited initial security vetting for such nationals of Afghanistan, to be conducted remotely before their departure from Afghanistan;

(C) to facilitate, after such vetting, the rapid departure from Afghanistan by air charter and land passage of such nationals of Afghanistan who satisfy the requirements of such vetting;

(D) to provide letters of support, diplomatic notes, and other documentation, as appropriate, to ease transit for such nationals of Afghanistan;

(E) to engage governments of relevant countries to better facilitate evacuation of such nationals of Afghanistan;

(F) to disseminate frequent updates to such nationals of Afghanistan and relevant nongovernmental organizations with respect to evacuation from Afghanistan;

(G) to identify and establish sufficient locations outside Afghanistan and the United States that will accept such nationals of Afghanistan during application processing (including during the processes of vetting and establishing the eligibility of such nationals of Afghanistan before their travel to the United States, which shall include any required in-person interviews) for—

(i) the special immigrant visas described in paragraph (1) of subsection (a); or

(ii) referral to the United States Refugee Admissions Program described in paragraph (2) of that subsection;

(H) to identify necessary resource, personnel, and equipment requirements to increase capacity to better support such nationals of Afghanistan and reduce their application processing times, while ensuring strict and necessary security vetting, including, to the extent practicable, by allowing such nationals of Afghanistan to receive referrals to the United States Refugee Admissions Program while they are still in Afghanistan so as to initiate application processing more expeditiously; and

(I) to provide for relocation outside Afghanistan to third countries for nationals of Afghanistan described in subsection (a) who are unable to successfully complete security vetting and application processing to establish eligibility to travel to the United States.

(3) FORM.—The strategy required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(c) MONTHLY REPORT.—

(1) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, and monthly thereafter until December 31, 2022, the Secretary of State, in coordination with the Secretary of Homeland Security and the heads of other relevant Federal departments and agencies, shall submit to the appropriate committees of Congress a report on efforts to support nationals of Afghanistan described in subsection (a).

(2) ELEMENTS.—Each report required by paragraph (1) shall include the following:

(A) The number of nationals of Afghanistan referred to the United States Refugee Admissions Program as Priority 1 and Priority 2 refugees since August 29, 2021.

(B) An assessment of whether each such refugee—

(i) remains in Afghanistan; or

(ii) is outside Afghanistan.

(C) With respect to nationals of Afghanistan who have applied for referral to the United States Refugee Program, the number applications that—

(i) have been approved;

(ii) have been denied; and

(iii) are pending adjudication.

(D) The number of nationals of Afghanistan who have pending applications for special immigrant visas described in subsection (a)(1), disaggregated by the special immigrant visa processing steps completed with respect to such individuals.

(E) A description of the measures taken to implement the strategy under subsection (b).

(d) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

(1) the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Homeland Security and Governmental Affairs; and the Committee on Armed Services of the Senate; and

(2) the Committee on Foreign Affairs, the Committee on the Judiciary, the Committee on Homeland Security, and the Committee on Armed Services of the House of Representatives.

SA 4829. Mr. LEE submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. RELEASE OF REVERSIONARY INTEREST OF THE UNITED STATES IN NON-FEDERAL LAND IN SALT LAKE CITY, UTAH.

(a) RELEASE.—There is released to the University of Utah, without consideration, the reversionary interest of the United States in the non-Federal land described in subsection (b).

(b) DESCRIPTION OF NON-FEDERAL LAND.—The non-Federal land referred to in subsection (a) is the approximately 593 acres of land of the University of Utah—

(1) depicted as ''U of U Research Park'' on the map—

(A) prepared by the Bureau of Land Management;

(B) entitled ''University of Utah-Research Park''; and

(C) dated September 23, 2021;

(2) identified in the patent—

(A) numbered 43–99–0012; and

(B) dated October 18, 1968; and

(3) more particularly described as tracts D (excluding the parcels numbered 1, 2, 3, 4, and 5), G, and J, T. 1 S., R. 1 E., Salt Lake Meridian.

SA 4830. Mr. MANCHIN (for himself, Mrs. CAPITO, Mrs. HYDE-SMITH, Mr. ROMNEY, Mr. COTTON, Mrs. BLACKBURN, and Mr. TESTER) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle E of title X, add the following:

SEC. 1043. HONORING HERSHEL WOODROW "WOODY" WILLIAMS AS THE LAST SURVIVING MEDAL OF HONOR RECIPIENT OF WORLD WAR II.

(a) USE OF ROTUNDA.—Upon his death, Hershel Woodrow ''Woody'' Williams, who is the last surviving recipient of the Medal of Honor for acts performed during World War II, shall be permitted to lie in state in the rotunda of the United States Capitol if he or his next of kin so elects.

(b) IMPLEMENTATION.—The Architect of the Capitol, under the direction of the President pro tempore of the Senate and the Speaker of the House of Representatives, shall take the necessary steps to implement subsection (a).

SA 4831. Mr. SCOTT of Florida submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

SEC. 5101. SHORT TITLE.

This division may be cited as the ''Federal Information Security Modernization Act of 2021''.

SEC. 5102. DEFINITIONS.

In this division, unless otherwise specified:

(1) ADDITIONAL CYBERSECURITY PROCEDURE.—The term ''additional cybersecurity procedure'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this division.

(2) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

(B) the Committee on Oversight and Reform of the House of Representatives; and

(C) the Committee on Homeland Security of the House of Representatives.

(4) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(5) INCIDENT.—The term ''incident'' has the meaning given the term in section 3552(b) of title 44, United States Code.

(6) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given the term in section 3552(b) of title 44, United States Code.

(7) PENETRATION TEST.—The term ''penetration test'' has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this division.

(8) THREAT HUNTING.—The term ''threat hunting'' means proactively and iteratively searching for threats to systems that evade detection by automated threat detection systems.

TITLE LI—UPDATES TO FISMA

SEC. 5121. TITLE 44 AMENDMENTS.

(a) SUBCHAPTER I AMENDMENTS.—Subchapter I of chapter 35 of title 44, United States Code, is amended—

(1) in section 3504—

(A) in subsection (a)(1)(B)—

(i) by striking clause (v) and inserting the following:

''(v) confidentiality, privacy, disclosure, and sharing of information;'';

(ii) by redesignating clause (vi) as clause (vii); and

(iii) by inserting after clause (v) the following:

''(vi) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, security of information; and''; and

(B) in subsection (g), by striking paragraph (1) and inserting the following:

''(1) develop, and in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and'';

(2) in section 3505—

(A) in paragraph (3) of the first subsection designated as subsection (c)—

(i) in subparagraph (B)—

(I) by inserting ''the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and'' before ''the Comptroller General''; and

(II) by striking ''and'' at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(D) maintained on a continual basis through the use of automation, machine-readable data, and scanning.''; and

(B) by striking the second subsection designated as subsection (c);

(3) in section 3506—

(A) in subsection (b)(1)(C), by inserting '', availability'' after ''integrity''; and

(B) in subsection (h)(3), by inserting ''security,'' after ''efficiency,''; and

(4) in section 3513—

(A) by redesignating subsection (c) as subsection (d); and

(B) by inserting after subsection (b) the following:

''(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.''.

(b) SUBCHAPTER II DEFINITIONS.—

(1) IN GENERAL.—Section 3552(b) of title 44, United States Code, is amended—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), (6), and (7) as paragraphs (2), (3), (4), (5), (6), (9), and (11), respectively;

(B) by inserting before paragraph (2), as so redesignated, the following:

''(1) The term 'additional cybersecurity procedure' means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.'';

(C) by inserting after paragraph (6), as so redesignated, the following:

''(7) The term 'high value asset' means information or an information system that the head of an agency determines so critical to the agency that the loss or corruption of the information or the loss of access to the information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

''(8) The term 'major incident' has the meaning given the term in guidance issued by the Director under section 3598(a).'';

(D) by inserting after paragraph (9), as so redesignated, the following:

''(10) The term 'penetration test' means a specialized type of assessment that—

''(A) is conducted on an information system or a component of an information system; and

''(B) emulates an attack or other exploitation capability of a potential adversary, typically under specific constraints, in order to identify any vulnerabilities of an information system or a component of an information system that could be exploited.''; and

(E) by inserting after paragraph (11), as so redesignated, the following:

''(12) The term 'shared service' means a centralized business or mission capability that is provided to multiple organizations within an agency or to multiple agencies.''.

(2) CONFORMING AMENDMENTS.—

(A) HOMELAND SECURITY ACT OF 2002.—Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''.

(B) TITLE 10.—

(i) SECTION 2222.—Section 2222(i)(8) of title 10, United States Code, is amended by striking ''section 3552(b)(6)(A)'' and inserting ''section 3552(b)(9)(A)''.

(ii) SECTION 2223.—Section 2223(c)(3) of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(iii) SECTION 2315.—Section 2315 of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(iv) SECTION 2339A.—Section 2339a(e)(5) of title 10, United States Code, is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(C) HIGH-PERFORMANCE COMPUTING ACT OF 1991.—Section 207(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5527(a)) is amended by striking ''section 3552(b)(6)(A)(i)'' and inserting ''section 3552(b)(9)(A)(i)''.

(D) INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 3(5) of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a) is amended by striking ''section 3552(b)(6)'' and inserting ''section 3552(b)''.

(E) NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013.—Section 933(e)(1)(B) of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(F) IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011.—The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) is amended—

(i) in section 806(e)(5) (10 U.S.C. 2304 note), by striking ''section 3542(b)'' and inserting ''section 3552(b)'';

(ii) in section 931(b)(3) (10 U.S.C. 2223 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''; and

(iii) in section 932(b)(2) (10 U.S.C. 2224 note), by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(G) E-GOVERNMENT ACT OF 2002.—Section 301(c)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended by striking ''section 3542(b)(2)'' and inserting ''section 3552(b)''.

(H) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT.—Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended—

(i) in subsection (a)(2), by striking ''section 3552(b)(5)'' and inserting ''section 3552(b)''; and

(ii) in subsection (f)—

(I) in paragraph (3), by striking ''section 3532(1)'' and inserting ''section 3552(b)''; and

(II) in paragraph (5), by striking ''section 3532(b)(2)'' and inserting ''section 3552(b)''.

(c) SUBCHAPTER II AMENDMENTS.—Subchapter II of chapter 35 of title 44, United States Code, is amended—

(1) in section 3551—

(A) in paragraph (4), by striking ''diagnose and improve'' and inserting ''integrate, deliver, diagnose, and improve'';

(B) in paragraph (5), by striking ''and'' at the end;

(C) in paragraph (6), by striking the period at the end and inserting a semi colon; and

(D) by adding at the end the following:

''(7) recognize that each agency has specific mission requirements and, at times, unique cybersecurity requirements to meet the mission of the agency;

''(8) recognize that each agency does not have the same resources to secure agency systems, and an agency should not be expected to have the capability to secure the systems of the agency from advanced adversaries alone; and

''(9) recognize that a holistic Federal cybersecurity model is necessary to account for differences between the missions and capabilities of agencies.'';

(2) in section 3553—

(A) by striking the section heading and inserting ''**Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency**''.

(B) in subsection (a)—

(i) in paragraph (1), by inserting '', in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director,'' before ''overseeing'';

(ii) in paragraph (5), by striking ''and'' at the end; and

(iii) by adding at the end the following:

''(8) promoting, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the

National Institute of Standards and Technology—

''(A) the use of automation to improve Federal cybersecurity and visibility with respect to the implementation of Federal cybersecurity; and

''(B) the use of presumption of compromise and least privilege principles to improve resiliency and timely response actions to incidents on Federal systems.'';

(C) in subsection (b)—

(i) by striking the subsection heading and inserting ''CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'';

(ii) in the matter preceding paragraph (1), by striking ''The Secretary, in consultation with the Director'' and inserting ''The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and the National Cyber Director'';

(iii) in paragraph (2)—

(I) in subparagraph (A), by inserting ''and reporting requirements under subchapter IV of this title'' after ''section 3556''; and

(II) in subparagraph (D), by striking ''the Director or Secretary'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(iv) in paragraph (5), by striking ''coordinating'' and inserting ''leading the coordination of'';

(v) in paragraph (8), by striking ''the Secretary's discretion'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency's discretion''; and

(vi) in paragraph (9), by striking ''as the Director or the Secretary, in consultation with the Director,'' and inserting ''as the Director of the Cybersecurity and Infrastructure Security Agency'';

(D) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking ''each year'' and inserting ''each year during which agencies are required to submit reports under section 3554(c)'';

(ii) by striking paragraph (1);

(iii) by redesignating paragraphs (2), (3), and (4) as paragraphs (1), (2), and (3), respectively;

(iv) in paragraph (3), as so redesignated, by striking ''and'' at the end;

(v) by inserting after paragraph (3), as so redesignated the following:

''(4) a summary of each assessment of Federal risk posture performed under subsection (i);''; and

(vi) in paragraph (5), by striking the period at the end and inserting ''; and'';

(E) by redesignating subsections (i), (j), (k), and (l) as subsections (j), (k), (l), and (m) respectively;

(F) by inserting after subsection (h) the following:

''(i) FEDERAL RISK ASSESSMENTS.—On an ongoing and continuous basis, the Director of the Cybersecurity and Infrastructure Security Agency shall perform assessments of Federal risk posture using any available information on the cybersecurity posture of agencies, and brief the Director and National Cyber Director on the findings of those assessments including—

''(1) the status of agency cybersecurity remedial actions described in section 3554(b)(7);

''(2) any vulnerability information relating to the systems of an agency that is known by the agency;

''(3) analysis of incident information under section 3597;

''(4) evaluation of penetration testing performed under section 3559A;

''(5) evaluation of vulnerability disclosure program information under section 3559B;

''(6) evaluation of agency threat hunting results;

''(7) evaluation of Federal and non-Federal cyber threat intelligence;

''(8) data on agency compliance with standards issued under section 11331 of title 40;

''(9) agency system risk assessments performed under section 3554(a)(1)(A); and

''(10) any other information the Director of the Cybersecurity and Infrastructure Security Agency determines relevant.''; and

(G) in subsection (j), as so redesignated—

(i) by striking ''regarding the specific'' and inserting ''that includes a summary of—

''(1) the specific'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and'' and

(iii) by adding at the end the following:

''(2) the trends identified in the Federal risk assessment performed under subsection (i).''; and

(H) by adding at the end the following:

''(n) BINDING OPERATIONAL DIRECTIVES.—If the Director of the Cybersecurity and Infrastructure Security Agency issues a binding operational directive or an emergency directive under this section, not later than 2 days after the date on which the binding operational directive requires an agency to take an action, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate reporting entities the status of the implementation of the binding operational directive at the agency.'';

(3) in section 3554—

(A) in subsection (a)—

(i) in paragraph (1)—

(I) by redesignating subparagraphs (A), (B), and (C) as subparagraphs (B), (C), and (D), respectively;

(II) by inserting before subparagraph (B), as so redesignated, the following:

''(A) on an ongoing and continuous basis, performing agency system risk assessments that—

''(i) identify and document the high value assets of the agency using guidance from the Director;

''(ii) evaluate the data assets inventoried under section 3511 for sensitivity to compromises in confidentiality, integrity, and availability;

''(iii) identify agency systems that have access to or hold the data assets inventoried under section 3511;

''(iv) evaluate the threats facing agency systems and data, including high value assets, based on Federal and non-Federal cyber threat intelligence products, where available;

''(v) evaluate the vulnerability of agency systems and data, including high value assets, including by analyzing—

''(I) the results of penetration testing performed by the Department of Homeland Security under section 3553(b)(9);

''(II) the results of penetration testing performed under section 3559A;

''(III) information provided to the agency through the vulnerability disclosure program of the agency under section 3559B;

''(IV) incidents; and

''(V) any other vulnerability information relating to agency systems that is known to the agency;

''(vi) assess the impacts of potential agency incidents to agency systems, data, and operations based on the evaluations described in clauses (ii) and (iv) and the agency systems identified under clause (iii); and

''(vii) assess the consequences of potential incidents occurring on agency systems that would impact systems at other agencies, including due to interconnectivity between different agency systems or operational reliance on the operations of the system or data in the system;'';

(III) in subparagraph (B), as so redesignated, in the matter preceding clause (i), by striking ''providing information'' and inserting ''using information from the assessment conducted under subparagraph (A), providing, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, information'';

(IV) in subparagraph (C), as so redesignated—

(aa) in clause (ii) by inserting ''binding'' before ''operational''; and

(bb) in clause (vi), by striking ''and'' at the end; and

(V) by adding at the end the following:

''(E) providing an update on the ongoing and continuous assessment performed under subparagraph (A)—

''(i) upon request, to the inspector general of the agency or the Comptroller General of the United States; and

''(ii) on a periodic basis, as determined by guidance issued by the Director but not less frequently than annually, to—

''(I) the Director;

''(II) the Director of the Cybersecurity and Infrastructure Security Agency; and

''(III) the National Cyber Director;

''(F) in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and not less frequently than once every 3 years, performing an evaluation of whether additional cybersecurity procedures are appropriate for securing a system of, or under the supervision of, the agency, which shall—

''(i) be completed considering the agency system risk assessment performed under subparagraph (A); and

''(ii) include a specific evaluation for high value assets;

''(G) not later than 30 days after completing the evaluation performed under subparagraph (F), providing the evaluation and an implementation plan, if applicable, for using additional cybersecurity procedures determined to be appropriate to—

''(i) the Director of the Cybersecurity and Infrastructure Security Agency;

''(ii) the Director; and

''(iii) the National Cyber Director; and

''(H) if the head of the agency determines there is need for additional cybersecurity procedures, ensuring that those additional cybersecurity procedures are reflected in the budget request of the agency in accordance with the risk-based cyber budget model developed pursuant to section 3553(a)(7);'';

(ii) in paragraph (2)—

(I) in subparagraph (A), by inserting ''in accordance with the agency system risk assessment performed under paragraph (1)(A)'' after ''information systems'';

(II) in subparagraph (B)—

(aa) by striking ''in accordance with standards'' and inserting ''in accordance with—

''(i) standards''; and

(bb) by adding at the end the following:

''(ii) the evaluation performed under paragraph (1)(F); and

''(iii) the implementation plan described in paragraph (1)(G);''; and

(III) in subparagraph (D), by inserting '', through the use of penetration testing, the vulnerability disclosure program established under section 3559B, and other means,'' after ''periodically'';

(iii) in paragraph (3)—

(I) in subparagraph (A)—

(aa) in clause (iii), by striking ''and'' at the end;

(bb) in clause (iv), by adding ''and'' at the end; and

(cc) by adding at the end the following:

''(v) ensure that—

''(I) senior agency information security officers of component agencies carry out responsibilities under this subchapter, as directed by the senior agency information security officer of the agency or an equivalent official; and

''(II) senior agency information security officers of component agencies report to—

''(aa) the senior information security officer of the agency or an equivalent official; and

''(bb) the Chief Information Officer of the component agency or an equivalent official;''; and

(iv) in paragraph (5), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' before ''on the effectiveness'';

(B) in subsection (b)—

(i) by striking paragraph (1) and inserting the following:

''(1) pursuant to subsection (a)(1)(A), performing ongoing and continuous agency system risk assessments, which may include using guidelines and automated tools consistent with standards and guidelines promulgated under section 11331 of title 40, as applicable;'';

(ii) in paragraph (2)—

(I) by striking subparagraph (B) and inserting the following:

''(B) comply with the risk-based cyber budget model developed pursuant to section 3553(a)(7);''; and

(II) in subparagraph (D)—

(aa) by redesignating clauses (iii) and (iv) as clauses (iv) and (v), respectively;

(bb) by inserting after clause (ii) the following:

''(iii) binding operational directives and emergency directives promulgated by the Director of the Cybersecurity and Infrastructure Security Agency under section 3553;''; and

(cc) in clause (iv), as so redesignated, by striking ''as determined by the agency; and'' and inserting ''as determined by the agency, considering—

''(I) the agency risk assessment performed under subsection (a)(1)(A); and

''(II) the determinations of applying more stringent standards and additional cybersecurity procedures pursuant to section 11331(c)(1) of title 40; and'';

(iii) in paragraph (5)(A), by inserting '', including penetration testing, as appropriate,'' after ''shall include testing'';

(iv) in paragraph (6), by striking ''planning, implementing, evaluating, and documenting'' and inserting ''planning and implementing and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, evaluating and documenting'';

(v) by redesignating paragraphs (7) and (8) as paragraphs (8) and (9), respectively;

(vi) by inserting after paragraph (6) the following:

''(7) a process for providing the status of every remedial action and known system vulnerability to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable;''; and

(vii) in paragraph (8)(C), as so redesignated—

(I) by striking clause (ii) and inserting the following:

''(ii) notifying and consulting with the Federal information security incident center established under section 3556 pursuant to the requirements of section 3594;'';

(II) by redesignating clause (iii) as clause (iv);

(III) by inserting after clause (ii) the following:

''(iii) performing the notifications and other activities required under subchapter IV of this title; and''; and

(IV) in clause (iv), as so redesignated—

(aa) in subclause (I), by striking ''and relevant offices of inspectors general'';

(bb) in subclause (II), by adding ''and'' at the end;

(cc) by striking subclause (III); and

(dd) by redesignating subclause (IV) as subclause (III);

(C) in subsection (c)—

(i) by redesignating paragraph (2) as paragraph (5);

(ii) by striking paragraph (1) and inserting the following:

''(1) BIANNUAL REPORT.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021 and not less frequently than once every 2 years thereafter, using the continuous and ongoing agency system risk assessment under subsection (a)(1)(A), the head of each agency shall submit to the Director, the Director of the Cybersecurity and Infrastructure Security Agency, the majority and minority leaders of the Senate, the Speaker and minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the appropriate authorization and appropriations committees of Congress, the National Cyber Director, and the Comptroller General of the United States a report that—

''(A) summarizes the agency system risk assessment performed under subsection (a)(1)(A);

''(B) evaluates the adequacy and effectiveness of information security policies, procedures, and practices of the agency to address the risks identified in the agency system risk assessment performed under subsection (a)(1)(A), including an analysis of the agency's cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c));

''(C) summarizes the evaluation and implementation plans described in subparagraphs (F) and (G) of subsection (a)(1) and whether those evaluation and implementation plans call for the use of additional cybersecurity procedures determined to be appropriate by the agency; and

''(D) summarizes the status of remedial actions identified by inspector general of the agency, the Comptroller General of the United States, and any other source determined appropriate by the head of the agency.

''(2) UNCLASSIFIED REPORTS.—Each report submitted under paragraph (1)—

''(A) shall be, to the greatest extent practicable, in an unclassified and otherwise uncontrolled form; and

''(B) may include a classified annex.

''(3) ACCESS TO INFORMATION.—The head of an agency shall ensure that, to the greatest extent practicable, information is included in the unclassified form of the report submitted by the agency under paragraph (2)(A).

''(4) BRIEFINGS.—During each year during which a report is not required to be submitted under paragraph (1), the Director shall provide to the congressional committees described in paragraph (1) a briefing summarizing current agency and Federal risk postures.''; and

(iii) in paragraph (5), as so redesignated, by striking the period at the end and inserting '', including the reporting procedures established under section 11315(d) of title 40 and subsection (a)(3)(A)(v) of this section.''; and

(D) in subsection (d)(1), in the matter preceding subparagraph (A), by inserting ''and the Director of the Cybersecurity and Infrastructure Security Agency'' after ''the Director''; and

(4) in section 3555—

(A) in the section heading, by striking ''**ANNUAL INDEPENDENT**'' and inserting ''**INDEPENDENT**'';

(B) in subsection (a)—

(i) in paragraph (1), by inserting ''during which a report is required to be submitted under section 3553(c),'' after ''Each year'';

(ii) in paragraph (2)(A), by inserting '', including by penetration testing and analyzing the vulnerability disclosure program of the agency'' after ''information systems''; and

(iii) by adding at the end the following:

''(3) An evaluation under this section may include recommendations for improving the cybersecurity posture of the agency.'';

(C) in subsection (b)(1), by striking ''annual'';

(D) in subsection (e)(1), by inserting ''during which a report is required to be submitted under section 3553(c)'' after ''Each year'';

(E) by striking subsection (f) and inserting the following:

''(f) PROTECTION OF INFORMATION.—(1) Agencies, evaluators, and other recipients of information that, if disclosed, may cause grave harm to the efforts of Federal information security officers shall take appropriate steps to ensure the protection of that information, including safeguarding the information from public disclosure.

''(2) The protections required under paragraph (1) shall be commensurate with the risk and comply with all applicable laws and regulations.

''(3) With respect to information that is not related to national security systems, agencies and evaluators shall make a summary of the information unclassified and publicly available, including information that does not identify—

''(A) specific information system incidents; or

''(B) specific information system vulnerabilities.'';

(F) in subsection (g)(2)—

(i) by striking ''this subsection shall'' and inserting ''this subsection—

''(A) shall'';

(ii) in subparagraph (A), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(B) identify any entity that performs an independent evaluation under subsection (b).''; and

(G) by striking subsection (j) and inserting the following:

''(j) GUIDANCE.—

''(1) IN GENERAL.—The Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Chief Information Officers Council, the Council of the Inspectors General on Integrity and Efficiency, and other interested parties as appropriate, shall ensure the development of guidance for evaluating the effectiveness of an information security program and practices

''(2) PRIORITIES.—The guidance developed under paragraph (1) shall prioritize the identification of—

''(A) the most common threat patterns experienced by each agency;

''(B) the security controls that address the threat patterns described in subparagraph (A); and

''(C) any other security risks unique to the networks of each agency.''; and

(5) in section 3556(a)—

(A) in the matter preceding paragraph (1), by inserting ''within the Cybersecurity and Infrastructure Security Agency'' after ''incident center''; and

(B) in paragraph (4), by striking ''3554(b)'' and inserting ''3554(a)(1)(A)''.

(d) CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44, United States Code, is amended—

(A) by striking the item relating to section 3553 and inserting the following:

''3553. Authority and functions of the Director and the Director of the Cybersecurity and Infrastructure Security Agency.''; and

(B) by striking the item relating to section 3555 and inserting the following:

''3555. Independent evaluation.''.

(2) OMB REPORTS.—Section 226(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1524(c)) is amended—

(A) in paragraph (1)(B), in the matter preceding clause (i), by striking ''annually thereafter'' and inserting ''thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code''; and

(B) in paragraph (2)(B), in the matter preceding clause (i)—

(i) by striking ''annually thereafter'' and inserting ''thereafter during the years during which a report is required to be submitted under section 3553(c) of title 44, United States Code''; and

(ii) by striking ''the report required under section 3553(c) of title 44, United States Code'' and inserting ''that report''.

(3) NIST RESPONSIBILITIES.—Section 20(d)(3)(B) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)(3)(B)) is amended by striking ''annual''.

(e) FEDERAL SYSTEM INCIDENT RESPONSE.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

''§ 3591. Definitions

''(a) IN GENERAL.—Except as provided in subsection (b), the definitions under sections 3502 and 3552 shall apply to this subchapter.

''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter:

''(1) APPROPRIATE REPORTING ENTITIES.—The term 'appropriate reporting entities' means—

''(A) the majority and minority leaders of the Senate;

''(B) the Speaker and minority leader of the House of Representatives;

''(C) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(D) the Committee on Oversight and Reform of the House of Representatives;

''(E) the Committee on Homeland Security of the House of Representatives;

''(F) the appropriate authorization and appropriations committees of Congress;

''(G) the Director;

''(H) the Director of the Cybersecurity and Infrastructure Security Agency;

''(I) the National Cyber Director;

''(J) the Comptroller General of the United States; and

''(K) the inspector general of any impacted agency.

''(2) AWARDEE.—The term 'awardee'—

''(A) means a person, business, or other entity that receives a grant from, or is a party to a cooperative agreement or an other transaction agreement with, an agency; and

''(B) includes any subgrantee of a person, business, or other entity described in subparagraph (A).

''(3) BREACH.—The term 'breach' means—

''(A) a compromise of the security, confidentiality, or integrity of data in electronic form that results in unauthorized access to, or an acquisition of, personal information; or

''(B) a loss of data in electronic form that results in unauthorized access to, or an acquisition of, personal information.

''(4) CONTRACTOR.—The term 'contractor' means—

''(A) a prime contractor of an agency or a subcontractor of a prime contractor of an agency; and

''(B) any person or business that collects or maintains information, including personally identifiable information, on behalf of an agency.

''(5) FEDERAL INFORMATION.—The term 'Federal information' means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government in any medium or form.

''(6) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an agency, a contractor, an awardee, or another organization on behalf of an agency.

''(7) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

''(8) NATIONWIDE CONSUMER REPORTING AGENCY.—The term 'nationwide consumer reporting agency' means a consumer reporting agency described in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

''(9) VULNERABILITY DISCLOSURE.—The term 'vulnerability disclosure' means a vulnerability identified under section 3559B.

''§ 3592. Notification of breach

''(a) NOTIFICATION.—As expeditiously as practicable and without unreasonable delay, and in any case not later than 45 days after an agency has a reasonable basis to conclude that a breach has occurred, the head of the agency, in consultation with a senior privacy officer of the agency, shall—

''(1) determine whether notice to any individual potentially affected by the breach is appropriate based on an assessment of the risk of harm to the individual that considers—

''(A) the nature and sensitivity of the personally identifiable information affected by the breach;

''(B) the likelihood of access to and use of the personally identifiable information affected by the breach;

''(C) the type of breach; and

''(D) any other factors determined by the Director; and

''(2) as appropriate, provide written notice in accordance with subsection (b) to each individual potentially affected by the breach—

''(A) to the last known mailing address of the individual; or

''(B) through an appropriate alternative method of notification that the head of the agency or a designated senior-level individual of the agency selects based on factors determined by the Director.

''(b) CONTENTS OF NOTICE.—Each notice of a breach provided to an individual under subsection (a)(2) shall include—

''(1) a brief description of the rationale for the determination that notice should be provided under subsection (a);

''(2) if possible, a description of the types of personally identifiable information affected by the breach;

''(3) contact information of the agency that may be used to ask questions of the agency, which—

''(A) shall include an e-mail address or another digital contact mechanism; and

''(B) may include a telephone number or a website;

''(4) information on any remedy being offered by the agency;

''(5) any applicable educational materials relating to what individuals can do in response to a breach that potentially affects their personally identifiable information, including relevant contact information for Federal law enforcement agencies and each nationwide consumer reporting agency; and

''(6) any other appropriate information, as determined by the head of the agency or established in guidance by the Director.

''(c) DELAY OF NOTIFICATION.—

''(1) IN GENERAL.—The Attorney General, the Director of National Intelligence, or the Secretary of Homeland Security may delay a notification required under subsection (a) if the notification would—

''(A) impede a criminal investigation or a national security activity;

''(B) reveal sensitive sources and methods;

''(C) cause damage to national security; or

''(D) hamper security remediation actions.

''(2) DOCUMENTATION.—

''(A) IN GENERAL.—Any delay under paragraph (1) shall be reported in writing to the Director, the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Director of the Cybersecurity and Infrastructure Security Agency, and the head of the agency and the inspector general of the agency that experienced the breach.

''(B) CONTENTS.—A report required under subparagraph (A) shall include a written statement from the entity that delayed the notification explaining the need for the delay.

''(C) FORM.—The report required under subparagraph (A) shall be unclassified but may include a classified annex.

''(3) RENEWAL.—A delay under paragraph (1) shall be for a period of 60 days and may be renewed.

''(d) UPDATE NOTIFICATION.—If an agency determines there is a significant change in the reasonable basis to conclude that a breach occurred, a significant change to the determination made under subsection (a)(1), or that it is necessary to update the details of the information provided to impacted individuals as described in subsection (b), the agency shall as expeditiously as practicable and without unreasonable delay, and in any case not later than 30 days after such a determination, notify each individual who received a notification pursuant to subsection (a) of those changes.

''(e) EXEMPTION FROM NOTIFICATION.—

''(1) IN GENERAL.—The head of an agency, in consultation with the inspector general of the agency, may request an exemption from the Director from complying with the notification requirements under subsection (a) if the information affected by the breach is determined by an independent evaluation to be unreadable, including, as appropriate, instances in which the information is—

''(A) encrypted; and

''(B) determined by the Director of the Cybersecurity and Infrastructure Security Agency to be of sufficiently low risk of exposure.

''(2) APPROVAL.—The Director shall determine whether to grant an exemption requested under paragraph (1) in consultation with—

''(A) the Director of the Cybersecurity and Infrastructure Security Agency; and

''(B) the Attorney General.

''(3) DOCUMENTATION.—Any exemption granted by the Director under paragraph (1) shall be reported in writing to the head of the agency and the inspector general of the agency that experienced the breach and the Director of the Cybersecurity and Infrastructure Security Agency.

''(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

''(1) the Director from issuing guidance relating to notifications or the head of an

agency from notifying individuals potentially affected by breaches that are not determined to be major incidents; or

''(2) the Director from issuing guidance relating to notifications of major incidents or the head of an agency from providing more information than described in subsection (b) when notifying individuals potentially affected by breaches.

''§ 3593. Congressional and Executive Branch reports

''(a) INITIAL REPORT.—

''(1) IN GENERAL.—Not later than 72 hours after an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency impacted by the major incident shall submit to the appropriate reporting entities a written report and, to the extent practicable, provide a briefing to the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Reform of the House of Representatives, the Committee on Homeland Security of the House of Representatives, and the appropriate authorization and appropriations committees of Congress, taking into account—

''(A) the information known at the time of the report;

''(B) the sensitivity of the details associated with the major incident; and

''(C) the classification level of the information contained in the report.

''(2) CONTENTS.—A report required under paragraph (1) shall include, in a manner that excludes or otherwise reasonably protects personally identifiable information and to the extent permitted by applicable law, including privacy and statistical laws—

''(A) a summary of the information available about the major incident, including how the major incident occurred, information indicating that the major incident may be a breach, and information relating to the major incident as a breach, based on information available to agency officials as of the date on which the agency submits the report;

''(B) if applicable, a description and any associated documentation of any circumstances necessitating a delay in or exemption to notification to individuals potentially affected by the major incident under subsection (c) or (e) of section 3592; and

''(C) if applicable, an assessment of the impacts to the agency, the Federal Government, or the security of the United States, based on information available to agency officials on the date on which the agency submits the report.

''(b) SUPPLEMENTAL REPORT.—Within a reasonable amount of time, but not later than 30 days after the date on which an agency submits a written report under subsection (a), the head of the agency shall provide to the appropriate reporting entities written updates on the major incident and, to the extent practicable, provide a briefing to the congressional committees described in subsection (a)(1), including summaries of—

''(1) vulnerabilities, means by which the major incident occurred, and impacts to the agency relating to the major incident;

''(2) any risk assessment and subsequent risk-based security implementation of the affected information system before the date on which the major incident occurred;

''(3) the status of compliance of the affected information system with applicable security requirements at the time of the major incident;

''(4) an estimate of the number of individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

''(5) an assessment of the risk of harm to individuals potentially affected by the major incident based on information available to agency officials as of the date on which the agency provides the update;

''(6) an update to the assessment of the risk to agency operations, or to impacts on other agency or non-Federal entity operations, affected by the major incident based on information available to agency officials as of the date on which the agency provides the update; and

''(7) the detection, response, and remediation actions of the agency, including any support provided by the Cybersecurity and Infrastructure Security Agency under section 3594(d) and status updates on the notification process described in section 3592(a), including any delay or exemption described in subsection (c) or (e), respectively, of section 3592, if applicable.

''(c) UPDATE REPORT.—If the agency determines that there is any significant change in the understanding of the agency of the scope, scale, or consequence of a major incident for which an agency submitted a written report under subsection (a), the agency shall provide an updated report to the appropriate reporting entities that includes information relating to the change in understanding.

''(d) ANNUAL REPORT.—Each agency shall submit as part of the annual report required under section 3554(c)(1) of this title a description of each major incident that occurred during the 1-year period preceding the date on which the report is submitted.

''(e) DELAY AND EXEMPTION REPORT.—

''(1) IN GENERAL.—The Director shall submit to the appropriate notification entities an annual report on all notification delays and exemptions granted pursuant to subsections (c) and (d) of section 3592.

''(2) COMPONENT OF OTHER REPORT.—The Director may submit the report required under paragraph (1) as a component of the annual report submitted under section 3597(b).

''(f) REPORT DELIVERY.—Any written report required to be submitted under this section may be submitted in a paper or electronic format.

''(g) THREAT BRIEFING.—

''(1) IN GENERAL.—Not later than 7 days after the date on which an agency has a reasonable basis to conclude that a major incident occurred, the head of the agency, jointly with the National Cyber Director and any other Federal entity determined appropriate by the National Cyber Director, shall provide a briefing to the congressional committees described in subsection (a)(1) on the threat causing the major incident.

''(2) COMPONENTS.—The briefing required under paragraph (1)—

''(A) shall, to the greatest extent practicable, include an unclassified component; and

''(B) may include a classified component.

''(h) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to limit—

''(1) the ability of an agency to provide additional reports or briefings to Congress; or

''(2) Congress from requesting additional information from agencies through reports, briefings, or other means.

''§ 3594. Government information sharing and incident response

''(a) IN GENERAL.—

''(1) INCIDENT REPORTING.—The head of each agency shall provide any information relating to any incident, whether the information is obtained by the Federal Government directly or indirectly, to the Cybersecurity and Infrastructure Security Agency and the Office of Management and Budget.

''(2) CONTENTS.—A provision of information relating to an incident made by the head of an agency under paragraph (1) shall—

''(A) include detailed information about the safeguards that were in place when the incident occurred;

''(B) whether the agency implemented the safeguards described in subparagraph (A) correctly;

''(C) in order to protect against a similar incident, identify—

''(i) how the safeguards described in subparagraph (A) should be implemented differently; and

''(ii) additional necessary safeguards; and

''(D) include information to aid in incident response, such as—

''(i) a description of the affected systems or networks;

''(ii) the estimated dates of when the incident occurred; and

''(iii) information that could reasonably help identify the party that conducted the incident.

''(3) INFORMATION SHARING.—To the greatest extent practicable, the Director of the Cybersecurity and Infrastructure Security Agency shall share information relating to an incident with any agencies that may be impacted by the incident.

''(4) NATIONAL SECURITY SYSTEMS.—Each agency operating or exercising control of a national security system shall share information about incidents that occur on national security systems with the Director of the Cybersecurity and Infrastructure Security Agency to the extent consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President.

''(b) COMPLIANCE.—The information provided under subsection (a) shall take into account the level of classification of the information and any information sharing limitations and protections, such as limitations and protections relating to law enforcement, national security, privacy, statistical confidentiality, or other factors determined by the Director

''(c) INCIDENT RESPONSE.—Each agency that has a reasonable basis to conclude that a major incident occurred involving Federal information in electronic medium or form, as defined by the Director and not involving a national security system, regardless of delays from notification granted for a major incident, shall coordinate with the Cybersecurity and Infrastructure Security Agency regarding—

''(1) incident response and recovery; and

''(2) recommendations for mitigating future incidents.

''§ 3595. Responsibilities of contractors and awardees

''(a) NOTIFICATION.—

''(1) IN GENERAL.—Unless otherwise specified in a contract, grant, cooperative agreement, or an other transaction agreement, any contractor or awardee of an agency shall report to the agency within the same amount of time such agency is required to report an incident to the Cybersecurity and Infrastructure Security Agency, if the contractor or awardee has a reasonable basis to conclude that—

''(A) an incident or breach has occurred with respect to Federal information collected, used, or maintained by the contractor or awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee;

''(B) an incident or breach has occurred with respect to a Federal information system used or operated by the contractor or awardee in connection with the contract, grant, cooperative agreement, or other transaction agreement of the contractor or awardee; or

''(C) the contractor or awardee has received information from the agency that the contractor or awardee is not authorized to receive in connection with the contract,

grant, cooperative agreement, or other transaction agreement of the contractor or awardee.

''(2) PROCEDURES.—

''(A) MAJOR INCIDENT.—Following a report of a breach or major incident by a contractor or awardee under paragraph (1), the agency, in consultation with the contractor or awardee, shall carry out the requirements under sections 3592, 3593, and 3594 with respect to the major incident.

''(B) INCIDENT.—Following a report of an incident by a contractor or awardee under paragraph (1), an agency, in consultation with the contractor or awardee, shall carry out the requirements under section 3594 with respect to the incident.

''(b) EFFECTIVE DATE.—This section shall apply on and after the date that is 1 year after the date of enactment of the Federal Information Security Modernization Act of 2021.

''§ 3596. Training

''(a) COVERED INDIVIDUAL DEFINED.—In this section, the term 'covered individual' means an individual who obtains access to Federal information or Federal information systems because of the status of the individual as an employee, contractor, awardee, volunteer, or intern of an agency.

''(b) REQUIREMENT.—The head of each agency shall develop training for covered individuals on how to identify and respond to an incident, including—

''(1) the internal process of the agency for reporting an incident; and

''(2) the obligation of a covered individual to report to the agency a confirmed major incident and any suspected incident involving information in any medium or form, including paper, oral, and electronic.

''(c) INCLUSION IN ANNUAL TRAINING.—The training developed under subsection (b) may be included as part of an annual privacy or security awareness training of an agency.

''§ 3597. Analysis and report on Federal incidents

''(a) ANALYSIS OF FEDERAL INCIDENTS.—

''(1) QUANTITATIVE AND QUALITATIVE ANALYSES.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop, in consultation with the Director and the National Cyber Director, and perform continuous monitoring and quantitative and qualitative analyses of incidents at agencies, including major incidents, including—

''(A) the causes of incidents, including—

''(i) attacker tactics, techniques, and procedures; and

''(ii) system vulnerabilities, including zero days, unpatched systems, and information system misconfigurations;

''(B) the scope and scale of incidents at agencies;

''(C) cross Federal Government root causes of incidents at agencies;

''(D) agency incident response, recovery, and remediation actions and the effectiveness of those actions, as applicable;

''(E) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

''(F) trends in cross-Federal Government cybersecurity and incident response capabilities using the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

''(2) AUTOMATED ANALYSIS.—The analyses developed under paragraph (1) shall, to the greatest extent practicable, use machine readable data, automation, and machine learning processes.

''(3) SHARING OF DATA AND ANALYSIS.—

''(A) IN GENERAL.—The Director shall share on an ongoing basis the analyses required under this subsection with agencies and the National Cyber Director to—

''(i) improve the understanding of cybersecurity risk of agencies; and

''(ii) support the cybersecurity improvement efforts of agencies.

''(B) FORMAT.—In carrying out subparagraph (A), the Director shall share the analyses—

''(i) in human-readable written products; and

''(ii) to the greatest extent practicable, in machine-readable formats in order to enable automated intake and use by agencies.

''(b) ANNUAL REPORT ON FEDERAL INCIDENTS.—Not later than 2 years after the date of enactment of this section, and not less frequently than annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director and other Federal agencies as appropriate, shall submit to the appropriate notification entities a report that includes—

''(1) a summary of causes of incidents from across the Federal Government that categorizes those incidents as incidents or major incidents;

''(2) the quantitative and qualitative analyses of incidents developed under subsection (a)(1) on an agency-by-agency basis and comprehensively across the Federal Government, including—

''(A) a specific analysis of breaches; and

''(B) an analysis of the Federal Government's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)); and

''(3) an annex for each agency that includes—

''(A) a description of each major incident;

''(B) the total number of compromises of the agency; and

''(C) an analysis of the agency's performance against the metrics established under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

''(c) PUBLICATION.—A version of each report submitted under subsection (b) shall be made publicly available on the website of the Cybersecurity and Infrastructure Security Agency during the year in which the report is submitted.

''(d) INFORMATION PROVIDED BY AGENCIES.—

''(1) IN GENERAL.—The analysis required under subsection (a) and each report submitted under subsection (b) shall use information provided by agencies under section 3594(a).

''(2) NONCOMPLIANCE REPORTS.—

''(A) IN GENERAL.—Subject to subparagraph (B), during any year during which the head of an agency does not provide data for an incident to the Cybersecurity and Infrastructure Security Agency in accordance with section 3594(a), the head of the agency, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Director, shall submit to the appropriate reporting entities a report that includes—

''(i) data for the incident; and

''(ii) the information described in subsection (b) with respect to the agency.

''(B) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The head of an agency that owns or exercises control of a national security system shall not include data for an incident that occurs on a national security system in any report submitted under subparagraph (A).

''(3) NATIONAL SECURITY SYSTEM REPORTS.—

''(A) IN GENERAL.—Annually, the head of an agency that operates or exercises control of a national security system shall submit a report that includes the information described in subsection (b) with respect to the agency to the extent that the submission is consistent with standards and guidelines for national security systems issued in accordance with law and as directed by the President to—

''(i) the majority and minority leaders of the Senate,

''(ii) the Speaker and minority leader of the House of Representatives;

''(iii) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(iv) the Select Committee on Intelligence of the Senate;

''(v) the Committee on Armed Services of the Senate;

''(vi) the Committee on Appropriations of the Senate;

''(vii) the Committee on Oversight and Reform of the House of Representatives;

''(viii) the Committee on Homeland Security of the House of Representatives;

''(ix) the Permanent Select Committee on Intelligence of the House of Representatives;

''(x) the Committee on Armed Services of the House of Representatives; and

''(xi) the Committee on Appropriations of the House of Representatives.

''(B) CLASSIFIED FORM.—A report required under subparagraph (A) may be submitted in a classified form.

''(e) REQUIREMENT FOR COMPILING INFORMATION.—In publishing the public report required under subsection (c), the Director of the Cybersecurity and Infrastructure Security Agency shall sufficiently compile information such that no specific incident of an agency can be identified, except with the concurrence of the Director of the Office of Management and Budget and in consultation with the impacted agency.

''§ 3598. Major incident definition

''(a) IN GENERAL.—Not later than 180 days after the date of enactment of the Federal Information Security Modernization Act of 2021, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, shall develop and promulgate guidance on the definition of the term 'major incident' for the purposes of subchapter II and this subchapter.

''(b) REQUIREMENTS.—With respect to the guidance issued under subsection (a), the definition of the term 'major incident' shall—

''(1) include, with respect to any information collected or maintained by or on behalf of an agency or an information system used or operated by an agency or by a contractor of an agency or another organization on behalf of an agency—

''(A) any incident the head of the agency determines is likely to have an impact on—

''(i) the national security, homeland security, or economic security of the United States; or

''(ii) the civil liberties or public health and safety of the people of the United States;

''(B) any incident the head of the agency determines likely to result in an inability for the agency, a component of the agency, or the Federal Government, to provide 1 or more critical services;

''(C) any incident that the head of an agency, in consultation with a senior privacy officer of the agency, determines is likely to have a significant privacy impact on 1 or more individual;

''(D) any incident that the head of the agency, in consultation with a senior privacy official of the agency, determines is likely to have a substantial privacy impact on a significant number of individuals;

''(E) any incident the head of the agency determines impacts the operations of a high value asset owned or operated by the agency;

''(F) any incident involving the exposure of sensitive agency information to a foreign entity, such as the communications of the head of the agency, the head of a component of the agency, or the direct reports of the head

of the agency or the head of a component of the agency; and

''(G) any other type of incident determined appropriate by the Director;

''(2) stipulate that the National Cyber Director shall declare a major incident at each agency impacted by an incident if the Director of the Cybersecurity and Infrastructure Security Agency determines that an incident—

''(A) occurs at not less than 2 agencies; and

''(B) is enabled by—

''(i) a common technical root cause, such as a supply chain compromise, a common software or hardware vulnerability; or

''(ii) the related activities of a common threat actor; and

''(3) stipulate that, in determining whether an incident constitutes a major incident because that incident—

''(A) is any incident described in paragraph (1), the head of an agency shall consult with the Director of the Cybersecurity and Infrastructure Security Agency;

''(B) is an incident described in paragraph (1)(A), the head of the agency shall consult with the National Cyber Director; and

''(C) is an incident described in subparagraph (C) or (D) of paragraph (1), the head of the agency shall consult with—

''(i) the Privacy and Civil Liberties Oversight Board; and

''(ii) the Chair of the Federal Trade Commission.

''(c) SIGNIFICANT NUMBER OF INDIVIDUALS.—In determining what constitutes a significant number of individuals under subsection (b)(1)(D), the Director—

''(1) may determine a threshold for a minimum number of individuals that constitutes a significant amount; and

''(2) may not determine a threshold described in paragraph (1) that exceeds 5,000 individuals.

''(d) EVALUATION AND UPDATES.—Not later than 2 years after the date of enactment of the Federal Information Security Modernization Act of 2021, and not less frequently than every 2 years thereafter, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives an evaluation, which shall include—

''(1) an update, if necessary, to the guidance issued under subsection (a);

''(2) the definition of the term 'major incident' included in the guidance issued under subsection (a); and

''(3) an explanation of, and the analysis that led to, the definition described in paragraph (2).''.

(2) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''SUBCHAPTER IV—FEDERAL SYSTEM INCIDENT RESPONSE

''3591. Definitions.
''3592. Notification of breach.
''3593. Congressional and Executive Branch reports.
''3594. Government information sharing and incident response.
''3595. Responsibilities of contractors and awardees.
''3596. Training.
''3597. Analysis and report on Federal incidents.
''3598. Major incident definition.''.

SEC. 5122. AMENDMENTS TO SUBTITLE III OF TITLE 40.

(a) MODERNIZING GOVERNMENT TECHNOLOGY.—Subtitle G of title X of Division A of the National Defense Authorization Act for Fiscal Year 2018 (40 U.S.C. 11301 note) is amended—

(1) in section 1077(b)—

(A) in paragraph (5)(A), by inserting ''improving the cybersecurity of systems and'' before ''cost savings activities''; and

(B) in paragraph (7)—

(i) in the paragraph heading, by striking ''CIO'' and inserting ''CIO'';

(ii) by striking ''In evaluating projects'' and inserting the following:

''(A) CONSIDERATION OF GUIDANCE.—In evaluating projects'';

(iii) in subparagraph (A), as so designated, by striking ''under section 1094(b)(1)'' and inserting ''by the Director''; and

(iv) by adding at the end the following:

''(B) CONSULTATION.—In using funds under paragraph (3)(A), the Chief Information Officer of the covered agency shall consult with the necessary stakeholders to ensure the project appropriately addresses cybersecurity risks, including the Director of the Cybersecurity and Infrastructure Security Agency, as appropriate.''; and

(2) in section 1078—

(A) by striking subsection (a) and inserting the following:

''(a) DEFINITIONS.—In this section:

''(1) AGENCY.—The term 'agency' has the meaning given the term in section 551 of title 5, United States Code.

''(2) HIGH VALUE ASSET.—The term 'high value asset' has the meaning given the term in section 3552 of title 44, United States Code.'';

(B) in subsection (b), by adding at the end the following:

''(8) PROPOSAL EVALUATION.—The Director shall—

''(A) give consideration for the use of amounts in the Fund to improve the security of high value assets; and

''(B) require that any proposal for the use of amounts in the Fund includes a cybersecurity plan, including a supply chain risk management plan, to be reviewed by the member of the Technology Modernization Board described in subsection (c)(5)(C).''; and

(C) in subsection (c)—

(i) in paragraph (2)(A)(i), by inserting '', including a consideration of the impact on high value assets'' after ''operational risks'';

(ii) in paragraph (5)—

(I) in subparagraph (A), by striking ''and'' at the end;

(II) in subparagraph (B), by striking the period at the end and inserting ''and''; and

(III) by adding at the end the following:

''(C) a senior official from the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, appointed by the Director.''; and

(iii) in paragraph (6)(A), by striking ''shall be—'' and all that follows through ''4 employees'' and inserting ''shall be 4 employees''.

(b) SUBCHAPTER I.—Subchapter I of subtitle III of title 40, United States Code, is amended—

(1) in section 11302—

(A) in subsection (b), by striking ''use, security, and disposal of'' and inserting ''use, and disposal of, and, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, promote and improve the security of,'';

(B) in subsection (c)—

(i) in paragraph (3)—

(I) in subparagraph (A)—

(aa) by striking ''including data'' and inserting ''which shall—

''(i) include data'';

(bb) in clause (i), as so designated, by striking '', and performance'' and inserting ''security, and performance; and''; and

(cc) by adding at the end the following:

''(ii) specifically denote cybersecurity funding under the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44.''; and

(II) in subparagraph (B), adding at the end the following:

''(iii) The Director shall provide to the National Cyber Director any cybersecurity funding information described in subparagraph (A)(ii) that is provided to the Director under clause (ii) of this subparagraph.''; and

(ii) in paragraph (4)(B), in the matter preceding clause (i), by inserting ''not later than 30 days after the date on which the review under subparagraph (A) is completed,'' before ''the Administrator'';

(C) in subsection (f)—

(i) by striking ''heads of executive agencies to develop'' and inserting ''heads of executive agencies to—

''(1) develop'';

(ii) in paragraph (1), as so designated, by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following:

''(2) consult with the Director of the Cybersecurity and Infrastructure Security Agency for the development and use of supply chain security best practices.''; and

(D) in subsection (h), by inserting '', including cybersecurity performances,'' after ''the performances''; and

(2) in section 11303(b)—

(A) in paragraph (2)(B)—

(i) in clause (i), by striking ''or'' at the end;

(ii) in clause (ii), by adding ''or'' at the end; and

(iii) by adding at the end the following:

''(iii) whether the function should be performed by a shared service offered by another executive agency;''; and

(B) in paragraph (5)(B)(i), by inserting '', while taking into account the risk-based cyber budget model developed pursuant to section 3553(a)(7) of title 44'' after ''title 31''.

(c) SUBCHAPTER II.—Subchapter II of subtitle III of title 40, United States Code, is amended—

(1) in section 11312(a), by inserting '', including security risks'' after ''managing the risks'';

(2) in section 11313(1), by striking ''efficiency and effectiveness'' and inserting ''efficiency, security, and effectiveness'';

(3) in section 11315, by adding at the end the following:

''(d) COMPONENT AGENCY CHIEF INFORMATION OFFICERS.—The Chief Information Officer or an equivalent official of a component agency shall report to—

''(1) the Chief Information Officer designated under section 3506(a)(2) of title 44 or an equivalent official of the agency of which the component agency is a component; and

''(2) the head of the component agency.'';

(4) in section 11317, by inserting ''security,'' before ''or schedule''; and

(5) in section 11319(b)(1), in the paragraph heading, by striking ''CIOS'' and inserting ''CHIEF INFORMATION OFFICERS''.

(d) SUBCHAPTER III.—Section 11331 of title 40, United States Code, is amended—

(1) in subsection (a), by striking ''section 3532(b)(1)'' and inserting ''section 3552(b)'';

(2) in subsection (b)(1)(A), by striking ''the Secretary of Homeland Security'' and inserting ''the Director of the Cybersecurity and Infrastructure Security Agency'';

(3) by striking subsection (c) and inserting the following:

''(c) APPLICATION OF MORE STRINGENT STANDARDS.—

''(1) IN GENERAL.—The head of an agency shall—

''(A) evaluate, in consultation with the senior agency information security officers, the need to employ standards for cost-effective, risk-based information security for all systems, operations, and assets within or

under the supervision of the agency that are more stringent than the standards promulgated by the Director under this section, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

''(B) to the greatest extent practicable and if the head of the agency determines that the standards described in subparagraph (A) are necessary, employ those standards.

''(2) EVALUATION OF MORE STRINGENT STANDARDS.—In evaluating the need to employ more stringent standards under paragraph (1), the head of an agency shall consider available risk information, such as—

''(A) the status of cybersecurity remedial actions of the agency;

''(B) any vulnerability information relating to agency systems that is known to the agency;

''(C) incident information of the agency;

''(D) information from—

''(i) penetration testing performed under section 3559A of title 44; and

''(ii) information from the vulnerability disclosure program established under section 3559B of title 44;

''(E) agency threat hunting results under section 5145 of the Federal Information Security Modernization Act of 2021;

''(F) Federal and non-Federal cyber threat intelligence;

''(G) data on compliance with standards issued under this section;

''(H) agency system risk assessments performed under section 3554(a)(1)(A) of title 44; and

''(I) any other information determined relevant by the head of the agency.'';

(4) in subsection (d)(2)—

(A) in the paragraph heading, by striking ''NOTICE AND COMMENT'' and inserting ''CONSULTATION, NOTICE, AND COMMENT'';

(B) by inserting ''promulgate,'' before ''significantly modify''; and

(C) by striking ''shall be made after the public is given an opportunity to comment on the Director's proposed decision.'' and inserting ''shall be made—

''(A) for a decision to significantly modify or not promulgate such a proposed standard, after the public is given an opportunity to comment on the Director's proposed decision;

''(B) in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency;

''(C) considering the Federal risk assessments performed under section 3553(i) of title 44; and

''(D) considering the extent to which the proposed standard reduces risk relative to the cost of implementation of the standard.''; and

(5) by adding at the end the following:

''(e) REVIEW OF OFFICE OF MANAGEMENT AND BUDGET GUIDANCE AND POLICY.—

''(1) CONDUCT OF REVIEW.—

''(A) IN GENERAL.—Not less frequently than once every 3 years, the Director of the Office of Management and Budget, in consultation with the Chief Information Officers Council, the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, the Comptroller General of the United States, and the Council of the Inspectors General on Integrity and Efficiency shall review the efficacy of the guidance and policy promulgated by the Director in reducing cybersecurity risks, including an assessment of the requirements for agencies to report information to the Director, and determine whether any changes to that guidance or policy is appropriate.

''(B) FEDERAL RISK ASSESSMENTS.—In conducting the review described in subparagraph (A), the Director shall consider the Federal risk assessments performed under section 3553(i) of title 44.

''(2) UPDATED GUIDANCE.—Not later than 90 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall issue updated guidance or policy to agencies determined appropriate by the Director, based on the results of the review.

''(3) PUBLIC REPORT.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director of the Office of Management and Budget shall make publicly available a report that includes—

''(A) an overview of the guidance and policy promulgated under this section that is currently in effect;

''(B) the cybersecurity risk mitigation, or other cybersecurity benefit, offered by each guidance or policy document described in subparagraph (A); and

''(C) a summary of the guidance or policy to which changes were determined appropriate during the review and what the changes are anticipated to include.

''(4) CONGRESSIONAL BRIEFING.—Not later than 30 days after the date on which a review is completed under paragraph (1), the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the review.

''(f) AUTOMATED STANDARD IMPLEMENTATION VERIFICATION.—When the Director of the National Institute of Standards and Technology issues a proposed standard pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), the Director of the National Institute of Standards and Technology shall consider developing and, if appropriate and practical, develop, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, specifications to enable the automated verification of the implementation of the controls within the standard.''.

SEC. 5123. ACTIONS TO ENHANCE FEDERAL INCIDENT RESPONSE.

(a) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall—

(A) develop a plan for the development of the analysis required under section 3597(a) of title 44, United States Code, as added by this division, and the report required under subsection (b) of that section that includes—

(i) a description of any challenges the Director anticipates encountering; and

(ii) the use of automation and machine-readable formats for collecting, compiling, monitoring, and analyzing data; and

(B) provide to the appropriate congressional committees a briefing on the plan developed under subparagraph (A).

(2) BRIEFING.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the appropriate congressional committees a briefing on—

(A) the execution of the plan required under paragraph (1)(A); and

(B) the development of the report required under section 3597(b) of title 44, United States Code, as added by this division.

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET.—

(1) FISMA.—Section 2 of the Federal Information Security Modernization Act of 2014 (44 U.S.C. 3554 note) is amended—

(A) by striking subsection (b); and

(B) by redesignating subsections (c) through (f) as subsections (b) through (e), respectively.

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director shall develop guidance, to be updated not less frequently than once every 2 years, on the content, timeliness, and format of the information provided by agencies under section 3594(a) of title 44, United States Code, as added by this division.

(B) REQUIREMENTS.—The guidance developed under subparagraph (A) shall—

(i) prioritize the availability of data necessary to understand and analyze—

(I) the causes of incidents;

(II) the scope and scale of incidents within the environments and systems of an agency;

(III) a root cause analysis of incidents that—

(aa) are common across the Federal Government; or

(bb) have a Government-wide impact;

(IV) agency response, recovery, and remediation actions and the effectiveness of those actions; and

(V) the impact of incidents;

(ii) enable the efficient development of—

(I) lessons learned and recommendations in responding to, recovering from, remediating, and mitigating future incidents; and

(II) the report on Federal incidents required under section 3597(b) of title 44, United States Code, as added by this division;

(iii) include requirements for the timeliness of data production; and

(iv) include requirements for using automation and machine-readable data for data sharing and availability.

(3) GUIDANCE ON RESPONDING TO INFORMATION REQUESTS.—Not later than 1 year after the date of enactment of this Act, the Director shall develop guidance for agencies to implement the requirement under section 3594(c) of title 44, United States Code, as added by this division, to provide information to other agencies experiencing incidents.

(4) STANDARD GUIDANCE AND TEMPLATES.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this division.

(5) CONTRACTOR AND AWARDEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to Federal agencies on how to deconflict, to the greatest extent practicable, existing regulations, policies, and procedures relating to the responsibilities of contractors and awardees established under section 3595 of title 44, United States Code, as added by this division.

(B) EXISTING PROCESSES.—To the greatest extent practicable, the guidance issued under subparagraph (A) shall allow contractors and awardees to use existing processes for notifying Federal agencies of incidents involving information of the Federal Government.

(6) UPDATED BRIEFINGS.—Not less frequently than once every 2 years, the Director shall provide to the appropriate congressional committees an update on the guidance and templates developed under paragraphs (2) through (4).

(c) UPDATE TO THE PRIVACY ACT OF 1974.—Section 552a(b) of title 5, United States Code (commonly known as the ''Privacy Act of 1974'') is amended—

(1) in paragraph (11), by striking ''or'' at the end;

(2) in paragraph (12), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following:

''(13) to another agency in furtherance of a response to an incident (as defined in section 3552 of title 44) and pursuant to the information sharing requirements in section 3594 of title 44 if the head of the requesting agency has made a written request to the agency that maintains the record specifying the particular portion desired and the activity for which the record is sought.''.

SEC. 5124. ADDITIONAL GUIDANCE TO AGENCIES ON FISMA UPDATES.

Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance for agencies on—

(1) performing the ongoing and continuous agency system risk assessment required under section 3554(a)(1)(A) of title 44, United States Code, as amended by this division;

(2) implementing additional cybersecurity procedures, which shall include resources for shared services;

(3) establishing a process for providing the status of each remedial action under section 3554(b)(7) of title 44, United States Code, as amended by this division, to the Director and the Cybersecurity and Infrastructure Security Agency using automation and machine-readable data, as practicable, which shall include—

(A) specific guidance for the use of automation and machine-readable data; and

(B) templates for providing the status of the remedial action;

(4) interpreting the definition of ''high value asset'' under section 3552 of title 44, United States Code, as amended by this division; and

(5) a requirement to coordinate with inspectors general of agencies to ensure consistent understanding and application of agency policies for the purpose of evaluations by inspectors general.

SEC. 5125. AGENCY REQUIREMENTS TO NOTIFY PRIVATE SECTOR ENTITIES IMPACTED BY INCIDENTS.

(a) DEFINITIONS.—In this section:

(1) REPORTING ENTITY.—The term ''reporting entity'' means private organization or governmental unit that is required by statute or regulation to submit sensitive information to an agency.

(2) SENSITIVE INFORMATION.—The term ''sensitive information'' has the meaning given the term by the Director in guidance issued under subsection (b).

(b) GUIDANCE ON NOTIFICATION OF REPORTING ENTITIES.—Not later than 180 days after the date of enactment of this Act, the Director shall issue guidance requiring the head of each agency to notify a reporting entity of an incident that is likely to substantially affect—

(1) the confidentiality or integrity of sensitive information submitted by the reporting entity to the agency pursuant to a statutory or regulatory requirement; or

(2) the agency information system or systems used in the transmission or storage of the sensitive information described in paragraph (1).

TITLE LII—IMPROVING FEDERAL CYBERSECURITY

SEC. 5141. MOBILE SECURITY STANDARDS.

(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director shall—

(1) evaluate mobile application security guidance promulgated by the Director; and

(2) issue guidance to secure mobile devices, including for mobile applications, for every agency.

(b) CONTENTS.—The guidance issued under subsection (a)(2) shall include—

(1) a requirement, pursuant to section 3506(b)(4) of title 44, United States Code, for every agency to maintain a continuous inventory of every—

(A) mobile device operated by or on behalf of the agency; and

(B) vulnerability identified by the agency associated with a mobile device; and

(2) a requirement for every agency to perform continuous evaluation of the vulnerabilities described in paragraph (1)(B) and other risks associated with the use of applications on mobile devices.

(c) INFORMATION SHARING.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to agencies for sharing the inventory of the agency required under subsection (b)(1) with the Director of the Cybersecurity and Infrastructure Security Agency, using automation and machine-readable data to the greatest extent practicable.

(d) BRIEFING.—Not later than 60 days after the date on which the Director issues guidance under subsection (a)(2), the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall provide to the appropriate congressional committees a briefing on the guidance.

SEC. 5142. DATA AND LOGGING RETENTION FOR INCIDENT RESPONSE.

(a) RECOMMENDATIONS.—Not later than 2 years after the date of enactment of this Act, and not less frequently than every 2 years thereafter, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Attorney General, shall submit to the Director recommendations on requirements for logging events on agency systems and retaining other relevant data within the systems and networks of an agency.

(b) CONTENTS.—The recommendations provided under subsection (a) shall include—

(1) the types of logs to be maintained;

(2) the time periods to retain the logs and other relevant data;

(3) the time periods for agencies to enable recommended logging and security requirements;

(4) how to ensure the confidentiality, integrity, and availability of logs;

(5) requirements to ensure that, upon request, in a manner that excludes or otherwise reasonably protects personally identifiable information, and to the extent permitted by applicable law (including privacy and statistical laws), agencies provide logs to—

(A) the Director of the Cybersecurity and Infrastructure Security Agency for a cybersecurity purpose; and

(B) the Federal Bureau of Investigation to investigate potential criminal activity; and

(6) requirements to ensure that, subject to compliance with statistical laws and other relevant data protection requirements, the highest level security operations center of each agency has visibility into all agency logs.

(c) GUIDANCE.—Not later than 90 days after receiving the recommendations submitted under subsection (a), the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall, as determined to be appropriate by the Director, update guidance to agencies regarding requirements for logging, log retention, log management, sharing of log data with other appropriate agencies, or any other logging activity determined to be appropriate by the Director.

SEC. 5143. CISA AGENCY ADVISORS.

(a) IN GENERAL.—Not later than 120 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall assign not less than 1 cybersecurity professional employed by the Cybersecurity and Infrastructure Security Agency to be the Cybersecurity and Infrastructure Security Agency advisor to the senior agency information security officer of each agency.

(b) QUALIFICATIONS.—Each advisor assigned under subsection (a) shall have knowledge of—

(1) cybersecurity threats facing agencies, including any specific threats to the assigned agency;

(2) performing risk assessments of agency systems; and

(3) other Federal cybersecurity initiatives.

(c) DUTIES.—The duties of each advisor assigned under subsection (a) shall include—

(1) providing ongoing assistance and advice, as requested, to the agency Chief Information Officer;

(2) serving as an incident response point of contact between the assigned agency and the Cybersecurity and Infrastructure Security Agency; and

(3) familiarizing themselves with agency systems, processes, and procedures to better facilitate support to the agency in responding to incidents.

(d) LIMITATION.—An advisor assigned under subsection (a) shall not be a contractor.

(e) MULTIPLE ASSIGNMENTS.—One individual advisor may be assigned to multiple agency Chief Information Officers under subsection (a).

SEC. 5144. FEDERAL PENETRATION TESTING POLICY.

(a) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended by adding at the end the following:

''§ 3559A. Federal penetration testing

''(a) DEFINITIONS.—In this section:

''(1) AGENCY OPERATIONAL PLAN.—The term 'agency operational plan' means a plan of an agency for the use of penetration testing.

''(2) RULES OF ENGAGEMENT.—The term 'rules of engagement' means a set of rules established by an agency for the use of penetration testing.

''(b) GUIDANCE.—

''(1) IN GENERAL.—The Director shall issue guidance that—

''(A) requires agencies to use, when and where appropriate, penetration testing on agency systems; and

''(B) requires agencies to develop an agency operational plan and rules of engagement that meet the requirements under subsection (c).

''(2) PENETRATION TESTING GUIDANCE.—The guidance issued under this section shall—

''(A) permit an agency to use, for the purpose of performing penetration testing—

''(i) a shared service of the agency or another agency; or

''(ii) an external entity, such as a vendor; and

''(B) require agencies to provide the rules of engagement and results of penetration testing to the Director and the Director of the Cybersecurity and Infrastructure Security Agency, without regard to the status of the entity that performs the penetration testing.

''(c) AGENCY PLANS AND RULES OF ENGAGEMENT.—The agency operational plan and rules of engagement of an agency shall—

''(1) require the agency to—

''(A) perform penetration testing on the high value assets of the agency; or

''(B) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency to ensure that penetration testing is being performed;

''(2) establish guidelines for avoiding, as a result of penetration testing—

''(A) adverse impacts to the operations of the agency;

''(B) adverse impacts to operational environments and systems of the agency; and

''(C) inappropriate access to data;

''(3) require the results of penetration testing to include feedback to improve the cybersecurity of the agency; and

''(4) include mechanisms for providing consistently formatted, and, if applicable, automated and machine-readable, data to the Director and the Director of the Cybersecurity and Infrastructure Security Agency.

''(d) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

''(1) establish a process to assess the performance of penetration testing by both Federal and non-Federal entities that establishes minimum quality controls for penetration testing;

''(2) develop operational guidance for instituting penetration testing programs at agencies;

''(3) develop and maintain a centralized capability to offer penetration testing as a service to Federal and non-Federal entities; and

''(4) provide guidance to agencies on the best use of penetration testing resources.

''(e) RESPONSIBILITIES OF OMB.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

''(1) not less frequently than annually, inventory all Federal penetration testing assets; and

''(2) develop and maintain a standardized process for the use of penetration testing.

''(f) PRIORITIZATION OF PENETRATION TESTING RESOURCES.—

''(1) IN GENERAL.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop a framework for prioritizing Federal penetration testing resources among agencies.

''(2) CONSIDERATIONS.—In developing the framework under this subsection, the Director shall consider—

''(A) agency system risk assessments performed under section 3554(a)(1)(A);

''(B) the Federal risk assessment performed under section 3553(i);

''(C) the analysis of Federal incident data performed under section 3597; and

''(D) any other information determined appropriate by the Director or the Director of the Cybersecurity and Infrastructure Security Agency.

''(g) EXCEPTION FOR NATIONAL SECURITY SYSTEMS.—The guidance issued under subsection (b) shall not apply to national security systems.

''(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director described in subsection (b) shall be delegated—

''(1) to the Secretary of Defense in the case of systems described in section 3553(e)(2); and

''(2) to the Director of National Intelligence in the case of systems described in 3553(e)(3).''.

(b) DEADLINE FOR GUIDANCE.—Not later than 180 days after the date of enactment of this Act, the Director shall issue the guidance required under section 3559A(b) of title 44, United States Code, as added by subsection (a).

(c) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559 the following:

''3559A. Federal penetration testing.''.

(d) PENETRATION TESTING BY THE SECRETARY OF HOMELAND SECURITY.—Section 3553(b) of title 44, United States Code, as amended by section 5121, is further amended—

(1) in paragraph (8)(B), by striking ''and'' at the end;

(2) by redesignating paragraph (9) as paragraph (10); and

(3) by inserting after paragraph (8) the following:

''(9) performing penetration testing with or without advance notice to, or authorization from, agencies, to identify vulnerabilities within Federal information systems; and''.

SEC. 5145. ONGOING THREAT HUNTING PROGRAM.

(a) THREAT HUNTING PROGRAM.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall establish a program to provide ongoing, hypothesis-driven threat-hunting services on the network of each agency.

(2) PLAN.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish the program required under paragraph (1) that describes how the Director of the Cybersecurity and Infrastructure Security Agency plans to—

(A) determine the method for collecting, storing, accessing, and analyzing appropriate agency data;

(B) provide on-premises support to agencies;

(C) staff threat hunting services;

(D) allocate available human and financial resources to implement the plan; and

(E) provide input to the heads of agencies on the use of—

(i) more stringent standards under section 11331(c)(1) of title 40, United States Code; and

(ii) additional cybersecurity procedures under section 3554 of title 44, United States Code.

(b) REPORTS.—The Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees—

(1) not later than 30 days after the date on which the Director of the Cybersecurity and Infrastructure Security Agency completes the plan required under subsection (a)(2), a report on the plan to provide threat hunting services to agencies;

(2) not less than 30 days before the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services under the program under subsection (a)(1), a report providing any updates to the plan developed under subsection (a)(2); and

(3) not later than 1 year after the date on which the Director of the Cybersecurity and Infrastructure Security Agency begins providing threat hunting services to agencies other than the Cybersecurity and Infrastructure Security Agency, a report describing lessons learned from providing those services.

SEC. 5146. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by inserting after section 3559A, as added by section 5144 of this division, the following:

''§ 3559B. Federal vulnerability disclosure programs

''(a) DEFINITIONS.—In this section:

''(1) REPORT.—The term 'report' means a vulnerability disclosure made to an agency by a reporter.

''(2) REPORTER.—The term 'reporter' means an individual that submits a vulnerability report pursuant to the vulnerability disclosure process of an agency.

''(b) RESPONSIBILITIES OF OMB.—

''(1) LIMITATION ON LEGAL ACTION.—The Director, in consultation with the Attorney General, shall issue guidance to agencies to not recommend or pursue legal action against a reporter or an individual that conducts a security research activity that the head of the agency determines—

''(A) represents a good faith effort to follow the vulnerability disclosure policy of the agency developed under subsection (d)(2); and

''(B) is authorized under the vulnerability disclosure policy of the agency developed under subsection (d)(2).

''(2) SHARING INFORMATION WITH CISA.—The Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with the National Cyber Director, shall issue guidance to agencies on sharing relevant information in a consistent, automated, and machine readable manner with the Cybersecurity and Infrastructure Security Agency, including—

''(A) any valid or credible reports of newly discovered or not publicly known vulnerabilities (including misconfigurations) on Federal information systems that use commercial software or services;

''(B) information relating to vulnerability disclosure, coordination, or remediation activities of an agency, particularly as those activities relate to outside organizations—

''(i) with which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency can assist; or

''(ii) about which the head of the agency believes the Director of the Cybersecurity and Infrastructure Security Agency should know; and

''(C) any other information with respect to which the head of the agency determines helpful or necessary to involve the Cybersecurity and Infrastructure Security Agency.

''(3) AGENCY VULNERABILITY DISCLOSURE POLICIES.—The Director shall issue guidance to agencies on the required minimum scope of agency systems covered by the vulnerability disclosure policy of an agency required under subsection (d)(2).

''(c) RESPONSIBILITIES OF CISA.—The Director of the Cybersecurity and Infrastructure Security Agency shall—

''(1) provide support to agencies with respect to the implementation of the requirements of this section;

''(2) develop tools, processes, and other mechanisms determined appropriate to offer agencies capabilities to implement the requirements of this section; and

''(3) upon a request by an agency, assist the agency in the disclosure to vendors of newly identified vulnerabilities in vendor products and services.

''(d) RESPONSIBILITIES OF AGENCIES.—

''(1) PUBLIC INFORMATION.—The head of each agency shall make publicly available, with respect to each internet domain under the control of the agency that is not a national security system—

''(A) an appropriate security contact; and

''(B) the component of the agency that is responsible for the internet accessible services offered at the domain.

''(2) VULNERABILITY DISCLOSURE POLICY.—The head of each agency shall develop and

make publicly available a vulnerability disclosure policy for the agency, which shall—

''(A) describe—

''(i) the scope of the systems of the agency included in the vulnerability disclosure policy;

''(ii) the type of information system testing that is authorized by the agency;

''(iii) the type of information system testing that is not authorized by the agency; and

''(iv) the disclosure policy of the agency for sensitive information;

''(B) with respect to a report to an agency, describe—

''(i) how the reporter should submit the report; and

''(ii) if the report is not anonymous, when the reporter should anticipate an acknowledgment of receipt of the report by the agency;

''(C) include any other relevant information; and

''(D) be mature in scope, to cover all Federal information systems used or operated by that agency or on behalf of that agency.

''(3) IDENTIFIED VULNERABILITIES.—The head of each agency shall incorporate any vulnerabilities reported under paragraph (2) into the vulnerability management process of the agency in order to track and remediate the vulnerability.

''(e) PAPERWORK REDUCTION ACT EXEMPTION.—The requirements of subchapter I (commonly known as the 'Paperwork Reduction Act') shall not apply to a vulnerability disclosure program established under this section.

''(f) CONGRESSIONAL REPORTING.—Not later than 90 days after the date of enactment of the Federal Information Security Modernization Act of 2021, and annually thereafter for a 3-year period, the Director shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives a briefing on the status of the use of vulnerability disclosure policies under this section at agencies, including, with respect to the guidance issued under subsection (b)(3), an identification of the agencies that are compliant and not compliant.

''(g) EXEMPTIONS.—The authorities and functions of the Director and Director of the Cybersecurity and Infrastructure Security Agency under this section shall not apply to national security systems.

''(h) DELEGATION OF AUTHORITY FOR CERTAIN SYSTEMS.—The authorities of the Director and the Director of the Cybersecurity and Infrastructure Security Agency described in this section shall be delegated—

''(1) to the Secretary of Defense in the case of systems described in section 3553(e)(2); and

''(2) to the Director of National Intelligence in the case of systems described in section 3553(e)(3).''.

(b) CLERICAL AMENDMENT.—The table of sections for chapter 35 of title 44, United States Code, is amended by adding after the item relating to section 3559A, as added by section 204, the following:

''3559B. Federal vulnerability disclosure programs.''.

SEC. 5147. IMPLEMENTING PRESUMPTION OF COMPROMISE AND LEAST PRIVILEGE PRINCIPLES.

(a) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Director shall provide an update to the appropriate congressional committees on progress in increasing the internal defenses of agency systems, including—

(1) shifting away from ''trusted networks'' to implement security controls based on a presumption of compromise;

(2) implementing principles of least privilege in administering information security programs;

(3) limiting the ability of entities that cause incidents to move laterally through or between agency systems;

(4) identifying incidents quickly;

(5) isolating and removing unauthorized entities from agency systems quickly;

(6) otherwise increasing the resource costs for entities that cause incidents to be successful; and

(7) a summary of the agency progress reports required under subsection (b).

(b) AGENCY PROGRESS REPORTS.—Not later than 1 year after the date of enactment of this Act, the head of each agency shall submit to the Director a progress report on implementing an information security program based on the presumption of compromise and least privilege principles, which shall include—

(1) a description of any steps the agency has completed, including progress toward achieving requirements issued by the Director;

(2) an identification of activities that have not yet been completed and that would have the most immediate security impact; and

(3) a schedule to implement any planned activities.

SEC. 5148. AUTOMATION REPORTS.

(a) OMB REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit to the appropriate congressional committees a report on the use of automation under paragraphs (1), (5)(C) and (8)(B) of section 3554(b) of title 44, United States Code.

(b) GAO REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall perform a study on the use of automation and machine readable data across the Federal Government for cybersecurity purposes, including the automated updating of cybersecurity tools, sensors, or processes by agencies.

SEC. 5149. EXTENSION OF FEDERAL ACQUISITION SECURITY COUNCIL.

Section 1328 of title 41, United States Code, is amended by striking ''the date that'' and all that follows and inserting ''December 31, 2026.''.

SEC. 5150. COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY DASHBOARD.

(a) DASHBOARD REQUIRED.—Section 11(e)(2) of the Inspector General Act of 1978 (5 U.S.C. App.) is amended—

(1) in subparagraph (A), by striking ''and'' at the end;

(2) by redesignating subparagraph (B) as subparagraph (C); and

(3) by inserting after subparagraph (A) the following:

''(B) that shall include a dashboard of open information security recommendations identified in the independent evaluations required by section 3555(a) of title 44, United States Code; and''.

SEC. 5151. QUANTITATIVE CYBERSECURITY METRICS.

(a) DEFINITION OF COVERED METRICS.—In this section, the term ''covered metrics'' means the metrics established, reviewed, and updated under section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c)).

(b) UPDATING AND ESTABLISHING METRICS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall—

(1) evaluate any covered metrics established as of the date of enactment of this Act; and

(2) as appropriate and pursuant to section 224(c) of the Cybersecurity Act of 2015 (6 U.S.C. 1522(c))—

(A) update the covered metrics; and

(B) establish new covered metrics.

(c) IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 540 days after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall promulgate guidance that requires each agency to use covered metrics to track trends in the cybersecurity and incident response capabilities of the agency.

(2) PERFORMANCE DEMONSTRATION.—The guidance issued under paragraph (1) and any subsequent guidance shall require agencies to share with the Director of the Cybersecurity and Infrastructure Security Agency data demonstrating the performance of the agency using the covered metrics included in the guidance.

(3) PENETRATION TESTS.—On not less than 2 occasions during the 2-year period following the date on which guidance is promulgated under paragraph (1), the Director shall ensure that not less than 3 agencies are subjected to substantially similar penetration tests, as determined by the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, in order to validate the utility of the covered metrics.

(4) ANALYSIS CAPACITY.—The Director of the Cybersecurity and Infrastructure Security Agency shall develop a capability that allows for the analysis of the covered metrics, including cross-agency performance of agency cybersecurity and incident response capability trends.

(d) CONGRESSIONAL REPORTS.—

(1) UTILITY OF METRICS.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees a report on the utility of the covered metrics.

(2) USE OF METRICS.—Not later than 180 days after the date on which the Director promulgates guidance under subsection (c)(1), the Director shall submit to the appropriate congressional committees a report on the results of the use of the covered metrics by agencies.

(e) CYBERSECURITY ACT OF 2015 UPDATES.—Section 224 of the Cybersecurity Act of 2015 (6 U.S.C. 1522) is amended—

(1) by striking subsection (c) and inserting the following:

''(c) IMPROVED METRICS.—

''(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall establish, review, and update metrics to measure the cybersecurity and incident response capabilities of agencies in accordance with the responsibilities of agencies under section 3554 of title 44, United States Code.

''(2) QUALITIES.—With respect to the metrics established, reviewed, and updated under paragraph (1)—

''(A) not less than 2 of the metrics shall be time-based, such as a metric of—

''(i) the amount of time it takes for an agency to detect an incident; and

''(ii) the amount of time that passes between—

''(I) the detection of an incident and the remediation of the incident; and

''(II) the remediation of an incident and the recovery from the incident; and

''(B) the metrics may include other measurable outcomes.'';

(2) by striking subsection (e); and

(3) by redesignating subsection (f) as subsection (e).

TITLE LIII—RISK-BASED BUDGET MODEL

SEC. 5161. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate; and

(B) the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives.

(2) COVERED AGENCY.—The term ''covered agency'' has the meaning given the term ''executive agency'' in section 133 of title 41, United States Code.

(3) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(4) INFORMATION TECHNOLOGY.—The term ''information technology''—

(A) has the meaning given the term in section 11101 of title 40, United States Code; and

(B) includes the hardware and software systems of a Federal agency that monitor and control physical equipment and processes of the Federal agency.

(5) RISK-BASED BUDGET.—The term ''risk-based budget'' means a budget—

(A) developed by identifying and prioritizing cybersecurity risks and vulnerabilities, including impact on agency operations in the case of a cyber attack, through analysis of cyber threat intelligence, incident data, and tactics, techniques, procedures, and capabilities of cyber threats; and

(B) that allocates resources based on the risks identified and prioritized under subparagraph (A).

SEC. 5162. ESTABLISHMENT OF RISK-BASED BUDGET MODEL.

(a) IN GENERAL.—

(1) MODEL.—Not later than 1 year after the first publication of the budget submitted by the President under section 1105 of title 31, United States Code, following the date of enactment of this Act, the Director, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director and in coordination with the Director of the National Institute of Standards and Technology, shall develop a standard model for creating a risk-based budget for cybersecurity spending.

(2) RESPONSIBILITY OF DIRECTOR.—Section 3553(a) of title 44, United States Code, as amended by section 5121 of this division, is further amended by inserting after paragraph (6) the following:

''(7) developing a standard risk-based budget model to inform Federal agency cybersecurity budget development; and''.

(3) CONTENTS OF MODEL.—The model required to be developed under paragraph (1) shall—

(A) consider Federal and non-Federal cyber threat intelligence products, where available, to identify threats, vulnerabilities, and risks;

(B) consider the impact of agency operations of compromise of systems, including the interconnectivity to other agency systems and the operations of other agencies;

(C) indicate where resources should be allocated to have the greatest impact on mitigating current and future threats and current and future cybersecurity capabilities;

(D) be used to inform acquisition and sustainment of—

(i) information technology and cybersecurity tools;

(ii) information technology and cybersecurity architectures;

(iii) information technology and cybersecurity personnel; and

(iv) cybersecurity and information technology concepts of operations; and

(E) be used to evaluate and inform Government-wide cybersecurity programs of the Department of Homeland Security.

(4) REQUIRED UPDATES.—Not less frequently than once every 3 years, the Director shall review, and update as necessary, the model required to be developed under this subsection.

(5) PUBLICATION.—The Director shall publish the model required to be developed under this subsection, and any updates necessary under paragraph (4), on the public website of the Office of Management and Budget.

(6) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for each of the 2 following fiscal years or until the date on which the model required to be developed under this subsection is completed, whichever is sooner, the Director shall submit a report to Congress on the development of the model.

(b) REQUIRED USE OF RISK-BASED BUDGET MODEL.—

(1) IN GENERAL.—Not later than 2 years after the date on which the model developed under subsection (a) is published, the head of each covered agency shall use the model to develop the annual cybersecurity and information technology budget requests of the agency.

(2) AGENCY PERFORMANCE PLANS.—Section 3554(d)(2) of title 44, United States Code, is amended by inserting ''and the risk-based budget model required under section 3553(a)(7)'' after ''paragraph (1)''.

(c) VERIFICATION.—

(1) IN GENERAL.—Section 1105(a)(35)(A)(i) of title 31, United States Code, is amended—

(A) in the matter preceding subclause (I), by striking ''by agency, and by initiative area (as determined by the administration)'' and inserting ''and by agency'';

(B) in subclause (III), by striking ''and'' at the end; and

(C) by adding at the end the following:

''(V) a validation that the budgets submitted were developed using a risk-based methodology; and

''(VI) a report on the progress of each agency on closing recommendations identified under the independent evaluation required by section 3555(a)(1) of title 44.''.

(2) EFFECTIVE DATE.—The amendments made by paragraph (1) shall take effect on the date that is 2 years after the date on which the model developed under subsection (a) is published.

(d) REPORTS.—

(1) INDEPENDENT EVALUATION.—Section 3555(a)(2) of title 44, United States Code, is amended—

(A) in subparagraph (B), by striking ''and'' at the end;

(B) in subparagraph (C), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(D) an assessment of how the agency implemented the risk-based budget model required under section 3553(a)(7) and an evaluation of whether the model mitigates agency cyber vulnerabilities.''.

(2) ASSESSMENT.—Section 3553(c) of title 44, United States Code, as amended by section 5121, is further amended by inserting after paragraph (5) the following:

''(6) an assessment of—

''(A) Federal agency implementation of the model required under subsection (a)(7);

''(B) how cyber vulnerabilities of Federal agencies changed from the previous year; and

''(C) whether the model mitigates the cyber vulnerabilities of the Federal Government.''.

(e) GAO REPORT.—Not later than 3 years after the date on which the first budget of the President is submitted to Congress containing the validation required under section 1105(a)(35)(A)(i)(V) of title 31, United States Code, as amended by subsection (c), the Comptroller General of the United States shall submit to the appropriate congressional committees a report that includes—

(1) an evaluation of the success of covered agencies in developing risk-based budgets;

(2) an evaluation of the success of covered agencies in implementing risk-based budgets;

(3) an evaluation of whether the risk-based budgets developed by covered agencies mitigate cyber vulnerability, including the extent to which the risk-based budgets inform Federal Government-wide cybersecurity programs; and

(4) any other information relating to risk-based budgets the Comptroller General determines appropriate.

TITLE LIV—PILOT PROGRAMS TO ENHANCE FEDERAL CYBERSECURITY

SEC. 5181. ACTIVE CYBER DEFENSIVE STUDY.

(a) DEFINITION.—In this section, the term ''active defense technique''—

(1) means an action taken on the systems of an entity to increase the security of information on the network of an agency by misleading an adversary; and

(2) includes a honeypot, deception, or purposefully feeding false or misleading data to an adversary when the adversary is on the systems of the entity.

(b) STUDY.—Not later than 180 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Director, shall perform a study on the use of active defense techniques to enhance the security of agencies, which shall include—

(1) a review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice;

(2) an evaluation of—

(A) the efficacy of a selection of active defense techniques determined by the Director of the Cybersecurity and Infrastructure Security Agency; and

(B) factors that impact the efficacy of the active defense techniques evaluated under subparagraph (A);

(3) recommendations on safeguards and procedures that shall be established to require that active defense techniques are adequately coordinated to ensure that active defense techniques do not impede threat response efforts, criminal investigations, and national security activities, including intelligence collection; and

(4) the development of a framework for the use of different active defense techniques by agencies.

SEC. 5182. SECURITY OPERATIONS CENTER AS A SERVICE PILOT.

(a) PURPOSE.—The purpose of this section is for the Cybersecurity and Infrastructure Security Agency to run a security operation center on behalf of another agency, alleviating the need to duplicate this function at every agency, and empowering a greater centralized cybersecurity capability.

(b) PLAN.—Not later than 1 year after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall develop a plan to establish a centralized Federal security operations center shared service offering within the Cybersecurity and Infrastructure Security Agency.

(c) CONTENTS.—The plan required under subsection (b) shall include considerations for—

(1) collecting, organizing, and analyzing agency information system data in real time;

(2) staffing and resources; and

(3) appropriate interagency agreements, concepts of operations, and governance plans.

(d) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date on which the plan required under subsection (b) is developed, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, shall enter into a 1-year agreement with not less than 2 agencies to offer a security operations center as a shared service.

(2) ADDITIONAL AGREEMENTS.—After the date on which the briefing required under subsection (e)(1) is provided, the Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Director, may enter into additional 1-year agreements described in paragraph (1) with agencies.

(e) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 260 days after the date of enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall provide to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a briefing on the parameters of any 1-year agreements entered into under subsection (d)(1).

(2) REPORT.—Not later than 90 days after the date on which the first 1-year agreement entered into under subsection (d) expires, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security and the Committee on Oversight and Reform of the House of Representatives a report on—

(A) the agreement; and

(B) any additional agreements entered into with agencies under subsection (d).

DIVISION F—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

TITLE LXI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 6101. SHORT TITLE.

This title may be cited as the ''Cyber Incident Reporting Act of 2021''.

SEC. 6102. DEFINITIONS.

In this title:

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.—The terms ''covered cyber incident'', ''covered entity'', and ''cyber incident'' have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 6103 of this title.

(2) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms ''information system'', ''ransom payment'', ''ransomware attack'', and ''security vulnerability'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 6203 of this division.

SEC. 6103. CYBER INCIDENT REPORTING.

(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 6203(b) of this division—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.''; and

(2) by adding at the end the following:

''Subtitle C—Cyber Incident Reporting

''SEC. 2230. DEFINITIONS.

''In this subtitle:

''(1) CENTER.—The term 'Center' means the center established under section 2209.

''(2) COUNCIL.—The term 'Council' means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

''(3) COVERED CYBER INCIDENT.—The term 'covered cyber incident' means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

''(4) COVERED ENTITY.—The term 'covered entity' means—

''(A) any Federal contractor; or

''(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

''(5) CYBER INCIDENT.—The term 'cyber incident' has the meaning given the term 'incident' in section 2200.

''(6) CYBER THREAT.—The term 'cyber threat'—

''(A) has the meaning given the term 'cybersecurity threat' in section 2200; and

''(B) does not include any activity related to good faith security research, including participation in a bug-bounty program or a vulnerability disclosure program.

''(7) FEDERAL CONTRACTOR.—The term 'Federal contractor' means a business, nonprofit organization, or other private sector entity that holds a Federal Government contract or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity is a party only to—

''(A) a service contract to provide housekeeping or custodial services; or

''(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

''(8) FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.—The terms 'Federal entity', 'information system', and 'security control' have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

''(9) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(10) SMALL ORGANIZATION.—The term 'small organization'—

''(A) means—

''(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

''(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

''(B) does not include—

''(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

''(ii) a Federal contractor.

''SEC. 2231. CYBER INCIDENT REVIEW.

''(a) ACTIVITIES.—The Center shall—

''(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

''(2) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetuate cyber incidents and ransomware attacks;

''(3) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

''(4) leverage information gathered about cybersecurity incidents to—

''(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and incident response firms, and security researchers; and

''(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2235;

''(5) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

''(6) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

''(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

''(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the briefings required under subsection (c);

''(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

''(11) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

''(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and

''(13) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2233, or information received pursuant to a request for information or subpoena under section 2234, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

''(b) INTERAGENCY SHARING.—The National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

''(1) may establish a specific time requirement for sharing information under subsection (a)(13); and

''(2) shall determine the appropriate Federal agencies under subsection (a)(13).

''(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

''(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

''(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

''(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

''(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

''(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

''(4) be unclassified, but may include a classified annex.

''SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

''(a) IN GENERAL.—

''(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

''(2) RANSOM PAYMENT REPORTS.—A covered entity, except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

''(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

''(4) PRESERVATION OF INFORMATION.—Any covered entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(5) EXCEPTIONS.—

''(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

''(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to a covered entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

''(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to an entity or the functions of an entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

''(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

''(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

''(b) RULEMAKING.—

''(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

''(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

''(3) SUBSEQUENT RULEMAKINGS.—

''(A) IN GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

''(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

''(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

''(1) A clear description of the types of entities that constitute covered entities, based on—

''(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

''(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

''(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

''(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

''(A) at a minimum, require the occurrence of—

''(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes;

''(ii) a disruption of business or industrial operations due to a cyber incident; or

''(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

''(B) consider—

''(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

''(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

''(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

''(C) exclude—

''(i) any event where the cyber incident is perpetuated by good faith security research or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and

''(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

''(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

''(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable

and available, with respect to a covered cyber incident:

''(A) A description of the covered cyber incident, including—

''(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

''(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

''(iii) the estimated date range of such incident; and

''(iv) the impact to the operations of the covered entity.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

''(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

''(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

''(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

''(F) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist with compliance with the requirements of this subtitle.

''(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

''(A) A description of the ransomware attack, including the estimated date range of the attack.

''(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

''(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

''(D) The name and other information that clearly identifies the entity that made the ransom payment.

''(E) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

''(F) The date of the ransom payment.

''(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

''(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

''(I) The amount of the ransom payment.

''(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

''(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

''(A) be established by the Director in consultation with the Council;

''(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

''(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

''(8) Procedures for—

''(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

''(B) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

''(C) implementing the exceptions provided in subsection (a)(5); and

''(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

''(d) THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.—

''(1) REPORT SUBMISSION.—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under subsection (a).

''(2) RANSOM PAYMENT.—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

''(3) DUTY TO REPORT.—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

''(4) RESPONSIBILITY TO ADVISE.—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding reporting ransom payments under this section.

''(e) OUTREACH TO COVERED ENTITIES.—

''(1) IN GENERAL.—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

''(2) ELEMENTS.—The outreach and education campaign under paragraph (1) shall include the following:

''(A) An overview of the final rule issued pursuant to subsection (b).

''(B) An overview of mechanisms to submit to the Center covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

''(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

''(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

''(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

''(F) An overview of the privacy and civil liberties requirements in this subtitle.

''(3) COORDINATION.—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

''(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

''(B) information sharing and analysis organizations;

''(C) trade associations;

''(D) information sharing and analysis centers;

''(E) sector coordinating councils; and

''(F) any other entity as determined appropriate by the Director.

''(f) ORGANIZATION OF REPORTS.—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), the Director may request information within the scope of the final rule issued under subsection (b) by the alteration of existing questions or response fields and the reorganization and reformatting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.

''SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.

''(a) IN GENERAL.—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

''(b) VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

''(c) APPLICATION OF PROTECTIONS.—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

''SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.

''(a) PURPOSE.—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity,

pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

''(b) INITIAL REQUEST FOR INFORMATION.—

''(1) IN GENERAL.—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(a), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Center within 72 hours in accordance with section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

''(2) TREATMENT.—Information provided to the Center in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

''(c) AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.—

''(1) IN GENERAL.—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

''(2) CIVIL ACTION.—

''(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

''(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

''(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

''(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

''(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity that is a Federal contractor fails to comply with a subpoena issued under this subsection—

''(A) the Director may refer the matter to the Administrator of General Services; and

''(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

''(5) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

''(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

''(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

''(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency determines, based on information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may use that information for a regulatory enforcement action or criminal prosecution.

''(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

''(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

''(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

''(1) the size and complexity of the entity;

''(2) the complexity in determining if a covered cyber incident has occurred; and

''(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

''(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

''(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b);

''(2) issued a subpoena pursuant to subsection (c); or

''(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

''(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

''(1) issued an initial request for information pursuant to subsection (b); or

''(2) issued a subpoena pursuant to subsection (c).

''(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

''SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

''(a) DISCLOSURE, RETENTION, AND USE.—

''(1) AUTHORIZED ACTIVITIES.—Information provided to the Center or Agency pursuant to section 2232 or 2233 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

''(A) a cybersecurity purpose;

''(B) the purpose of identifying—

''(i) a cyber threat, including the source of the cyber threat; or

''(ii) a security vulnerability;

''(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

''(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

''(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2232 or 2233 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

''(2) AGENCY ACTIONS AFTER RECEIPT.—

''(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the center shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

''(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

''(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Center or the Agency pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

''(A) personal information of a specific individual; or

''(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

''(4) DIGITAL SECURITY.—The Center and the Agency shall ensure that reports submitted to the Center or the Agency pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

''(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment.

''(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

''(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the 'Freedom of Information Act') and any State, Tribal, or local provision of law requiring disclosure of information or records.

''(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

''(e) LIABILITY PROTECTIONS.—

''(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rule promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

''(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Center or the Agency.

''(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

''(f) SHARING WITH NON-FEDERAL ENTITIES.—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

''(g) PROPRIETARY INFORMATION.—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.

''(h) STORED COMMUNICATIONS ACT.—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the items relating to subtitle B of title XXII the following:

''Subtitle C—Cyber Incident Reporting

''Sec. 2230. Definitions.
''Sec. 2231. Cyber Incident Review.
''Sec. 2232. Required reporting of certain cyber incidents.
''Sec. 2233. Voluntary reporting of other cyber incidents.
''Sec. 2234. Noncompliance with required reporting.
''Sec. 2235. Information shared with or provided to the Federal Government.''.

SEC. 6104. FEDERAL SHARING OF INCIDENT REPORTS.

(a) CYBER INCIDENT REPORTING SHARING.—

(1) IN GENERAL.—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Director as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 6103 of this title.

(2) RULE OF CONSTRUCTION.—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) PROTECTION OF INFORMATION.—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this Act or the amendments made by this Act.

(4) FOIA EXEMPTION.—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the ''Freedom of Information Act'').

(b) CREATION OF COUNCIL.—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is amended—

(1) in paragraph (1)—

(A) in subparagraph (G), by striking ''and'' at the end;

(B) by redesignating subparagraph (H) as subparagraph (I); and

(C) by inserting after subparagraph (G) the following:

''(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget, the Attorney General, and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and''; and

(2) by adding at the end the following:

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any Federal entity.''.

(c) HARMONIZING REPORTING REQUIREMENTS.—The National Cyber Director shall, in consultation with the Director, the Attorney General, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director, the Attorney General, and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 6105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) PROGRAM.—Not later than 1 year after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) IDENTIFICATION OF VULNERABLE SYSTEMS.—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).

(c) ENTITY NOTIFICATION.—

(1) IDENTIFICATION.—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) NO IDENTIFICATION.—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.

(3) REQUIRED INFORMATION.—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) PRIORITIZATION OF NOTIFICATIONS.—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) LIMITATION ON PROCEDURES.—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(g) TERMINATION.—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.

SEC. 6106. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) JOINT RANSOMWARE TASK FORCE.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in consultation

with the Attorney General and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) RESPONSIBILITIES.—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) CLARIFYING PRIVATE SECTOR LAWFUL DEFENSIVE MEASURES.—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 6107. CONGRESSIONAL REPORTING.

(a) REPORT ON STAKEHOLDER ENGAGEMENT.—Not later than 30 days after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103(b) of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 6103(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 6105, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 6105(c) in mitigating security vulnerabilities and the threat of ransomware.

(2) Identification of the most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated under this pilot by the Agency during the preceding year.

(d) REPORT ON HARMONIZATION OF REPORTING REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the National Cyber Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) GAO REPORTS.—

(1) IMPLEMENTATION OF THIS ACT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this Act and the amendments made by this Act.

(2) EXEMPTIONS TO REPORTING.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (2) and (5) of section 2232(a) of the Homeland Security Act of 2002, as added by section 6103 of this title, which shall include—

(A) to the extent practicable, an evaluation of the quantity of incidents not reported to the Federal Government;

(B) an evaluation of the impact on impacted entities, homeland security, and the national economy of the ransomware criminal ecosystem of incidents and ransom payments, including a discussion on the scope of impact of incidents that were not reported to the Federal Government;

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this Act, including an analysis of entities that meet the definition of a small organization and would be exempt from ransom payment reporting but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 6103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2234 of the Homeland Security Act of 2002, as added by section 6103 of this title.

TITLE LXII—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 6201. SHORT TITLE.

This title may be cited as the ''CISA Technical Corrections and Improvements Act of 2021''.

SEC. 6202. REDESIGNATIONS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217; and

(5) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (11), by striking ''and'' at the end;

(2) in the first paragraph (12)—

(A) by striking ''section 2215'' and inserting ''section 2217''; and

(B) by striking ''and'' at the end; and

(3) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) ADDITIONAL TECHNICAL AMENDMENT.—

(1) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if

enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

SEC. 6203. CONSOLIDATION OF DEFINITIONS.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitle A heading the following:

"SEC. 2200. DEFINITIONS.

''Except as otherwise specifically provided, in this title:

''(1) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(2) AGENCY INFORMATION.—The term 'agency information' means information collected or maintained by or on behalf of an agency.

''(3) AGENCY INFORMATION SYSTEM.—The term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency.

''(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(B) the Committee on Homeland Security of the House of Representatives.

''(5) CLOUD SERVICE PROVIDER.—The term 'cloud service provider' means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

''(6) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

''(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

''(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

''(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

''(7) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' means information that is necessary to describe or identify—

''(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

''(B) a method of defeating a security control or exploitation of a security vulnerability;

''(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

''(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

''(E) malicious cyber command and control;

''(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

''(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

''(H) any combination thereof.

''(8) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

''(9) CYBERSECURITY RISK.—The term 'cybersecurity risk'—

''(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

''(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

''(10) CYBERSECURITY THREAT.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'cybersecurity threat' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

''(B) EXCLUSION.—The term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

''(11) DEFENSIVE MEASURE.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

''(B) EXCLUSION.—The term 'defensive measure' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

''(i) the entity operating the measure; or

''(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

''(12) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

''(13) INCIDENT.—The term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

''(14) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

''(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

''(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

''(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

''(15) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(16) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(17) MANAGED SERVICE PROVIDER.—The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

''(18) MONITOR.—The term 'monitor' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

''(19) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

''(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

''(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

''(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

''(D) facilitating information sharing and operational coordination with threat response; and

''(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

''(20) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(21) RANSOM PAYMENT.—The term 'ransom payment' means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

''(22) RANSOMWARE ATTACK.—The term 'ransomware attack'—

''(A) means a cyber incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

''(B) does not include any such event where the demand for payment is made by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

''(23) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

''(24) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

''(25) SECURITY VULNERABILITY.—The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

''(26) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

''(27) SUPPLY CHAIN COMPROMISE.—The term 'supply chain compromise' means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize the confidentiality, integrity, or availability of the information technology system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

''(28) VIRTUAL CURRENCY.—The term 'virtual currency' means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

''(29) VIRTUAL CURRENCY ADDRESS.—The term 'virtual currency address' means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

''SEC. 2201. DEFINITION.

''In this subtitle, the term 'Cybersecurity Advisory Committee' means the advisory committee established under section 2219(a).'';

(2) in section 2202—

(A) in subsection (a)(1), by striking ''(in this subtitle referred to as the Agency)'';

(B) in subsection (f)—

(i) in paragraph (1), by inserting ''Executive'' before ''Assistant Director''; and

(ii) in paragraph (2), by inserting ''Executive'' before ''Assistant Director'';

(3) in section 2203(a)(2), by striking ''as the 'Assistant Director' '' and inserting ''as the 'Executive Assistant Director' '';

(4) in section 2204(a)(2), by striking ''as the 'Assistant Director' '' and inserting ''as the 'Executive Assistant Director' '';

(5) in section 2209—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)—

(i) in subparagraph (A)(iii), as so redesignated, by striking '', as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))''; and

(ii) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(ii) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(E) in subsection (j), as so redesignated, by striking ''subsection (c)(8)'' and inserting ''subsection (b)(8)''; and

(F) in subsection (n), as so redesignated—

(i) in paragraph (2)(A), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)''; and

(ii) in paragraph (3)(B)(i), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)'';

(6) in section 2210—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(C) in subsection (b), as so redesignated—

(i) by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations''; and

(ii) by striking ''(as defined in section 2209)''; and

(D) in subsection (c), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (b)'';

(7) in section 2211, by striking subsection (h);

(8) in section 2212, by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations'';

(9) in section 2213—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (f) as subsections (a) through (e); respectively;

(C) in subsection (b), as so redesignated, by striking ''subsection (b)'' each place it appears and inserting ''subsection (a)'';

(D) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking ''subsection (b)'' and inserting ''subsection (a)''; and

(E) in subsection (d), as so redesignated—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(II) in subparagraph (A), by striking ''subsection (c)(1)'' and inserting ''subsection (b)(1)''; and

(III) in subparagraph (B), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)''; and

(ii) in paragraph (2), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(10) in section 2216, as so redesignated—

(A) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(B) by striking subsection (f) and inserting the following:

''(f) CYBER DEFENSE OPERATION DEFINED.—In this section, the term 'cyber defense operation' means the use of a defensive measure.'';

(11) in section 2218(c)(4)(A), as so redesignated, by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(12) in section 2222—

(A) by striking paragraphs (3), (5), and (8);

(B) by redesignating paragraph (4) as paragraph (3); and

(C) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXII the following:

''Sec. 2200. Definitions.'';

(2) by striking the item relating to section 2201 and inserting the following:

''Sec. 2201. Definition.''; and

(3) by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint Cyber Planning Office.
''Sec. 2217. Cybersecurity State Coordinator.
''Sec. 2218. Sector Risk Management Agencies.
''Sec. 2219. Cybersecurity Advisory Committee.
''Sec. 2220. Cybersecurity Education and Training Programs.''.

(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

''(4) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(6) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(7) DEFENSIVE MEASURE.—The term 'defensive measure' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) by striking paragraph (13) and inserting the following:

''(13) MONITOR.— The term 'monitor' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''; and

(3) by striking paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''.

SEC. 6204. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking ''section 2210'' and inserting ''section 2200''; and

(B) in paragraph (4), by striking ''section 2209'' and inserting ''section 2200'';

(2) in section 223(b) (6 U.S.C. 151 note), by striking ''section 2213(b)(1)'' each place it appears and inserting ''section 2213(a)(1)'';

(3) in section 226 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

(iii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iv) in paragraph (5), by striking ''section 2213(b)'' and inserting ''section 2213(a)''; and

(B) in subsection (c)(1)(A)(vi), by striking ''section 2213(c)(5)'' and inserting ''section 2213(b)(5)''; and

(4) in section 227(b) (6 U.S.C. 1525(b)), by striking ''section 2213(d)(2)'' and inserting ''section 2213(c)(2)''.

(b) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking ''section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))'' and inserting ''section 2210(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

(c) WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))'' and inserting ''section 2200 of the Homeland Security Act of 2002''; and

(B) by amending paragraph (7) to read as follows:

''(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) in subsection (c)(3)(B), by striking ''section 2201(5)'' and inserting ''section 2200''; and

(3) in subsection (d)—

(A) by striking ''section 2215'' and inserting ''section 2218''; and

(B) by striking '', as added by this section''.

(d) NATIONAL SECURITY ACT OF 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking ''section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147)'' and inserting ''section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(e) IOT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking ''section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(l))''.

(f) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of the Small Business Act (15 U.S.C. 648(a)(8)(B)) is amended by striking ''section 2209(a)'' and inserting ''section 2200''.

(g) TITLE 46.—Section 70101(2) of title 46, United States Code, is amended by striking ''section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)'' and inserting ''section 2200 of the Homeland Security Act of 2002''.

TITLE LXIII—FEDERAL CYBERSECURITY REQUIREMENTS

SEC. 6301. EXEMPTION FROM FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IN GENERAL.—Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) is amended to read as follows:

''(2) EXCEPTION.—

''(A) IN GENERAL.—A particular requirement under paragraph (1) shall not apply to an agency information system of an agency if—

''(i) with respect to the agency information system, the head of the agency submits to the Director an application for an exemption from the particular requirement, in which the head of the agency personally certifies to the Director with particularity that—

''(I) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the particular requirement;

''(II) the particular requirement is not necessary to secure the agency information system or agency information stored on or transiting the agency information system; and

''(III) the agency has taken all necessary steps to secure the agency information system and agency information stored on or transiting the agency information system;

''(ii) the head of the agency or the designee of the head of the agency has submitted the certification described in clause (i) to the appropriate congressional committees and any other congressional committee with jurisdiction over the agency; and

''(iii) the Director grants the exemption from the particular requirement.

''(B) DURATION OF EXEMPTION.—

''(i) IN GENERAL.—An exemption granted under subparagraph (A) shall expire on the date that is 1 year after the date on which the Director grants the exemption.

''(ii) RENEWAL.—Upon the expiration of an exemption granted to an agency under subparagraph (A), the head of the agency may apply for an additional exemption.''.

(b) REPORT ON EXEMPTIONS.—Section 3554(c)(1) of title 44, United States Code, as amended by section 5121 of this Act, is further amended—

(1) in subparagraph (C), by striking ''and'' at the end;

(2) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(E) with respect to any exemptions the agency is granted by the Director of the Office of Management and Budget under section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1523(b)(2)) that is effective on the date of submission of the report, includes—

''(i) an identification of the particular requirements from which any agency information system (as defined in section 2210 of the Homeland Security Act of 2002 (6 U.S.C. 660)) is exempted; and

''(ii) for each requirement identified under subclause (I)—

''(I) an identification of the agency information system described in subclause (I) exempted from the requirement; and

''(II) an estimate of the date on which the agency will to be able to comply with the requirement.''.

(c) EFFECTIVE DATE.—This section and the amendments made by this section shall take effect on the date that is 1 year after the date of enactment of this Act.

SA 4832. Mr. MENENDEZ submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title XII, add the following:

Subtitle H—Sanctions Relating to the Actions of the Russian Federation With Respect to Ukraine

SEC. 1291. DEFINITIONS.

In this subtitle:

(1) ADMISSION; ADMITTED; ALIEN.—The terms ''admission'', ''admitted'', and ''alien'' have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations and the Committee on Banking, Housing, and Urban Affairs of the Senate; and

(B) the Committee on Foreign Affairs and the Committee on Financial Services of the House of Representatives.

(3) DEFENSE ARTICLE; DEFENSE SERVICE.—The terms ''defense article'' and ''defense service'' have the meanings given those terms in section 47 of the Arms Export Control Act (22 U.S.C. 2794).

(4) FINANCIAL INSTITUTION.—The term ''financial institution'' means a financial institution specified in subparagraph (A), (B), (C), (D), (E), (F), (G), (H), (I), (J), (M), or (Y) of section 5312(a)(2) of title 31, United States Code.

(5) FOREIGN FINANCIAL INSTITUTION.—The term ''foreign financial institution'' has the meaning given that term in regulations prescribed by the Secretary of the Treasury.

(6) FOREIGN PERSON.—The term ''foreign person'' means an individual or entity that is not a United States person.

(7) KNOWINGLY.—The term ''knowingly'' with respect to conduct, a circumstance, or a result, means that a person has actual knowledge, or should have known, of the conduct, the circumstance, or the result.

(8) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity.

SEC. 1292. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) it is in the national security interests of the United States to continue and deepen the security partnership between the United States and Ukraine, including through providing both lethal and non-lethal assistance to Ukraine;

(2) aggression and malign influence by the Government of the Russian Federation in Ukraine is a threat to the democratic sovereignty of Ukraine, a valued and key partner of the United States;

(3) economic and financial sanctions, when used as part of a coordinated and comprehensive strategy, are a powerful tool to advance United States foreign policy and national security interests;

(4) the United States should expedite the provision of lethal and non-lethal assistance to Ukraine, and use all available tools to support and bolster the defense of Ukraine against potential aggression and military escalation by the Government of the Russian Federation;

(5) the United States should work closely with partners and allies to encourage the provision of lethal and non-lethal assistance to support and bolster the defense of Ukraine; and

(6) substantial new sanctions should be imposed in the event that the Government of

the Russian Federation engages in escalatory military or other offensive operations against Ukraine.

SEC. 1293. DETERMINATION WITH RESPECT TO OPERATIONS OF THE RUSSIAN FEDERATION IN UKRAINE.

Not later than 15 days after the date of the enactment of this Act, and periodically as necessary thereafter, the President shall—

(1) determine whether—

(A) the Government of the Russian Federation is engaged in or knowingly supporting a significant escalation in hostilities or hostile action in or against Ukraine, compared to the level of hostilities or hostile action in or against Ukraine prior to November 1, 2021; and

(B) if so, whether such escalation has the aim of undermining, overthrowing, or dismantling the Government of Ukraine, occupying the territory of Ukraine, or interfering with the sovereignty or territorial integrity of Ukraine; and

(2) submit to the appropriate congressional committees a report on that determination.

SEC. 1294. IMPOSITION OF SANCTIONS WITH RESPECT TO OFFICIALS OF THE GOVERNMENT OF THE RUSSIAN FEDERATION RELATING TO OPERATIONS IN UKRAINE.

(a) IN GENERAL.—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (d) with respect to each of the officials specified in subsection (b).

(b) OFFICIALS SPECIFIED.—The officials specified in this subsection are the following:

(1) The President of the Russian Federation.

(2) The Prime Minister of the Russian Federation.

(3) The Foreign Minister of the Russian Federation.

(4) The Minister of Defense of the Russian Federation.

(5) The Chief of the General Staff of the Armed Forces of the Russian Federation.

(6) The Commander-in-Chief of the Land Forces of the Russian Federation.

(7) The Commander of the Aerospace Forces of the Russian Federation.

(8) The Commander of the Airborne Forces of the Russian Federation.

(9) The Commander in Chief of the Navy of the Russian Federation.

(10) The Commander of the Strategic Rocket Forces of the Russian Federation.

(11) The Commander of the Special Operations Forces of the Russian Federation.

(12) The Commander of Logistical Support of the Russian Armed Forces.

(c) ADDITIONAL OFFICIALS.—

(1) LIST REQUIRED.—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall submit to the appropriate congressional committees a list of foreign persons that the President determines are—

(A) senior officials of any branch of the armed forces of the Russian Federation leading any of the operations described in section 1293(1); or

(B) senior officials of the Government of the Russian Federation, including any branch of the armed forces or intelligence agencies of the Russian Federation, engaged in planning or implementing such operations.

(2) IMPOSITION OF SANCTIONS.—Upon the submission of each list required by paragraph (1), the President shall impose the sanctions described in subsection (d) with respect to each foreign person identified on the list.

(d) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person under this section are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (b) or (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1295. IMPOSITION OF SANCTIONS WITH RESPECT TO FOREIGN FINANCIAL INSTITUTIONS.

(a) IMPOSITION OF SANCTIONS.—

(1) IN GENERAL.—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (c) with respect to 3 or more of the following financial institutions:

(A) Sberbank.

(B) VTB.

(C) Gazprombank.

(D) VEB.RF.

(E) RDIF.

(F) Promsvyazbank.

(2) SUBSIDIARIES AND SUCCESSOR ENTITIES.—The President may impose the sanctions described in subsection (c) with respect to any subsidiary of, or successor entity to, a financial institution specified in paragraph (1).

(b) ADDITIONAL FOREIGN FINANCIAL INSTITUTIONS.—

(1) LIST REQUIRED.—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall submit to the appropriate congressional committees a list of foreign persons that the President determines—

(A) are significant financial institutions owned or operated by the Government of the Russian Federation; and

(B) should be sanctioned in the interest of United States national security.

(2) IMPOSITION OF SANCTIONS.—Upon the submission of each list required by paragraph (1), the President shall impose the sanctions described in subsection (c) with respect to each foreign person identified on the list.

(c) SANCTIONS DESCRIBED.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a foreign person subject to subsection (a) or (b) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

SEC. 1296. PROHIBITION ON AND IMPOSITION OF SANCTIONS WITH RESPECT TO TRANSACTIONS INVOLVING RUSSIAN SOVEREIGN DEBT.

(a) PROHIBITION ON TRANSACTIONS.—Upon making an affirmative determination under section 1293(1) and not later than 30 days following such a determination, the President shall prohibit all transactions by United States persons involving the sovereign debt of the Government of the Russian Federation issued on or after the date of the enactment of this Act, including governmental bonds.

(b) IMPOSITION OF SANCTIONS WITH RESPECT TO STATE-OWNED ENTERPRISES.—

(1) IN GENERAL.—Not later than 60 days after making an affirmative determination under section 1293(1), the President shall identify and impose the sanctions described in subsection (d) with respect to foreign persons that the President determines engage in transactions involving the debt—

(A) of not less than 10 entities owned or controlled by the Government of the Russian Federation; and

(B) that is not subject to any other sanctions imposed by the United States.

(2) APPLICABILITY.—Sanctions imposed under paragraph (1) shall apply with respect to debt of an entity described in subparagraph (A) of that paragraph that is issued after the date that is 90 days after the President makes an affirmative determination under section 1293(1).

(c) LIST; IMPOSITION OF SANCTIONS.—Not later than 30 days after making an affirmative determination under section 1293(1), and every 90 days thereafter, the President shall—

(1) submit to the appropriate congressional committees a list of foreign persons that the President determines are engaged in transactions described in subsection (a); and

(2) impose the sanctions described in subsection (d) with respect to each such person.

(d) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person described in subsection (b) or (c) are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (b) or (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1297. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Upon making an affirmative determination under section 1293(1) and

not later than 30 days following such a determination, the President shall impose the sanctions described in subsection (b) with respect to a foreign person that is—

(1) any entity established for or responsible for the planning, construction, or operation of the Nord Stream 2 pipeline or a successor entity; and

(2) any corporate officer of an entity described in paragraph (1).

(b) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person under this section are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (a)(2) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1298. SANCTIONS WITH RESPECT TO RUSSIAN EXTRACTIVE INDUSTRIES.

(a) IDENTIFICATION.—Not later than 60 days after making an affirmative determination under section 1293(1), the President shall identify foreign persons in any of the sectors or industries described in subsection (b) that the President determines should be sanctioned in the interest of United States national security.

(b) SECTORS AND INDUSTRIES DESCRIBED.—The sectors and industries described in this subsection are the following:

(1) Oil and gas extraction and production.

(2) Coal extraction, mining, and production.

(3) Minerals extraction and processing.

(4) Any other sector or industry with respect to which the President determines the imposition of sanctions is in the United States national security interest.

(c) LIST; IMPOSITION OF SANCTIONS.—Not later than 90 days after making an affirmative determination under section 1293(1), the President shall—

(1) submit to the appropriate congressional committees a list of the persons identified under subsection (a); and

(2) impose the sanctions described in subsection (d) with respect to each such person.

(d) SANCTIONS DESCRIBED.—The sanctions to be imposed with respect to a foreign person under subsection (c) are the following:

(1) PROPERTY BLOCKING.—The President shall exercise all of the powers granted by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of the foreign person if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(2) ALIENS INADMISSIBLE FOR VISAS, ADMISSION, OR PAROLE.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (c) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

SEC. 1299. AUTHORIZATION FOR USE OF WAR RESERVE STOCKPILE FOR ARMED FORCES OF UKRAINE.

Notwithstanding section 514 of the Foreign Assistance Act of 1961 (22 U.S.C. 2321h) or any other authorized limits set in law, the Secretary of Defense, in concurrence with the Secretary of State, is authorized to transfer defense articles from any war reserve stockpile to Ukraine for the purpose of assisting and supporting the Armed Forces of Ukraine.

SEC. 1299A. USE OF DEPARTMENT OF DEFENSE LEASE AUTHORITY AND SPECIAL DEFENSE ACQUISITION FUND TO SUPPORT UKRAINE.

(a) USE OF SPECIAL DEFENSE ACQUISITION FUND.—The Secretary of Defense, in concurrence with the Secretary of State, shall utilize, to the maximum extent possible, the Special Defense Acquisition Fund established under section 51 of the Arms Export Control Act (22 U.S.C. 2795) to expedite the procurement and delivery of defense articles and defense services for the purpose of assisting and supporting the Armed Forces of Ukraine.

(b) USE OF LEASE AUTHORITY.—The Secretary of Defense, in concurrence with the Secretary of State, shall utilize, to the maximum extent possible, its lease authority, including with respect to no-cost leases, to provide defense articles to Ukraine for the purpose of assisting and supporting the Armed Forces of Ukraine.

SEC. 1299B. IMPLEMENTATION; REGULATIONS; PENALTIES.

(a) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this subtitle.

(b) REGULATIONS.—The President shall issue such regulations, licenses, and orders as are necessary to carry out this subtitle.

(c) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this subtitle or any regulation, license, or order issued to carry out this subtitle shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

SEC. 1299C. EXCEPTIONS; WAIVER.

(a) EXCEPTIONS.—

(1) INTELLIGENCE ACTIVITIES.—This subtitle shall not apply with respect to activities subject to the reporting requirements under title V of the National Security Act of 1947 (50 U.S.C. 3091 et seq.) or any authorized intelligence activities of the United States.

(2) EXCEPTION COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT AND LAW ENFORCEMENT OBJECTIVES.—Sanctions under this subtitle shall not apply to an alien if admitting the alien into the United States—

(A) is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success on June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations of the United States; or

(B) would further important law enforcement objectives.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—The authority or a requirement to impose sanctions under this subtitle shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term ''good'' means any article, natural or manmade substance, material, supply, or manufactured product, including inspection and test equipment, and excluding technical data.

(b) NATIONAL SECURITY WAIVER.—The President may waive the imposition of sanctions under this subtitle with respect to a person if the President—

(1) determines that such a waiver is in the national security interests of the United States; and

(2) submits to the appropriate congressional committees a notification of the waiver and the reasons for the waiver.

SEC. 1299D. TERMINATION.

The President may terminate the sanctions imposed under this subtitle after determining and certifying to the appropriate congressional committees that the Government of the Russian Federation has—

(1) verifiably withdrawn all of its forces from Ukrainian territory that was not occupied or subject to control by forces or proxies of the Government of the Russian Federation prior to November 1, 2021;

(2) ceased supporting proxies in Ukrainian territory described in paragraph (1); and

(3) has entered into an agreed settlement with a legitimate democratic government of Ukraine.

SEC. 1299E. SUNSET.

The provisions of this subtitle shall terminate on the date that is 3 years after the date of the enactment of this Act.

SA 4833. Mr. BARRASSO (for himself, Mr. CRUZ, and Mr. JOHNSON) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle D of title XII, add the following:

SEC. 1237. IMPOSITION OF SANCTIONS WITH RESPECT TO NORD STREAM 2.

(a) IN GENERAL.—Not later than 15 days after the date of the enactment of this Act, the President shall—

(1) impose sanctions under subsection (b) with respect to—

(A) Nord Stream 2 AG or a successor entity;

(B) Matthias Warnig; and

(C) any other corporate officer of or principal shareholder with a controlling interest in Nord Stream 2 AG or a successor entity; and

(2) impose sanctions under subsection (c) with respect to—

(A) Nord Stream 2 AG or a successor entity; and

(B) Matthias Warnig.

(b) INELIGIBILITY FOR VISAS, ADMISSION, OR PAROLE OF IDENTIFIED PERSONS AND CORPORATE OFFICERS.—

(1) IN GENERAL.—

(A) VISAS, ADMISSION, OR PAROLE.—An alien described in subsection (a)(1) is—

(i) inadmissible to the United States;

(ii) ineligible to receive a visa or other documentation to enter the United States; and

(iii) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(B) CURRENT VISAS REVOKED.—

(i) IN GENERAL.—The visa or other entry documentation of an alien described in subsection (a)(1) shall be revoked, regardless of when such visa or other entry documentation is or was issued.

(ii) IMMEDIATE EFFECT.—A revocation under clause (i) shall—

(I) take effect immediately; and

(II) automatically cancel any other valid visa or entry documentation that is in the alien's possession.

(c) BLOCKING OF PROPERTY OF IDENTIFIED PERSONS.—The President shall exercise all powers granted to the President by the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) to the extent necessary to block and prohibit all transactions in all property and interests in property of a person described in subsection (a)(2) if such property and interests in property are in the United States, come within the United States, or are or come within the possession or control of a United States person.

(d) IMPLEMENTATION; PENALTIES.—

(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this section.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of this section or any regulation, license, or order issued to carry out this section shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

(e) EXCEPTIONS.—

(1) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under this section shall not apply to any authorized intelligence, law enforcement, or national security activities of the United States.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under this section shall not apply with respect to the admission of an alien to the United States if the admission of the alien is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or other applicable international obligations.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—Notwithstanding any other provision of this section, the authorities and requirements to impose sanctions under this section shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term ''good'' means any article, natural or man-made substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(f) SUNSET.—The authority to impose sanctions under this section shall terminate on the date that is 5 years after the date of the enactment of this Act.

(g) DEFINITIONS.—In this section:

(1) ADMISSION; ADMITTED; ALIEN.—The terms ''admission'' , ''admitted'' , and ''alien'' have the meanings given those terms in section 101 of the Immigration and Nationality Act (8 U.S.C. 1101).

(2) UNITED STATES PERSON.—The term ''United States person'' means—

(A) a United States citizen or an alien lawfully admitted for permanent residence to the United States;

(B) an entity organized under the laws of the United States or any jurisdiction within the United States, including a foreign branch of such an entity; or

(C) any person within the United States.

AUTHORITY FOR COMMITTEES TO MEET

Mr. TESTER. Mr. President, I have 6 requests for committees to meet during today's session of the Senate. They have the approval of the Majority and Minority Leaders.

Pursuant to rule XXVI, paragraph 5(a), of the Standing Rules of the Senate, the following committees are authorized to meet during today's session of the Senate:

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

The Committee on Banking, Housing, and Urban Affairs is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9:30 a.m., to conduct a hearing on a nomination.

COMMITTEE ON ENERGY AND NATURAL RESOURCES

The Committee on Energy and Natural Resources is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10 a.m., to conduct a business meeting.

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

The Committee on Homeland Security and Governmental Affairs is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10:15 a.m., to conduct a hearing on nominations.

COMMITTEE ON THE JUDICIARY

The Committee on the Judiciary is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9 a.m., to conduct a hearing.

SPECIAL COMMITTEE ON AGING

The Special Committee on Aging is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 9:30 a.m., to conduct a hearing.

SUBCOMMITTEE ON WESTERN HEMISPHERE, TRANSNATIONAL CRIME, CIVILIAN SECURITY, DEMOCRACY, HUMAN RIGHTS, AND GLOBAL WOMEN'S ISSUES

The Subcommittee on Western Hemisphere, Transnational Crime, Civilian Security, Democracy, Human Rights, and Global Women's Issues of the Committee on Foreign Relations is authorized to meet during the session of the Senate on Thursday, November 18, 2021, at 10 a.m., to conduct a hearing.

PRIVILEGES OF THE FLOOR

Mr. REED. Mr. President, I ask unanimous consent that Leslie Ashton and Cami Pease, Government Accountability Office detailees to the Senate Armed Services Committee, have floor privileges during consideration of the fiscal year 2022 National Defense Authorization Act.

The PRESIDING OFFICER. Without objection, it is so ordered.

The PRESIDING OFFICER. The majority leader.

EXECUTIVE SESSION

EXECUTIVE CALENDAR

Mr. SCHUMER. Madam President, I ask unanimous consent that the Senate proceed to executive session to consider the following nominations en bloc: Calendar Nos. 332 and 444; that the Senate vote on the nominations en bloc without intervening action or debate; that the motions to reconsider be considered made and laid upon the table with no intervening action or debate; that any statements related to the nominations be printed in the RECORD; that the President be immediately notified of the Senate's action, and the Senate resume legislative session.

There being no objection, the Senate proceeded to consider the nominations.

The PRESIDING OFFICER. The question is, Will the Senate advise and consent to the nominations of Lee Satterfield, of South Carolina, to be an Assistant Secretary of State (Educational and Cultural Affairs) and Jeffrey M. Hovenier, of Washington, a Career Member of the Senior Foreign Service, Class of Minister-Counselor, to be Ambassador Extraordinary and Plenipotentiary of the United States of America to the Republic of Kosovo en bloc?

The nominations were confirmed en bloc.

LEGISLATIVE SESSION

The PRESIDING OFFICER. The Senate will now resume legislative session.

ORDERS FOR FRIDAY, NOVEMBER 19, 2021

Mr. SCHUMER. Madam President, I ask unanimous consent that when the

Senate complete its business today, it adjourn until 10 a.m., Friday, November 19; that following the prayer and pledge, the morning hour be deemed expired, the Journal of proceedings be approved to date, the time for the two leaders be reserved for their use later in the day, and morning business be closed; that upon the conclusion of morning business, the Senate resume consideration of the motion to proceed to H.R. 4350, the National Defense Authorization Act, postcloture; further, that all time during adjournment, morning business, recess, and leader time count postcloture.

The PRESIDING OFFICER. Without objection, it is so ordered.

ADJOURNMENT UNTIL 10 A.M. TOMORROW

Mr. SCHUMER. Madam President, if there is no further business to come before the Senate, I ask unanimous consent that it stand adjourned under the previous order.

There being no objection, the Senate, at 10:14 p.m., adjourned until Friday, November 19, 2021, at 10: a.m.

NOMINATIONS

Executive nominations received by the Senate:

THE JUDICIARY

ANDRE B. MATHIS, OF TENNESSEE, TO BE UNITED STATES CIRCUIT JUDGE FOR THE SIXTH CIRCUIT, VICE BERNICE BOUIE DONALD, RETIRING.

ALISON J. NATHAN, OF NEW YORK, TO BE UNITED STATES CIRCUIT JUDGE FOR THE SECOND CIRCUIT, VICE ROSEMARY S. POOLER, RETIRING.

CONFIRMATIONS

Executive nominations confirmed by the Senate November 18, 2021:

DEPARTMENT OF STATE

LEE SATTERFIELD, OF SOUTH CAROLINA, TO BE AN ASSISTANT SECRETARY OF STATE (EDUCATIONAL AND CULTURAL AFFAIRS).

JULIANNE SMITH, OF MICHIGAN, TO BE UNITED STATES PERMANENT REPRESENTATIVE ON THE COUNCIL OF THE NORTH ATLANTIC TREATY ORGANIZATION , WITH THE RANK AND STATUS OF AMBASSADOR EXTRAORDINARY AND PLENIPOTENTIARY.

JEFFREY M. HOVENIER, OF WASHINGTON, A CAREER MEMBER OF THE SENIOR FOREIGN SERVICE, CLASS OF MINISTER–COUNSELOR, TO BE AMBASSADOR EXTRAORDINARY AND PLENIPOTENTIARY OF THE UNITED STATES OF AMERICA TO THE REPUBLIC OF KOSOVO.

DEPARTMENT OF THE INTERIOR

CHARLES F. SAMS III, OF OREGON, TO BE DIRECTOR OF THE NATIONAL PARK SERVICE.