

DEPARTMENT OF HOMELAND SECURITY  
APPROPRIATIONS FOR 2024

---

HEARINGS  
BEFORE A  
SUBCOMMITTEE OF THE  
COMMITTEE ON APPROPRIATIONS  
HOUSE OF REPRESENTATIVES  
ONE HUNDRED EIGHTEENTH CONGRESS  
FIRST SESSION

SUBCOMMITTEE ON HOMELAND SECURITY

**DAVID P. JOYCE, Ohio, *Chairman***

JOHN H. RUTHERFORD, Florida  
ANDY HARRIS, Maryland  
DAN NEWHOUSE, Washington  
ASHLEY HINSON, Iowa  
MICHAEL CLOUD, Texas  
MICHAEL GUEST, Mississippi

HENRY CUELLAR, Texas  
LAUREN UNDERWOOD, Illinois  
ED CASE, Hawaii  
DAVID J. TRONE, Maryland

NOTE: Under committee rules, Ms. Granger, as chairwoman of the full committee, and Ms. DeLauro, as ranking minority member of the full committee, are authorized to sit as members of all subcommittees.

PAUL ANSTINE, LAURA CYLKE, ANNA LANIER FISCHER, FERN TOLLEY GIBBONS,  
EMILY TRAPANI and BROOKLYN TUCKER  
*Subcommittee Staff*

**PART 1**

**DEPARTMENT OF HOMELAND SECURITY**

	Page
<b>Cybersecurity and Infrastructure Fiscal Year 2024</b>	
<b>Budget Request</b> .....	<b>1</b>
<b>Transportation Security Administration Fiscal Year</b>	
<b>2024 Budget Request</b> .....	<b>47</b>
<b>Department of Homeland Security Fiscal Year 2024</b>	
<b>Budget Request</b> .....	<b>91</b>



Printed for the use of the Committee on Appropriations

U.S. GOVERNMENT PUBLISHING OFFICE

## COMMITTEE ON APPROPRIATIONS

KAY GRANGER, Texas, *Chairwoman*

HAROLD ROGERS, Kentucky	ROSA L. DeLAURO, Connecticut
ROBERT B. ADERHOLT, Alabama	STENY H. HOYER, Maryland
MICHAEL K. SIMPSON, Idaho	MARCY KAPTUR, Ohio
JOHN R. CARTER, Texas	SANFORD D. BISHOP, Jr., Georgia
KEN CALVERT, California	BARBARA LEE, California
TOM COLE, Oklahoma	BETTY McCOLLUM, Minnesota
MARIO DIAZ-BALART, Florida	C. A. DUTCH RUPPERSBERGER, Maryland
STEVE WOMACK, Arkansas	DEBBIE WASSERMAN SCHULTZ, Florida
CHARLES J. "CHUCK" FLEISCHMANN, Tennessee	HENRY CUELLAR, Texas
DAVID P. JOYCE, Ohio	CHELLIE PINGREE, Maine
ANDY HARRIS, Maryland	MIKE QUIGLEY, Illinois
MARK E. AMODEI, Nevada	DEREK KILMER, Washington
CHRIS STEWART, Utah	MATT CARTWRIGHT, Pennsylvania
DAVID G. VALADAO, California	GRACE MENG, New York
DAN NEWHOUSE, Washington	MARK POCAN, Wisconsin
JOHN R. MOOLENAAR, Michigan	PETE AGUILAR, California
JOHN H. RUTHERFORD, Florida	LOIS FRANKEL, Florida
BEN CLINE, Virginia	BONNIE WATSON COLEMAN, New Jersey
GUY RESCHENTHALER, Pennsylvania	NORMA J. TORRES, California
MIKE GARCIA, California	ED CASE, Hawaii
ASHLEY HINSON, Iowa	ADRIANO ESPAILLAT, New York
TONY GONZALES, Texas	JOSH HARDER, California
JULIA LETLOW, Louisiana	JENNIFER WEXTON, Virginia
MICHAEL CLOUD, Texas	DAVID J. TRONE, Maryland
MICHAEL GUEST, Mississippi	LAUREN UNDERWOOD, Illinois
RYAN K. ZINKE, Montana	SUSIE LEE, Nevada
ANDREW S. CLYDE, Georgia	JOSEPH D. MORELLE, New York
JAKE LaTURNER, Kansas	
JERRY L. CARL, Alabama	
STEPHANIE I. BICE, Oklahoma	
C. SCOTT FRANKLIN, Florida	
JAKE ELLZEY, Texas	
JUAN CISCOMANI, Arizona	

ANNE MARIE CHOTVACS, *Clerk and Staff Director*

## **DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR 2024**

---

TUESDAY, MARCH 28, 2023.

### **CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY**

#### **WITNESS**

**HON. JEN EASTERLY, DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY**

Mr. JOYCE. The Subcommittee on Homeland Security will come to order.

I want to welcome everybody here today for the first subcommittee hearing of the 118th Congress.

Jen Easterly, welcome.

Ms. EASTERLY. Thank you, sir.

Mr. JOYCE. Ranking Member Mr. Cuellar.

Mr. CUELLAR. Mr. Chairman.

Mr. JOYCE. And I also want to welcome back Mr. Rutherford and Mrs. Hinson, who were here on the subcommittee last year. Dr. Harris and Mr. Newhouse have been on the Appropriations Committee for some time. We have two members in Mr. Guest and Mr. Cloud.

I look forward to working with everyone as we begin the fiscal 2024 appropriations cycle.

Thank you, Director, for joining us today. And I welcome to allow you to give your opening statement at this time.

#### **STATEMENT OF HON. JEN EASTERLY**

Ms. EASTERLY. Wonderful. Thank you so much.

Thanks to Chairman Joyce, Ranking Member Cuellar, and members of the subcommittee for the opportunity to testify regarding the fiscal year 2024 President's budget for CISA.

As the Nation's cyber defense agency and the national coordinator for critical infrastructure security and resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

And this mission has never been more urgent, as our Nation faces a wide array of threats that could undermine our national security, our economic prosperity, and our public health and safety, including the preeminent cyber threat we face from China.

I joined CISA nearly 2 years ago as the agency was still leading the national recovery from the widespread Russian cyber espionage campaign known as SolarWinds. In those dark days in the after-

math of intrusion into many of our government's most critical systems, we came to several realizations.

We realized our visibility into cyber threats and vulnerabilities was wildly incomplete. We realized our capability to ingest, analyze, and act upon cyber risk data was inadequate. And we realized that the breadth of the cyber threat facing our country required a new model of public-private partnership characterized by persistent operational collaboration.

Since that time, I am proud that Congress, the administration, CISA, and our partners have all stepped up to the challenge. And we have received sustained, generous, bipartisan investment from Congress and invaluable new authorities. And we have worked to be good stewards of this investment, executing 99.87 percent of our 1-year fiscal year 2022 funds.

This year's budget builds upon this progress, requesting \$3.1 billion for CISA, \$149 million more than what Congress appropriated to us in fiscal year 2023, reflecting the administration's commitment to our important mission in matching the strong and steady investment Congress has made in CISA, including in areas that we identified as essential in the aftermath of SolarWinds.

Specifically, we have made significant progress in expanding our visibility into cyber threats and vulnerabilities across the government and the private sector. Visibility is critical. If we can identify threats and vulnerabilities with speed and breadth, we can provide more support to victims, share more actionable info, and deliver more tailored guidance to reduce risk.

The resources requested will meaningfully advance this capability, first, by providing investments in the Continuous Diagnostics and Mitigation program, enabling greater real-time visibility into threats and vulnerabilities for every Federal civilian agency; second, by enabling us to modernize the array of cyber sensors to protect Federal agencies; third, by supporting the expansion of the CyberSentry program; and, finally, by allowing us to implement CIRCIA, the Cyber Incident Reporting for Critical Infrastructure Act, which Congress passed a year ago with broad, bipartisan support.

The budget provides \$97 million to ensure the staffing, processes, and technical capabilities to successfully implement CIRCIA and use incident reportings to limit the impact of cyber incidents targeting Americans.

As our visibility increases, our access to data increases, and our need to conduct big data analysis becomes increasingly acute. That is why we requested \$425 million for the Cyber Analysis and Data System, or CADS, to provide a modern, scalable, analytic infrastructure for our cyber operators. And CADS is a foundational step to building the joint collaborative environment that will enable collaborative analysis of cyber risk data across the government and private sector.

Now, at the same time, we can't do this alone. This is about collective cyber defense. We have to continue to bring together partners from government, the private sector, and the international community to address shared risks.

The budget sustains \$97 million for the JCDC, the Joint Cyber Defense Collaborative, the Nation's focal point for cyber defense



collaboration and planning. As we did in the lead-up to Russia's invasion of Ukraine, this will allow us to increase the number of cyber defense plans, expand persistent collaboration efforts, and improve our ability to conduct timely notifications of cyber threats before damaging incidents occur.

Of equal importance, we have to continue to grow and mature as a new agency in order to fully execute our essential mission. The budget consolidates mission support funding for dedicated efforts to secure our networks, to report with transparency, to acquire new technology, and to enable the continued growth of our workforce.

Over just the past 2 years, we have expanded our team by more than 560 people, hiring more than double the people in the last 2 years than we hired in the previous 2. And we project fiscal year 2023 will be our best hiring year yet. Our funding request is essential to sustaining this progress.

Before I close, I want to thank this committee. Because of your continued support and generosity, we have had a remarkable year, working in every State and territory to provide cyber and physical and chemical security assistance to our partners and dedicated support to public safety and emergency communications communities.

As one team unified behind our shared mission, we will continue to operate in an efficient and cost-effective manner. There is no shortage of work ahead of us, and I look forward to working with you during the appropriations cycle to continue strengthening CISA and, by extension, the security and resilience of our Nation's infrastructure.

Thank you. I look forward to your questions.  
[The information follows:]

Chairman Joyce, Ranking Member Cuellar, and Members of the Subcommittee, thank you for the opportunity to testify regarding the Fiscal Year (FY) 2024 President's Budget for the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The FY 2024 President's Budget of \$3.1 billion for CISA reflects our commitment to the broader DHS mission to safeguard our homeland, our values, and our way of life.

In today's interconnected society, our Nation faces a wide array of serious risks from many threats, all with the potential for significant consequences that can impact our critical national functions. These functions are built as "systems of systems" with complex designs, numerous interdependencies, and inherent risks. While this structure allows for significant gains in efficiency and productivity, it also allows opportunities for nation-state actors and criminals, foreign and domestic, to undermine our national security, economic prosperity, and public health and safety, creating cascading effects across our Nation.

As the Nation's cyber defense agency, CISA is charged with leading the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Securing our Nation's critical infrastructure is a shared responsibility requiring not just a whole-of-government, but a whole-of-Nation approach. CISA is only able to accomplish our mission by building collaborative, trusted partnerships across all levels and branches of government, the private sector, academia, and the international community. CISA's Joint Cyber Defense Collaborative (JCDC), for the first time, enables the government, the private sector, and U.S. international partners to come together to develop joint cyber defense plans and enable real-time information sharing.

As part of this mission, CISA plays two key operational roles. First, we are the operational lead for federal cybersecurity, charged with protecting and defending Federal Civilian Executive Branch (FCEB) networks (the ".gov"), in close partnership with the Office of Management and Budget, the Office of the National Cyber Director, and agency Chief Information Officers and Chief Information Security Officers. Second, we serve as the National Coordinator for critical infrastructure security and resilience, working with partners across government and industry to protect and defend the nation's critical infrastructure. In both roles, CISA leads incident response to significant cyber incidents in partnership with the Federal Bureau of Investigation (FBI) and the Intelligence Community.

I am truly honored to appear before this Committee today to discuss how the President's Budget for Fiscal year 2024 recognizes the criticality of our mission and provides CISA's exceptional workforce with the resources needed to achieve this mission. Since being sworn in as Director, I continue to be impressed with the talent, creativity, and enthusiasm of the dedicated CISA employees I am entrusted to lead. As I share with my team nearly every day, I have the best job in government.

#### **FY 2024 President's Budget: Priorities**

Looking forward into FY 2024, CISA will remain focused on strengthening our Nation's cyber and physical defenses. We will continue to work closely with our partners across every

level of government, in the private sector, and with local communities to protect our country's networks and critical infrastructure from malicious activity. We will continue to share timely and actionable information, intelligence, and guidance with our partners and the public to ensure they have the tools they need to keep our communities safe and secure and increase nationwide cybersecurity preparedness.

Building on the generous investments made by the Congress in FY 2023, the FY 2024 President's Budget provides the resources needed to continue these efforts. This budget represents a significant increased investment in CISA by the Biden Administration. The \$3.1 billion requested for CISA in FY 2024 provides approximately \$545.6 million or about 22% more than requested in FY 2023. The FY 2024 President's Budget recognizes the value of historical investments, and CISA's growing role in enhancing the security and resilience of our Nation, the work yet to be done, and confidence in our ability to execute.

The FY 2024 President's Budget continues to make critical investments in our mission enabling activities and functions that will mature the Agency and better support the execution of our operational capabilities. The Budget provides \$493.1 million for Mission Support. CISA's Mission Support program provides enterprise leadership, management, and business administrative services that sustain day-to-day management operations for the Agency. This is essential to ensure we can hire a diverse and talented workforce and execute our missions with the technology and speed that keep us ahead of our adversaries.

Included in the FY 2024 President's Budget Mission Support account is a transfer of \$191.7 million to centralize CISA Enterprise Wide Shared Services (EWSS) into the Mission Support PPA. This net zero transfer will allow for better management and greater transparency and oversight of the Mission Support requirements that sustain and support the whole CISA enterprise while providing the flexibility to address new and emerging threats that we may face.

In addition, the FY 2024 President's Budget includes \$97.7 million in funding to support work to implement the *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA). This funding will ensure CISA has the staffing, processes, and technology capabilities in place to successfully implement and utilize information provided through CIRCIA. The funding will support additional outreach efforts regarding the notice of public rulemaking and the planning efforts required to educate covered entities and CISA stakeholders on the cyber incident reporting requirements, reporting protocols, and reporting methods, as well as voluntary reporting options. In addition to the rulemaking process, this funding will ensure CISA can receive, manage, analyze, secure, and report on incidents reported under CIRCIA, maturing our current ability to receive and analyze incident reports, manage incidents, coordinate with and notify the interagency, and implement incident data protection functions required by CIRCIA, including additional staff to receive and route around-the-clock inbound reports.

### **Cybersecurity**

The Cybersecurity Division (CSD) spearheads the national effort to ensure the defense and resilience of cyberspace. The FY 2024 President's budget includes \$1.8 billion to build the national capacity to detect, defend against, and recover from, cyberattacks. CSD will continue working with federal partners to bolster their cybersecurity and incident response postures and

safeguard FCEB networks that support our nation's essential operations. CSD will also continue our critical work partnering with the private sector and State, Local, Territorial, and Tribal (SLTT) governments to detect and mitigate cyber threats and vulnerabilities before they become incidents.

The FY 2024 President's Budget initiates the Joint Collaborative Environment (JCE), which will enable CSD to develop an internal analytic environment that enables more efficient analysis of mission-relevant classified and unclassified data through automation and correlation to identify previously unidentified cybersecurity risks. The JCE enables CSD to fulfill its mission and better integrate cyber threat and vulnerability data across our federal, SLTT, and private sector stakeholders, and rapidly work with those stakeholders to reduce associated risk.

To effectively execute our role as the operational lead for federal civilian cybersecurity, CSD must maintain and advance our ability to actively detect threats targeting federal agencies and gain granular visibility into the security state of federal infrastructure. To effectuate these goals, the FY 2024 President's Budget request includes funding for the National Cybersecurity Protection System (NCPS) at \$67.4 million; and Cyber Analytics Data System (CADS) at \$424.9 million.

In FY 2024, portions of the NCPS will transition to the new CADS program with intrusion detection and intrusion prevention capabilities remaining under the legacy program. CADS will provide a robust and scalable analytic environment capable of integrating mission visibility data sets, visualization tools, and advanced analytic capabilities to cyber operators. CADS tools and capabilities will facilitate the ingestion and integration of data as well as orchestrate and automate analysis that supports the rapid identification, detection, mitigation, and prevention of malicious cyber activity.

Together with the Continuous Diagnostics and Mitigation (CDM) program, these programs provide the technological foundation to secure and defend federal civilian executive branch departments and agencies against advanced cyber threats. The FY 2024 President's Budget requests \$408.3 million for CDM. This investment in CDM enhances the overall security posture of FCEB networks by providing FCEB agencies and CISA's operators with the capability to identify, prioritize, and address cybersecurity threats and vulnerabilities, including through the deployment of Endpoint Detection and Response (EDR), cloud security capabilities, and network security controls.

The FY 2024 President's Budget also includes \$48.2 million for CyberSentry. CyberSentry is a voluntary partnership with private sector critical infrastructure operators designed to detect malicious activity on the Nation's highest-risk critical infrastructure networks. CyberSentry provides best-in-class commercial technologies that allow both CSD analysts and each partner organization to rapidly detect threats that attempt to move from an organization's business network to impact industrial control systems. While CyberSentry is intended only for the most at-risk or targeted critical infrastructure entities, the resources requested for FY 2024 will support growing CyberSentry operations and deploying capabilities to additional critical infrastructure partners to meet significant demand for the program based upon operational successes achieved to this point.

### **Integrated Operations**

The FY 2024 President's Budget includes \$244.5 million to enable seamless and timely support to CISA stakeholders across the nation, meeting our partners where they are in communities in every state. The Integrated Operations Division (IOD) coordinates CISA operations at the regional level and delivers CISA capabilities and services to support stakeholders in preparing for, mitigating, responding to, and recovering from incidents that impact critical infrastructure. Additionally, IOD includes monitoring and disseminating cyber and physical risk and threat information; providing intelligence context to support decision making; and performing Agency-designated Emergency Support Functions.

### **Infrastructure Security**

The FY 2024 President's Budget includes \$177.6 million for infrastructure security for CISA's efforts to enhance critical infrastructure protection through enabling risk-informed decision-making by owners and operators of critical infrastructure, as well as Federal and SLTT partners. To achieve this, CISA's Infrastructure Security Division (ISD) leads and coordinates national programs and policies on critical infrastructure security, including conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance. ISD's mission focuses on efforts such as reducing the risk of targeted violence directed at our Nation's schools, communities, houses of worship, and other public gathering locations. In addition, ISD leads programmatic efforts to secure our Nation's chemical infrastructure through implementation of the Chemical Facility Anti-Terrorism Standards (CFATS) regulation.

### **Emergency Communications**

The FY 2024 President's Budget includes \$126.6 million for emergency communications to ensure interoperability and to assist and support Federal and SLTT stakeholders. CISA's Emergency Communications Division (ECD) enhances public safety communications at all levels of government across the country through training, coordination, tools, and guidance. ECD leads the development of the National Emergency Communications Plan (NECP) and 56 Statewide Communications Interoperability Plans to maximize the use of all communications capabilities—voice, video, and data—available to emergency responders and ensure the security of data exchange. ECD also assists local emergency responders to communicate over commercial networks during natural disasters, acts of terrorism, and other significant disruptive events. As directed by statute, the Emergency Communications program supports nationwide sharing of best practices and lessons learned through facilitation of SAFECOM and Emergency Communications Preparedness Center governance bodies.

### **Stakeholder Engagement**

The FY 2024 President's Budget includes \$85.5 million for CISA Stakeholder Engagement Division (SED) activities focused on fostering collaboration, coordination, and a culture of shared responsibility for national critical infrastructure risk management with Federal, SLTT, and private sector partners in the United States, as well as international partners. With this funding, SED will continue to execute CISA's roles and functions as the Sector Risk

Management Agency (SRMA) for eight of the Nation's 16 critical infrastructure sectors and will lead coordination with SRMAs, with the broader national voluntary critical infrastructure partnership community, and across all sectors to ensure the timely exchange of information and best practices. In partnership with the Federal Emergency Management Agency (FEMA), SED will continue implementing the State and Local Cybersecurity Grant Program, including providing subject matter expertise and leading program evaluation efforts to ensure state and local entities can access grant resources to enhance cybersecurity resiliency and reduce cybersecurity risk. Additionally, in partnership with FEMA, SED will develop and implement the proposed Critical Infrastructure Grant program to complement our efforts to build sustainable cybersecurity while protecting the Nation's most vital critical infrastructure by shoring up the cyber defenses of those small, discrete, resource poor component level suppliers that provide irreplaceable supplies or services to systemically important entities.

#### **National Risk Management Center**

Finally, the FY 2024 President's Budget includes \$144.5 million for the National Risk Management Center (NRMC). NRMC develops analytic insights to identify and advance risk mitigation opportunities that improve national security and resiliency across critical infrastructure sectors. These analytic products support investment and operational decision making throughout the public and private sectors.

The FY 2024 President's Budget continues two critical efforts housed within NRMC related to SRMAs and National Critical Function (NCF) Analytics. First, funding will allow us to continue efforts to expand risk analysis and risk management across high priority critical infrastructure sectors. This risk analysis provides insight into cross-sectoral risk and significant sector-specific risks to support CISA in routinely identifying and prioritizing focused risk management opportunities to create tangible risk reduction outcomes.

Second, the FY 2024 President's Budget provides funding to continue our NCF efforts to enhance analytic capabilities, including methodology and framework development to identify and characterize critical infrastructure interdependencies within and across NCFs. This includes applied analysis to meet specific analytic requirements in the infrastructure community to enable CISA to understand consequences that extend beyond a single sector.

#### **Conclusion**

I am honored to represent my dedicated teammates at CISA who work tirelessly in support of our mission to understand, manage, and reduce risk to our cyber and physical infrastructure. The risks we face are complex, geographically dispersed, and affect a diverse array of our stakeholders, including federal civilian government agencies, private sector companies, SLTT governments, and ultimately the American people. The FY 2024 President's Budget requests the funding necessary for CISA to carry out these critical mission imperatives.

Before I close, I would like to take a moment to recognize this Committee's strong support for CISA. For myself, and on behalf of our CISA workforce, thank you for your support. As one team unified behind our shared mission, we will continue to operate in an

efficient and cost-effective manner. There is much work to be done and I look forward to working with you during the FY 2024 appropriations cycle to continue strengthening this Agency, and by extension, the security and resilience of our Nation's networks and critical infrastructure.

Thank you for the opportunity to appear before you today, and I look forward to your questions.

Mr. JOYCE. Thank you very much, Director Easterly.

And I wanted to get that out there ahead of time because some of us—this is the kickoff of the season for us in Appropriations, and so members may come and go, but I know they all wanted to hear your opening statement. And so, if they come and go, it is not meant to be disrespectful; they are just trying to attend other hearings at the same time.

And I truly thank you for your military service as well as your leadership here today.

In 2018, Congress authorized CISA to protect the Nation's cyber and physical critical infrastructure. We invested heavily in the operational agency and its mission over the last 3 years, increasing the budget by 44 percent, from \$2 billion to \$2.9 billion.

The President's latest request will put you over \$3 billion. That is a fair amount of dollars. Today, I would like to drill down and quantify the return on that investment for the American people, as CISA's mission has never been more important.

Nation-state actors backed by China, Russia, North Korea, Iran, and others are targeting government and private-sector networks to steal intellectual property, probe our defense, disrupt operations, cause panic, and inflict financial consequences on the homeland.

Simultaneously, cyber criminals are using ransomware to prey on vulnerable groups, including schools, local governments, and hospitals, for financial gain. These attacks can cost millions of dollars when a ransom is paid and also create additional costs from lost productivity and disrupted operations.

CISA is charged with coordinating the defense of 16 critical infrastructure sectors, including energy, healthcare, manufacturing, transportation, communications, and the defense industrial base, among with others.

We all remember the Colonial Pipeline, as you brought up, the ransomware attack that disrupted the flow of fuel to a large portion of our country, resulting in nearly \$5 million in damages. Imagine the impact of a coordinated, larger-scale attack, akin to the Nord Stream pipeline attack in the Baltic Sea last fall.

Increased vigilance on both the cyber and physical infrastructure front is critical to ensuring both our national and economic security and public trust. I look forward to hearing how CISA is leveraging its resources to harden our defenses against adversarial nation-state-sponsored threat actors, cyber criminals, and other nefarious actors.

But not all challenges CISA face are external. The rapid growth of the agency over the past 3 years brought hiring challenges, management and communication difficulties, and organizational growing pains. Without the right people, CISA cannot fully carry out its mission, regardless of its investment.

With the private sector also competing for cyber talent, I am interested to hear how you are attracting, hiring, developing, and retaining employees. As the country faces continually evolving threats, our workforce, too, must evolve. Rapid technological developments will continue to dramatically change network security, and CISA will need personnel with the right tools, training, and tenacity to meet those critical networks.



I look forward to a robust discussion today and working together to make sure we see the results from our significant investment in CISA.

I will turn to my colleague, Mr. Cuellar, for any opening remarks he may have.

Mr. CUELLAR. Thank you, Mr. Chairman. And, again, I congratulate you on your new role as chairman.

And I certainly welcome the new members both on—the committee itself, so I want to say, first of all, congratulations.

And, again, as you know, we do have a few members that are coming back. I know Ms. Lauren Underwood, Illinois, welcome back, because she has been on the committee, and appreciate all the good work.

And we got two new Democratic members, Congressman David Trone of Maryland—again, we welcome you and all the work that you are doing on fentanyl and other work like that—and then Mr. Ed Case will be joining us also.

So, again, good morning, Director Easterly. It is good to see you again. I am still very impressed—there is a story of why I have this—very impressed not only by your talents but by the work that you are doing.

As we all know, cyber threats pose a significant risk to our national security, our economy, and our way of life. These threats are posed by individual bad actors, transnational criminal organizations, foreign adversaries like state-sponsored groups and nations.

CISA plays a vital role in partnering with other Federal agencies, State and local governments, critical infrastructure owners and operators who protect against emerging and evolving threats.

Again, we appreciate your leadership. And at this, I will go ahead, because I do want to start into questions, but I do appreciate, Director Easterly, all the work that you are doing.

Mr. JOYCE. Thank you.

And your statement will be entered into the record.

I want to start on the return on investment that we discussed. As I mentioned in my remarks, Congress provided CISA with substantial increases in funding over the last 3 fiscal years due to the importance of the mission. I would like to drill down on the specific return on that investment for the American people. This in addition to the more than \$780 million provided through the American Rescue Plan and infrastructure law last Congress.

Director, can you quantify for the subcommittee how much safer the homeland is today than it was before these funding enhancements for CISA? And specifically in both the cybersecurity and infrastructure security buckets, how do you measure success?

Ms. EASTERLY. Thanks very much for asking that question.

You know, when I came to CISA, our mission was to lead the national effort to understand and manage risk. And we actually changed the mission statement to say that we were leading and managing and reducing risk, recognizing that we have to be able to measure and quantify those investments.

That said, Chairman, that is a very difficult thing to do, so we are starting on this journey about how we actually measure not only things, activities, or performance, but actually how we measure effectiveness.

So, for example, one of the things that we are very focused on, given the incredible investments that we have gotten from Congress after the SolarWinds incident, as I mentioned, through the Rescue Plan Act as well as our budget later this year, were investments designed to increase our visibility on the Federal civilian executive branch network, so the dot-gov, because, effectively, we saw that we were blind.

So many of the new authorities and the money that we were given allowed us to instantiate technology that we call EDR, end-point detection and response capabilities, across the dot-gov that allows us now to do persistent hunting based on new authorities that we have been given so that we have much more visibility to be able to say, we are seeing malicious activity on those networks. And we do this, obviously, in concert with Federal agencies.

It enables us to say, there is risky technology, like, for example, TikTok, on Federal Government devices, or risky technology from foreign adversaries on some of our technology. It also allows us to understand if there are vulnerabilities that need to be remediated.

But actually measuring that is a challenge. But I want to read you some of the things that we are specifically focused on here.

Percentage of Federal agencies that are sharing current and accurate data through our CDM Dashboard. So now we have a way to actually look across the dot-gov to see what agencies have what risk teed up to us.

Percentage that have developed internal vulnerability management and patching of vulnerability disclosure policy, end-of-life service and end-of-service policy; voluntary adoptions of our shared services, like protective domain name systems that allows us to see malicious traffic transiting the internet; and then, finally, that percentage that is covered by that EDR technology.

So we are, again, looking to measure aspects of instantiation of capabilities. What we hope to be able to get at the end of the full maturation—and much of our budget is focused on maturation—is actually showing the number of incidents that will be reduced.

And then the last thing I would say here, sir: As a measure of reducing risk, we don't have a lot of visibility into the overall ecosystem, but you all gave us CIRCIA last year, the Cyber Incident Reporting for Critical Infrastructure Act. That will be game-changing in allowing us to actually understand the ecosystem so we can say, here are the number of critical incidents that occurred across our critical infrastructure this year. And then we can measure the reduction given all of these improvements that we have put in place.

So we are on our journey to be able to give you very quantifiable metrics to allow us to articulate that return on investment.

Mr. JOYCE. Thank you, Director.

I am going to ask you to think about the funds CISA receives. Which are the most critical for deterring and preventing attacks on the homeland?

Ms. EASTERLY. Well, as we had to make hard choices in our budget this year, sir, you saw that we are putting new moneys—we are requesting new moneys in the budget to focus on these cyber threats.

We have built out capabilities over the past 20 years for integrated security across physical security, but where we are seeing threats from nation-states—China, as I mentioned, the preeminent; Russia, very focused on that with our Shields Up campaign; Iran; North Korea—and cyber criminals, we have seen ransomware as a scourge on schools, on municipalities, on hospitals, and we really want to drive down that risk there.

So some of the investments that we are making are focused on our field forces, which are working with State and local and with smaller infrastructure to be able to drive down risk on those entities. But the big-ticket items are really around CIRCIA so that we have the staff, the processes, and technical infrastructure to be able to receive reports, to triage them, and to respond to them so we can drive down risk to the Nation.

The other big investments have to do with the Federal civilian enterprise, where we play the role as operational lead for Federal cyber security. So the CADS system, the Cyber Analytic and Data System. Essentially we have been bringing in a lot more data, but we have to have a system to provide us cyber analytics to integrate, to enrich, to correlate it, so we can make use and make sense of that data to drive down risk.

And then, finally, some of the maturation around our Continuous Diagnostics and Mitigation team, which is really the foundational system for cybersecurity. And part of that is the maturation of the National Cyber Protection System, some of the things that we are doing with EINSTEIN.

So these investments are critical to actually take advantage of the investments that you have given us, because it really is an evolution of maturity. To get there, we have to be able to evolve with these new systems—in particular, the analytics.

Mr. JOYCE. Thank you very much, Director.

I now recognize our ranking member, Mr. Cuellar.

Mr. CUELLAR. Thank you, Mr. Chairman.

I also want to follow the line of questioning that the chairman brought up.

Back in 2010, I changed legislation that modernized the performance, results-oriented government legislation that got passed in the 1990s. And in there, in the 2010 legislation, we are asking agencies to make sure they have their mission statement, their objectives, key performance measures, which are some of the ones I have here. And I will be asking every agency before our committee about their performance measures.

And I have looked at some of the key performance measures, which are the big ones. And, again, I am not blaming you, but I—this has probably been in place for a while.

But one of the things, Members, that we need to realize, that in the State—and I was asking who has been in the State legislature, because in the State legislatures we use a lot of the performance measures, and it is a different process. And I was trying to do this in 2010. It is a little different in D.C., trying to change things. But, here, we leave agencies to develop their own performance measures. In State legislatures, I think in most State legislatures, the Congress or the legislature and the agencies actually sit down and agree on certain measures.

Because, for example, one of the key measures that you have here, or that the agency has, that is supposed to be a key measure is—"Key Measure: Landline priority call successfully connected." So is that important? Is that a key measure that we ought to be looking at? Or should we come up with—instead of measuring activity, we ought to measure results? If we put in \$1, what is the bang for that \$1?

And I am hoping that somewhere down the line we all can get involved, where we can have certain measures that we can negotiate, if I can use that term, or work out with you, and hopefully be part of the report language where we can actually look at the measures.

Because, right now, all of this are on websites. And I don't know if you look at every website out there. And I think this is what the chairman was saying—and I am in agreement with him—that if we put in money, what are we getting for that \$1?

For example, as the chairman mentioned, back in December 2020, we added \$650 million in supplemental funding to CISA through the American Rescue Plan Act to increase and enhance, you know, the work that you are doing. And the question is, as the chairman asked: So, given all that investment, plus other moneys that the chairman mentioned, describe how CISA is better positioned than it was in 2020 to protect against a response to cybersecurity attacks.

And one of the ways we could look at is the performance measures. But if we are looking at—and I don't want to go through all of them—but if we are looking at how many landline calls did you connect, I don't think that is the best measure to look at.

So we are hoping, one is, if you can answer the question, with all that investment, specifically, how are you in a better position now to protect the public? But I am hoping that we can look at and ask Members to start looking at every agency, we put in \$1, what is the bang? Not measure activity. I don't want to count how many pencils we have out there. I want to see results on that.

Ms. EASTERLY. Yeah. Hundred percent. And I think you have seen our strategic plan as well—

Mr. CUELLAR. Yes.

Ms. EASTERLY [continuing]. Where we have representative outcomes that are about outcomes, not activities, right? Measures of effectiveness, not measures of performance.

This is the agency's strategic plan, but every one of my divisions and mission-enabling offices has annual operating plans that then spreads out in more detail what we are looking to achieve. And I would love for us to come back to this committee to be able to talk to you, to get your guidance and counsel about what you would like to see.

I think we are moving in the right direction on this.

I had this same challenge when I was in the private sector, at Morgan Stanley, where we were putting hundreds of millions of dollars into the cybersecurity program and return of investment was things not happening. So, you know, at a broad level, bad things not happening is hard to measure.

So what we want to do is get more granular with the visibility that we have gotten out of that \$650 million to say, this is how we

have reduced the instance of bad things happening; and better metrics for things like, how have we recovered most effectively? How have we reduced our time to actually detect something and then to respond to it and recover from it? And that is the direction we are going in with metrics.

So I would love to spend more time on a deep dive with you on that.

Mr. CUELLAR. Thank you so much.

Thank you, Mr. Chairman.

Mr. JOYCE. Thank you, Mr. Cuellar.

I recognize Sheriff Rutherford for 5 minutes.

Mr. RUTHERFORD. Thank you, Mr. Chairman.

Director, it is really great to see you again.

And I would be remiss if I didn't thank you all, first and foremost, for the visit to the district that we had. I think building those local relationships is huge, and I know you are working hard on that. It was very well received by my community, so thank you.

Ms. EASTERLY. Thank you, sir.

Mr. RUTHERFORD. And I want to kind of follow up on the line of questioning so far in talking about CIRCIA.

So we are requiring the critical infrastructure to report. First of all, I know it has only been a year, but how has that been received? Are we getting the reporting that you think we should? Can you just give me an idea of how that is rolling out?

Ms. EASTERLY. Yeah, absolutely. Thank you for asking, because I think this is one of the most important things that has been happening—that happened legislatively since probably the establishment of CISA in 2018.

So, as you know, we are largely a voluntary agency. So I do want to thank you for hosting that meeting with my team. They loved it. And they love to spend time with constituents in the field. So I would ask any of you who wants to meet with our CISA team, please do so. Because that is where the rubber meets the road, right?

Mr. RUTHERFORD. Uh-huh.

Ms. EASTERLY. So, with CIRCIA, we are in a rulemaking process, sir. So we have been working over the past year to essentially put the infrastructure in place so that we can start defining what we need to receive from the private sector within 72 hours, how we define a covered entity, how we define a covered incident. And we are moving forward to actually create the notice of rulemaking, which should come out in March of next year, and then look for the final rule, which will be implemented in September of 2025.

We have worked really hard to make this a consultative process. Having come from a highly regulated industry in finance, I am very, very sensitive to not creating chaos when there are all kinds of regulations that are out there. We want to do this in a way that allows us to render assistance to the victim and then drive down risk to the Nation.

So we had 27 sessions—10 in person, 17 virtual—where we talked to the private sector to get their feedback. We did a request for information where we got over 100 comments back. So we are putting together that rule based on everything we have heard from

the private sector. That is hugely important to make sure that we do this right.

The other important thing is to ensure that this is harmonized. What we can't have is a bunch of different agencies asking slightly different questions to the private sector, because all we are going to create is chaos.

Mr. RUTHERFORD. Right.

Ms. EASTERLY. Then it becomes a box-checking compliance exercise, not about reducing risk to the Nation. So we are very mindful of leveraging the Cyber Incident Reporting Council that was in CIRCIA.

The other things with CIRCIA which we are already getting after are the Joint Ransomware Task Force to help reduce risk to the Nation through our Ransomware Vulnerability Warning Pilot that was mandated in the legislation, as well as our pre-notification of ransomware incidents that is driving down impact across the country.

So legislation moving forward, sir. We are being consultative about it.

But the additional moneys we asked for was really about putting the technical infrastructure in place to allow us to be able to receive this massive amount of new reporting, to analyze it, to correlate it, to enrich it, and then to use it to respond, but really to reduce risk to other sectors in the rest of the Nation.

Mr. RUTHERFORD. Good.

And you have subpoena power if they do not report. My question, though, is, is there any teeth behind that?

Because, you know, from experience, I think we see that there is quite a lot of reluctance for some of these organizations, maybe not in the critical infrastructure when it is governmental, but others—there is a lack of openness, I think, in wanting to lay out their problems.

Ms. EASTERLY. Yeah.

Mr. RUTHERFORD. Do we need to put more teeth into the reporting piece? Because I really don't see any teeth in that.

Ms. EASTERLY. Yeah. You are right. I think this was a hard-fought set of legislation, and a lot of views came in from the private sector. So there are not a lot of sticks, in terms of enforcement and compliance. If, in fact, we hear of an incident and it is not reported to us, we can use admin subpoena power.

You know, what I would say, though, is, we need a cultural transformation, frankly, in order for us to have a sustainable approach to cybersecurity. This has to be about collaboration over self-preservation.

I know that companies—because I was in one of them—worry about their reputation, they worry about their stock price. But, at the end of the day, the reporting came to CISA because we have the most robust authorities for information-sharing and protection of data.

We are not here to name, to shame, to stab the wounded.

Mr. RUTHERFORD. Right.

Ms. EASTERLY. We are here to render assistance and then to use that data, very importantly, to protect the rest of the ecosystem.

If you are in a neighborhood and your neighbor gets robbed, you are going to want to know that, so you can actually lock your doors and put your guard dog out. It is important for our collective defense.

We are facing some very, very serious threats to our Nation, to our critical infrastructure. If we don't work together to put collaboration over self-preservation and make sure that we are connected in this highly connected ecosystem, that we are not looking out to protect the Nation, we will fail.

So I am very much hoping that we are going to get the reports that we have asked for. And, quite frankly, sir, as part of our Shields Up campaign, we actually asked entities to reduce their threshold and voluntarily report to us. And we got in a ton of reports about potential scanning and activities.

So I am optimistic, as I always am, about the successful implementation of the legislation.

Mr. RUTHERFORD. Thank you very much.

And I see my time has expired. I yield back, but I will say, Mr. Chairman, we may need to look at some teeth. We will see how it goes.

Thank you.

Ms. EASTERLY. Yes, sir.

Mr. JOYCE. Thank you, Sheriff.

Ms. Underwood

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Director Easterly, thanks for being with us. It is good to see you again.

Ms. EASTERLY. You too, ma'am.

Ms. UNDERWOOD. First, I want to talk about election security, which is a critical pillar of our national security.

Over the past several elections, we have seen foreign adversaries, like Russia and Iran, deploy more sophisticated and brazen campaigns in attempts to influence and interfere with our elections.

And, most recently, in our 2022 midterm elections, we saw China using fake social media accounts with the goal of sowing distrust into our elections, something analysts noticed was a shift in strategy for China.

Director Easterly, can you tell us more about emerging threats and trends you are seeing recently when it comes to foreign attempts at election interference and from China in particular?

Ms. EASTERLY. Yeah, absolutely. Thank you for the question.

Just to level-set, as you know, we were designated in 2017 as the sector risk management agency. So we don't, obviously, run elections. We make sure that State and local election officials have the resources——

Ms. UNDERWOOD. Correct.

Ms. EASTERLY [continuing]. The capability, and the intelligence that they need.

And 2022 was my first election with these local officials. I will tell you, when we were first designated, there was massive pushback. They didn't want anything to do with the Federal Government. But through years and years of building partnerships, that is very solid now.

And what I hear from State and local election officials is that they are increasingly asking for more of our resources. In fact, we——

Ms. UNDERWOOD. Director——

Ms. EASTERLY [continuing]. Just met with——

Ms. UNDERWOOD. I am sorry, Director. I asked about the——

Ms. EASTERLY. Yes, ma'am.

Ms. UNDERWOOD [continuing]. Threats from China.

Ms. EASTERLY. So what they are telling us and what we are seeing, very complicated threat environment. Cyber threats from nation-state actors; physical threats to polling places, to election officials; insider threats; and then the threats of foreign influence and disinformation. As you mentioned, we saw it from Russia. We saw it from Iran in 2020. We saw it in China.

I have serious concerns, particularly given some of the capabilities that China has, like TikTok, to be able to use their data, the data that they have collected from us, capabilities, to be able to influence the American public.

So we are working very hard to make sure that we are amplifying the trusted voices of local officials, putting out election literacy information, and then providing them all the resources that they need, so that American people can have confidence in the integrity of their elections.

Ms. UNDERWOOD. Great.

Next, I want to talk about who the burden of cybersecurity generally falls on, because, frankly, I think our approach is backwards.

You and I have compared cybersecurity to auto safety. If a car today didn't have seatbelts or if an airbag didn't deploy, we wouldn't blame the driver; we would hold the auto manufacturer accountable. Cars undergo rigorous safety and crash tests before they can be sold to consumers. And roadways, themselves, have speed limits and traffic lights, all to ensure the end user is as safe as possible while driving.

Cybersecurity products should be treated the same way. But, in our current system, we leave individuals with no choice but to shoulder cyber risks and consequences, instead of the technology providers, who have more of the resources, capacity, and visibility to protect consumers from those risks in the first place. This model is not safe, sensible, or sustainable.

So, Director Easterly, how can we, as policymakers, help shift the burden away from the end user? And what does a more sustainable cyber model look like? And how is CISA helping getting us there?

Ms. EASTERLY. Thank you, thank you for asking that question, because I 100 percent agree with you. We are not in a sustainable place.

So, as you said, what we need to make sure is that we change the incentives. We have normalized a world where technology comes to us inherently unsafe, and then we developed a multibillion-dollar cyber security industry to basically deal with the fact that we are all walking around with unsafe technology.

So we have to change the incentives. Right now, the incentives are all about speed to market and competing on features and cost



reduction. We have to make safety baked in, and we have to make products safe by design.

We have asked for radical transparency so that we understand that consumers—so the burden isn't placed on them, so they know what they are buying. We have asked for technology providers to bake in security and to design in security. And, as the National Cybersecurity Strategy suggested, ma'am, we may need to look at certain liability for whether manufacturers have duty of care to be able to protect those consumers.

I realize this may be a long time coming. It was 1965 when Ralph Nader wrote "Unsafe At Any Speed" and 1983 when we had seatbelt legislation. But we absolutely have to get there. Take the burden off small businesses, take the burden off consumers, and push it on those most capable of bearing it.

Ms. UNDERWOOD. And I think that CISA is well-equipped to help lead that charge forward, as we work to make sure that we have robust protections for everybody, including the end user.

Director Easterly, thanks so much for appearing before our committee today.

I yield back.

Ms. EASTERLY. Thank you, ma'am.

Mr. JOYCE. Thank you very much, Ms. Underwood.

I recognize Mr. Newhouse for any comments he may have or questions.

Mr. NEWHOUSE. Thank you, Chairman Joyce.

Ranking Member, also, thank you very much.

Director, thanks for being with us today.

Ms. EASTERLY. Sir.

Mr. NEWHOUSE. So I come from the State of Washington, and we have had, it seems like, more than our fair share of issues on some of our local and, I believe, locally owned State and Federal power to substations.

Ms. EASTERLY. Yes.

Mr. NEWHOUSE. It has gotten a lot of press recently.

I had served on this committee prior to my term now, and I asked people, your predecessors, about the security of our grid and are we keeping up security protocols at the national, Federal level. So let me ask you about some of these 16 critical areas that you are responsible for.

Could you talk to me about CISA's Energy Sector-Specific Plan, the SSP?

And don't get me wrong here; I know cyber is vitally important. And, in fact, some of the briefings I have had keep me up at night, worrying about some of these things. But have we focused on cyber at the expense of some of our physical security? I know it is a balance.

In the coming budget year, do you think there is a need to update the sector-specific plans? The energy plan, for instance, hasn't been updated, I believe, since 2015. And you can update me on that if that isn't correct.

Should we revisit the National Infrastructure Protection Plan as well? I do have some concerns because the President's budget looks, to me, to be proposing a decrease in the overall infrastructure security account.

So just a rhetorical question: If we can't secure our physical assets here at home, how do we tackle cybersecurity and safeguard those new technologies that are coming, like fusion, the hydrogen, the small modular reactors? It seems to me we have to be able to do both.

So, your response?

Ms. EASTERLY. I 100 percent agree with you, which is why our mission is to reduce risk to cyber and physical infrastructure.

So, you know, in addition to being America's cyber defense agency, we serve as the national coordinator for critical infrastructure resilience and security. And that was what was in the statute.

So the SRMAs for the 16 sectors, we actually serve as 8, for 8 sectors, but there are other departments and agencies that serve—say, for energy, electricity, it is the Department of Energy.

And so our role is to work hand-in-hand with the sector risk management agencies who are responsible for updating those sector-specific plans to ensure that we are taking a cross-sector, coordinated approach to driving down both physical and cyber risk to the most systemically important entities.

So that is why Congress had the insight to have a coordinator role. Because it used to just be various sectors operating in silos. And so now bringing that together, knowing the dependencies are so important.

So, with respect to sector plans, the plan was to do the National Infrastructure Plan update. We are responsible for that. But we have been asked to first get done PPD-21. The White House is working on an update to the critical infrastructure Presidential Policy Directive. We will then do the national plan. And then the sector-specific plans will follow, to include the ones, the eight, that we are responsible for, as well as the elections subsector.

To your point on physical, the President's request in 2024 was actually the same as the request in 2023. The Congress generously gave us plus-ups on the physical security side in 2023. We didn't annualize them, sir, because we had to make tough decisions and we wanted to double-down on our investments in cyber given that threat.

All that said, we are continuing to do our work around school safety—more important than ever given the tragic events yesterday in Nashville—our work around the Office of Bombing Prevention, and all of the work we do on the physical security side.

But one of the things that we have recognized is, we can't look at these as separate things. There is the convergence of cyber and physical threats, so the convergence of cyber threats to physical buildings. We have to look at these in a converged way, which is why we are building out an integrated security model in the field, where our physical security advisors and our cybersecurity advisors look at these things together so we can maximally reduce risk to our national infrastructure.

Mr. NEWHOUSE. So you brought that up. Let me just ask you to delve into that just a little bit deeper in the seconds I have left.

It looks to me like there is a reduction in the security programs that would primarily benefit the K-12 school system.

Ms. EASTERLY. The \$3 million that was plussed up in 2023 by the Congress, sir?

Mr. NEWHOUSE. Well, the request is \$11.8 million less than the prior fiscal year, so just looking at the chart that you provided.

Ms. EASTERLY. Yes, sir. Let me follow up with you. That program is not hugely funded, so I think it was just \$3 million that was decremented. That is what I have in my notes. But happy to follow up.

And, again, we can always do more with more. So, if the Congress wants to put back that specific money that is all about creating safety for schools, we would certainly take advantage of it.

Mr. NEWHOUSE. OK. All right. Thank you very much.

Ms. EASTERLY. Yes, sir.

Mr. NEWHOUSE. Again, thanks for being here.

Ms. EASTERLY. My pleasure.

Mr. NEWHOUSE. I yield back, Mr. Chairman.

Mr. JOYCE. Thank you, Mr. Newhouse.

Mr. Trone, you are recognized for 5 minutes.

Mr. TRONE. Thank you, Mr. Chairman and Ranking Member Cuellar. I just want to say it is a pleasure to be here on this subcommittee, and you folks always work well together. You are totally bipartisan, and I just love the atmosphere that that generates. So thank you for having us here.

Director Easterly, we had a wonderful meeting, and you were most helpful and answered a bucketload of questions. And I can't thank you enough for going back to public service and leaving the corporate world. And you left all the money behind to be here for this. God bless you.

Ms. EASTERLY. Thank you, sir.

Mr. TRONE. The cyber area. As a businessperson, you know, all my life, I just checked with my CIO and asked him, how many hits do we get on our small company literally every day? And he said, over 150 from nation-states and actors mostly over in western Europe. So a company that doesn't even trade in anything of national security, we are getting hits all the time.

I look at Maryland and all these mom-and-pop businesses that can't afford the cyber infrastructure that I put in my company—which is basically, whatever those guys need, we get them. Because if we don't get it right in cyber, we are done. And it is just that simple.

But in Maryland there were 340 breaches last year. So Maryland was the fifth worst in the country on breaches. So business really needs the help.

And what Ms. Underwood talked about was, the products themselves don't come out safe. So we are certainly supportive of that point. I think that is a great point. But things not happening is the key, and it is hard to measure.

But tell me, for businesses looking to take their cybersecurity program up to the next level, how is there a best way to connect with CISA and stay up to date on the latest threats? Because the problem is, they don't stay up to date; then they are vulnerable.

Ms. EASTERLY. Yeah, 100 percent. Thank you for the question on that.

And thank you, also, for your leadership, because one of the things, to get to the point we were talking about on sustainable cybersecurity, is corporate cyber responsibility. We need CEOs and

leaders to actually put the resources that they need into their cybersecurity and to really empower and resource their CIOs and CISOs. That is what everybody needs to be doing, just as you are, sir. So thank you.

On small businesses in particular, right—33 million, 99.9 percent, median size is between 10 and 20 people, I think—they just don't have those resources. So we have provided, actually, a—we did last year—the Cybersecurity Action Plan. And we provided a kit for, what are those easy things that can be done?

And you can reach out and look—you can actually sign up for all of our products, our advisories and our alerts. You can take advantage of the kit, if you are a small business, on those basic steps that you can do. We have put out cybersecurity performance goals that are on our website that are basically breaking it down to, what are the top things you need to do, by cost complexity and impact, to drive down risk?

And then we have a field force, a growing field force of cybersecurity advisors, cybersecurity State coordinators, who are there to help, advise, provide assistance, and provide a massive amount of free services, government and industry, to help drive down risk.

So we recognize how important that is for some of the smaller businesses, particularly because some of these small and medium enterprises are in our supply chain in critical infrastructure. So we have to work together collectively to take responsibility as a Nation to drive down risk.

Mr. TRONE. That is a great idea. We are certainly going to get back to you and figure how to get that stuff out to our chambers of commerce, our rotaries. Because these folks are just—they are helpless. And they get hit, they get ransomware, they get shut down, and they can't absorb it. They have no resiliency.

Ms. EASTERLY. Yes, sir.

Mr. TRONE. So thank you for that, and I want to follow up.

Next quick question was: To run a business or run any organization, you have to have enough people and the right people. And that is where we get back to, you know, your situation on personnel, because it is so hard to find the talent in this area across the country.

So you set up—Homeland Security launched the Cyber Talent Management System back in November of 2021 to recruit, retain personnel. And the process has been tedious and difficult, and I understand that.

So how does the fiscal year 2024 request support the agency's recruitment and workforce goals, including the continued implementation of the Cyber Talent Management Program?

Ms. EASTERLY. Yeah. Thanks so much for asking.

Since I got here, day one, in July of 2021, we have made hiring a top priority here, to include using some of those new authorities for the Cyber Talent Management System. By the end of 2021, we had hired 200 more people than we hired the year before. 2022, more than 2021. 2023, we are on track to hire 600 people using those new authorities, but using a full range of other authorities to enable us to be able to more quickly recruit people and then to bring them into a culture where they feel like they can make impact.

As you well know, as somebody who has run a business for a long time, sir, we are not paying a big salary, right? People come here because of mission. We are looking for people who want a purposeful mission, who want a culture of collaboration and innovation, who want an environment that combines the entrepreneurialism of a start-up with the stability of a Federal job. And so those are the kinds of people that we have been able to tap into across the country.

As I said, 516 people last year. 600 people. We are going be down to—at the end of 2024, we are going to be down to less than 8 percent vacancies.

And so we are maximizing everything we can do to be more agile, to be more effective, and to drive down those vacancies in our workforce, and to keep attrition low, which is about 8 percent. But, you know, not all attrition is regretted. And so there is a natural flow, as you know from a business world, that people should go out and do other things if they are not the right fit for defending the Nation.

Mr. TRONE. Well, thank you very much for those answers. And I think this committee unanimously supports the importance of cyber. And it would be a fool's errand to cut that, just inviting China, inviting Russia and the other nation-states to devastate our small businesses around the country.

So thank you.

And I yield back.

Ms. EASTERLY. Thank you, sir.

Mr. JOYCE. Thank you, Mr. Trone.

Dr. Harris.

Mr. HARRIS. Thank you very much.

And thank you very much for being here with us today.

Let me just ask, one thing that we have seen kind of pervasive through the administration is spending money outside for purposes that, I will say, don't directly support your mission or the mission of any agency. Your mission is cybersecurity.

So I want to know how much you spend on DEI, because I think that distracts from your mission. I think that the SVB bank collapse shows in spades how distractions on things like DEI distract from what a regulator or a watchdog should be doing. So what part of your budget is spent on DEI?

Ms. EASTERLY. We don't break it down by diversity, equity, and inclusion—

Mr. HARRIS. Can you do that for me and get that figure to me? I mean, you have a DEI officer in your—

Ms. EASTERLY. We do. We do have an Office of DEIA—

Mr. HARRIS. So they have a salary, they have an office, they have employees. You can do that for me, can't you?

Ms. EASTERLY. I will, and I will get back to you.

Mr. HARRIS. Because you have asked for an extraordinary increase in personnel costs. So I am assuming some of that might be to maintain or actually amp up the DEI office. Is that true? Are there plans to actually expand it?

Ms. EASTERLY. I don't believe there are plans to expand that office, but I will certainly get back to you on that. Absolutely.

Mr. HARRIS. And just out of curiosity—because in your testimony you say you want to ensure we can hire a diverse and talented workforce. Now, what I want is the person looking after cyber to be the best.

So what do you do? Do you have a quota system for diversity? What do you do? Because you want to hire a diverse workforce. How does that work?

Ms. EASTERLY. No, we don't have quotas or targets. And when I say "diverse" I mean diversity of thought.

Mr. HARRIS. Let me tell you something, Madam Director: Wow. OK? Because we, on our side of the aisle, we have been kind of calling for diversity of thought as the real diversity that doesn't exist in academic institutions, for instance, that doesn't exist in many different things that we fund.

So I am going to leave that line of questioning alone. Let me just ask one other thing. And one of my colleagues may go further on that.

Part of your mission is election security. Is that right?

Ms. EASTERLY. That is right.

Mr. HARRIS. And disinformation or misinformation with election security.

Ms. EASTERLY. Foreign influence operations and disinformation.

Mr. HARRIS. OK. It has to be foreign—oh, OK. Well, foreign influence.

So, for instance, the Hunter Biden laptop was claimed to be a foreign disinfor—I mean, look, they said, look, this is Russian—we had numerous people in the security—I am sorry, former intelligence officials who said, oh, no, this has all the earmarks of Russian disinformation.

So CISA could have been involved. I mean, theoretically, that would fall, therefore, under what your agency could do. Is that right? Because it was claimed to be foreign disinformation affecting our election.

Ms. EASTERLY. No. I don't think we had any involvement. But that was before my time.

Mr. HARRIS. I am not saying it had your involvement. But according to what you said—you said you are disinformation and misinformation on election security.

The Hunter Biden laptop was, again, falsely blamed on Russian misinformation or disinformation.

So, therefore, theoretically, your agency could have been involved in interacting with social media companies to suppress any information on that.

Ms. EASTERLY. I don't want—

Mr. HARRIS. Theoretically.

Ms. EASTERLY. I don't want to talk about theory. What I want to talk about is what our actual mission is, what we are doing for State and local election officials, who have asked for our help in dealing with foreign influence and disinformation operations, and that is to support them in amplifying their trusted voices and providing them what they need to be able to ensure that the American people have confidence in the integrity of their elections.

And this is not a partisan issue, sir, as you know. This is entirely about supporting election officials of all parties, of all affiliation.

And as somebody who has served—beat Navy, by the way—as somebody who has served in the Army, I am very, very focused on just making sure we are defending and protecting every constitutional right that exists.

Mr. HARRIS. Thank you very much.

And, look, I am two for two, because I think both your answers are right. This shouldn't be a political issue. But it was pol—the Hunter Biden laptop was politicized. And we are trying to figure out at what level of the government's involvement in that politicization.

And I am very glad to hear that you want thought diversity. I am very glad about—I mean, I would rather have your employees understand a diverse group of threats as the meaning of “diversity.”

Thank you very much.

I yield back.

Ms. EASTERLY. Thank you, sir.

Mr. JOYCE. Thank you, Dr. Harris.

Mrs. Hinson.

Mrs. HINSON. Thank you, Mr. Chairman, and thank you, Ranking Member Cuellar, as well, for holding this hearing today.

Director Easterly, it is great to see you again. Thank you so much for meeting with me and answering some of my questions before the hearing today about what you are doing to help reduce cyber threats, also ensure that our critical cyber installations and infrastructure are resilient. So I appreciate that.

I know CISA is obviously working to secure cybersecurity and infrastructure but also to analyze and create tools to help build up that security across various sectors in the country. You mentioned collaborative analysis there.

And while that work is, of course, essential to protecting our national security now, what I am most concerned about is the agency's long-term stability and consistency toward that mission and that goal, if it is pulled into many different directions, with a focus on maintaining that unified mission. That is really what I want to see you do going forward.

So what do you see as CISA's primary function and driving focus? And what steps are you taking to rein in, to make sure you are focused on that mission?

Ms. EASTERLY. Yeah. Thank you very much. It was great to meet with you. And I appreciate your leadership.

We went through an exercise to ensure that we could create a strategic plan that lays out our goals in a unified way.

Mrs. HINSON. Uh-huh.

Ms. EASTERLY. So what we wanted to do was not to do a whole bunch of different things, just as you said. We wanted to focus on four key things: one, on cyber defense; two, on infrastructure risk and resilience; three, on operational collaboration; and, four, on unification.

All of that is spelled out in our strategic plan, along with our mission, which is to lead the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day, with the vision of secure and resilient infrastructure for the American people.

Every single person in my agency is focused on that very specific mission, and everybody sees themselves in that mission. So focus, focus, focus, continue to invest in those capabilities that will most effectively drive down risk to the Nation.

Mrs. HINSON. All right.

And I look forward to working with our ranking member on his initiatives to hopefully get some ROI and some firm requirements there and some teeth on what we are getting for our dollars.

With the ongoing cyber threats, of course, from foreign adversaries—you called them foreign influence operations—like the CCP, which is blatantly targeting Americans' data. Obviously, you mentioned TikTok, as well, as a huge threat. These are truly attacks on our critical physical infrastructure and on our Nation's security, so it is more essential than ever that our cyber platforms are secure.

I think we need to be forward-thinking and planning for that next threat. These attacks are happening every single day en masse, and we need to be confident we have guardrails in place to detect.

So, again, getting back to what you mentioned about collaborative analysis here, without going into too much detail timing-wise, what preventative measures is CISA utilizing to counter that increased aggression from foreign adversaries, like the CCP and Russia? As you mentioned, SolarWinds. We know they are not giving up. So can you just briefly dive into that for me?

Ms. EASTERLY. Yeah. And we have made significant investments even just the past 2 years, given the lessons learned out of SolarWinds.

The thing that I would highlight—because I think to get to that sustainable cybersecurity, we really do need a posture of persistent operational collaboration, a recognition that the government can't do it alone, industry can't do it alone. So that is why the Congress gave us these authorities to build the Joint Cyber Defense Collaborative. And we have been working with our partners since August of 2021 to operationalize that.

We did it to help drive down risk around a very serious software vulnerability called Log4j. We did it around the Russian invasion of Ukraine, working with our industry partners to come up with a four-phase plan where we could actually measurably do things if the Russians actually retaliated against our infrastructure. We were bringing in data, we were analyzing it, we were enriching it, and we were creating a picture that allowed us much more ability to actually drive down risk to the Nation.

And we have been expanding it. If you happened to see—if not, I will get it to you—our JCDC planning agenda, where there is a focus on working with energy companies, a focus on further collaboration on things like high-risk communities, further collaboration with cross-sector entities—so all kinds of things to continue to drive down risk. But collaboration and collective defense is the key to that.

Mrs. HINSON. You mentioned it was, I think, 560 new people is what I wrote down. How many of those people, would you say, are devoted to these types of priorities?

Ms. EASTERLY. So 516—



Mrs. HINSON. Sixteen. OK.

Ms. EASTERLY [continuing]. Actually.

And we have in our—so, in those priorities, frankly, I mean, I would say collaboration is one of our core values at CISA, so I would like to say everyone in collaboration. Because, as you know, we don't do law enforcement, we don't do intel, we don't do military, we are not a traditional regulator; we are a partnership agency. So I think everybody would say they are part of these collaboration efforts.

Specifically on the cyber side, that falls within our cyber team, which is about 1,000 people.

Mrs. HINSON. OK. Great. Thank you, Director.

Ms. EASTERLY. Thank you, ma'am.

Mrs. HINSON. And I yield back.

Mr. JOYCE. Thank you, Mrs. Hinson.

Mr. Guest, please.

Mr. GUEST. Thank you, Mr. Chairman.

Director Easterly, thank you again for being here.

I want to talk a little bit about the private sector and the hardening of cybersecurity. Would you agree that cost is a major disincentive for private companies to harden their cybersecurity as needed?

I am thinking, as we look at today's environment, we have inflationary costs which are extremely high. We know that energy costs are up, labor costs are up, input costs are up. And for many in the private sector, it is an allocation of where those dollars are spent.

And one of the things that I have heard talked about is the possibility of tax credits for private businesses, particularly those in the 16 critical infrastructure sectors, that if they are using those dollars to harden their cybersecurity, that they be given some sort of tax credit for that.

Would you be supportive of that as a way to encourage private companies to continue to invest in their cybersecurity?

Because we know it is not a one-time expense, you know. It is a continual upgrade, a continual cost that these companies are bearing. And should there not be some sort of tax credits, where these companies that are investing to the level approved by CISA would be able then to use some of that as a credit toward taxes to the Federal Government? Is that something that you would be supportive of?

Ms. EASTERLY. I haven't studied it, but generally I am supportive of anything that incentivizes our businesses to make their networks and systems more secure.

Mr. GUEST. And would you agree that cost is a disincentive for some companies as the reason that they don't properly invest in cybersecurity?

Ms. EASTERLY. Yeah, cost and, you know, frankly, some people look at tech as magic, and so it is hard to get the talent and the skills to be able to secure networks.

But I would say, sir, we should stop putting the burden on these small businesses and forcing them to make a decision between mission and security. I go back to: Technology providers should be baking in security so that we don't have to worry about bolting it on at the back end.

Mr. GUEST. Well, and at some point, if the providers are going to have to continue to do that, I mean, ultimately that is going to be a cost borne out by someone. And so it seems to me that tax credits would be a logical step to encourage businesses to do that.

I know TikTok has been brought up once or twice in this hearing, and I know that last week you probably saw there were lots of conversations about TikTok. As the Director of CISA, can you talk a little bit about the threat that TikTok poses?

Ms. EASTERLY. Yeah. I think anything that is in the control of a foreign adversary, to include our preeminent threat from China, where troves of data, to include data from kids, goes back to a foreign adversary for them to be able to use that data potentially for influence operations, for profiling, I think is a huge, huge risk, which is one of the reasons why TikTok is off Federal Government devices.

And I think we need to be really, really mindful, not just TikTok—that is an important and a prominent issue, but, in some ways, sir, it is a tactical issue. It is all sorts of Chinese technology that is in our critical infrastructure supply chain. We need to be very concerned about that.

And then, frankly, from a strategic level we need to be very concerned. We know that China for years has been doing espionage and stealing intellectual property, but every foothold for espionage can be a foothold for disruption and destruction. And so we need to be prepared to be able to respond to any type of incursions that might exist on our networks.

Mr. GUEST. And would you be supportive of a ban of TikTok?

Ms. EASTERLY. Across the country?

Mr. GUEST. Yes.

Ms. EASTERLY. I would be. I don't know if that is implementable though.

Mr. GUEST. And then, recently, we have seen reports of a data breach at the DC health insurance exchange, which many Members of Congress and our staff use that health exchange.

Can you talk a little bit about that breach, information that you may be able to share in a non-secure setting with myself and the other members of the committee?

Ms. EASTERLY. I don't want to talk specifically about that. I would be happy to do it in a closed session to give more information on that, sir.

Mr. GUEST. Are you able to say whether or not that breach occurred from a foreign adversary, someone—was it—because we know you have nation-states which are conducting cybersecurity threats, there are criminal organizations, and then we have the lone-wolf or the individual actors.

Of those three, could you classify which of those three was responsible for the data breach at the D.C. health exchange?

Ms. EASTERLY. I don't have the attribution at hand. I am happy to get back to you on that, sir. I don't know if final attribution has been made.

You know, when you talk about those categories, though, of course you have nation-states, but, you know, many of those cyber criminals are given safe haven and sponsorship by those nation-

states. So we don't see a lot of these lone-actor ones; there is usually some connection there.

But I am happy to get back to you with more specifics.

Mr. GUEST. Thank you, Mr. Chairman. I am out of time, so I yield back.

Mr. JOYCE. Thank you, Mr. Guest.

We will recognize Mr. Cloud upon his return, but we will go to a second round. And we will start with the distinguished ranking member, Mr. Cuellar.

Mr. CUELLAR. Thank you, Mr. Chairman.

And let me just add the same thought, thinking, on the private sector, trying to find that balance between the carrots and the sticks. And without going into details, I would ask you, if you have any suggestions, let us know.

Because, you know, one of the things I worry about is, I don't want the private sector just to depend on the Federal Government, and, at the same time, we want the private sector to do its fair share. So that balance is always hard.

So I just want to ask, if you have any thoughts, provide it to the committee, and we would appreciate that.

Ms. EASTERLY. Yes, sir.

Mr. CUELLAR. Then, second of all, I am now looking at your strategic plan, the vision, the mission, goals, and, of course, the objectives under each of the goals. And I am looking at this just right now.

I don't think I have a problem with your mission, your goals. I still go back, you know, to the performance measures. And I think anybody that has worked with performance measures or strategic plans, it is always hard trying to measure. So I would ask you, if you can, work with us, give us some suggestions.

And I would encourage all the members of the committee, like we do anybody that is over at the State, we get involved with the agency. Because if you let—again, not you, but I have seen some other ones where, if you let the agencies, they will come up with the measures where they basically are patting themselves on the back, and the difficult ones it is always hard to do. It is a lot easier to measure activity, and it is a lot harder to measure results.

So I just want to say, I want to work with you all—hopefully the committee will be willing in a bipartisan way—and ask that we all look at the performance measures not only for your agency but the other agencies under Homeland.

That is it. I want to work with you, and if you have any thoughts, let us know.

Ms. EASTERLY. Yes, sir. Absolutely. And we are not looking for a certificate of participation. We are looking to actually reduce risk to the Nation. So I would love to work with you to make sure that we are wisely investing what you have given us.

Mr. CUELLAR. Yes. Because I think taxpayers always want to see that.

Ms. EASTERLY. A hundred percent.

Mr. CUELLAR. You know, if we put in \$1, they want to know, what is the bang for that \$1? It is like, you know, in 2020, we invested \$650 million; people want to know, what did we get for the \$650 million? How is our country safer now?

Ms. EASTERLY. Yes, sir.

Just one thing on this that I would like to talk about is, you know, there have been ransomware incidents across the country for the last few years now on some of the target-rich, cyber-poor entities, like K-12 schools, like hospitals, like public utilities.

And so we made a very deliberate effort, starting in fiscal year 2023, to actually do outreach to those sectors very purposefully and use some of our Cybersecurity Performance Goals and our free services, both government and industry, to measurably and materially drive down risk by actually implementing the things we put in the CPG.

So what we are looking to do is actually look at the numbers, that we know of anyway, on incidents for those sectors, and then at the end of the year both measure the activities but, more importantly, see where we have been able to materially reduce risk.

So that may be a way to actually, at an outcome level, start to measure some of the investments that we are making, particularly for some of those cyber-poor entities.

Mr. CUELLAR. Right.

And one of the reasons we want to look at the measures is, for example, in your fiscal year 2024 request, it looks like CISA is shifting resources away from physical security programs in order to be more focused on cybersecurity missions. In other words, I think there are cuts to programs dealing with critical infrastructure, bombing prevention, school safety, and other programs that ensure the security of public gathering spaces. That is why those measures are going to be important.

Any reason why you are requesting reduction on some of those physical infrastructure that I mentioned, school safety and—

Ms. EASTERLY. Yeah.

Mr. CUELLAR [continuing]. Other programs like that?

Ms. EASTERLY. Sir, in a very tight budget year, we had to make some really tough choices. We just didn't annualize. It is the same request from the President's budget in 2023. You all were very generous with plussing us up in those areas. We just didn't annualize it, because we had to make really tough choices.

If the committee looks to put back money in school safety, which I think is \$3 million, and in the Office of Bombing Prevention, which was \$9 million, we could certainly do stuff with it.

Mr. CUELLAR. Yeah.

Mr. Chairman, thank you so much.

Mr. JOYCE. You are more than welcome, Ranking Member Cuellar.

Mrs. Hinson.

Mrs. HINSON. Thank you, Mr. Chair.

A quick followup. We have talked a lot about TikTok already, so I don't need to beat a dead horse here. But are there other platforms that you are very concerned about that maybe we are not paying as much attention to? Because, obviously, we are having a lot of hearings about TikTok, we are having a lot of discussions about it. What is the next thing that we are worried about?

Ms. EASTERLY. Yeah. So, in terms of those types of capabilities and platforms, I wouldn't, you know, name a specific one. But what I will say I am very concerned about is some of the emerging capa-

bilities specifically in artificial intelligence, which can be used by threat actors like China for weaponization—weaponization of cyber, weaponization of genetic engineering, weaponization of bioweapons.

And, you know, I am a techno optimist generally. I have seen technology save lives and do amazing things for our national security. But I have concerns, in my role, to see the rapid acceleration, almost the frantic pace of the implementation of some of this technology into actual things that we are using on a daily basis. And I do not think that there are the right guardrails in place to be able to assure us that this is not going to have cascading massive impacts on our safety.

Mrs. HINSON. Uh-huh.

Ms. EASTERLY. So those are the things that we are starting to work on as part of our overall technology safety efforts, is the safety of artificial intelligence. Because I think we are going too fast, and we don't know what is at the other end. And I think our adversaries can use this technology in very, very damaging ways, and we need to more fully understand that.

Mrs. HINSON. Right. They are weaponizing that information, as you said, to influence as well.

But you did mention something that is very important there: technology used to save lives, which is a critical part of our mission, I think, as Members of Congress but also in what you do.

And in my district in Iowa, we obviously know how important it is to make sure that those safety tools and emergency communications systems are up and running well and that they can deliver that lifesaving information, those alerts to people. We saw a failure in Iowa recently. We had some tornados about a year ago, and some people died.

So I would just be encouraged to hear a little bit more from you about what steps CISA is doing to ensure that our emergency comms networks are resilient, strong, and operating correctly, so we can avoid having a repeat of what happened in Iowa.

Ms. EASTERLY. Yeah. Thanks so much for that question.

So our Emergency Communications Division is so important. It really grew out of the entities that came out of 9/11—SAFECOM and now the National Council of Statewide Interoperability Coordinators.

So what we work on, along with all of our—we have ECCs, emergency comms coordinators, in every region. We are focused on working with the public safety community and the emergency responders to ensure that their comms are secure, resilient, and interoperable.

So, of course, it is Emergency Communications Month coming up in April, and we have a full-court press to make sure that we are bringing on more of these entities into our Government Emergency Telecommunications System and our Wireless Priority System, so when there are significant hazards or incidents, we can switch over to those capabilities and can be able to provide that same emergency comms.

So, day-in, day-out, working on collaborative planning, working on creating resilience. We are providing tools and assistance to the public safety community. And just incredibly important.

And, you know, I would love to follow up with you on this, because I think our work in this space is—you know, it is only really noticed when you have incidents like you had in Iowa when you can't use your 911, but critical to the security of the Nation.

Mrs. HINSON. Yeah.

And, obviously, the derecho came through, and people had no way to communicate even with the Governor's office. In my community, they were trying to get a hold of her, and they couldn't, right? I mean, so that is a huge challenge.

So I think what is important is redundancies there, to make sure that we are—you mentioned resilience, but, obviously, our threat actors that we are competing with and trying to counter, they are obviously looking for any vulnerability there. So that is a huge concern.

And I want to wrap up with just a question about supply-chain vulnerabilities, as far as hard infrastructure is concerned. Because, obviously, we are coming out of a major pandemic. We learned a lot of lessons about the supply chain in general. But what do you see as the biggest challenges there in terms of threats or vulnerabilities?

Ms. EASTERLY. Yeah. I think the biggest issue—and we run, as you probably know, the Information and Communication Technology Supply Chain Risk Management Task Force with many of our partners.

But, you know, I would just say that the biggest issues are that some of these supply chains are run by small businesses. And so these entities are part of this target-rich, cyber-poor group of people that, you know, the person doing HR is the person doing IT, is the person doing finance. And some of these entities are within our critical infrastructure.

Mrs. HINSON. Uh-huh.

Ms. EASTERLY. And so one of the things I was most excited about is we created these Cybersecurity Performance Goals.

Now, the gold standard for risk management is the NIST Cybersecurity Framework, and that is what we used at Morgan Stanley, for example. But if you are a small business, you look at that and it is just intimidating. So what we wanted to do was really take that document and distill it down to less than 40 things that can be done, characterized by cost, complexity, and impact, to drive down risk.

And we are most excited about being able to use that into some of these small companies that sit within the supply chain to really materially drive down risk. Because that will make us all safer just given how interconnected, how digitized, and how vulnerable we are because of some of those supply-chain components.

The last thing I would say is, we need to also look at some of the Chinese technology that is within our supply chains. FCC has a list of some of this technology that they are looking to come out of communications. But we are actually—because we have vulnerability scanning of the public internet, we can see some of these technologies in critical infrastructure. We have actually done outreach now to, I think, 120 entities to let them know, hey, you have Huawei, you have Hikvision, you have ZTE; you know, you should

think to pull that out, because it is creating risk in your network. So we need to do that as well.

Mrs. HINSON. Well, thank you, Director Easterly.

And I look forward to working with you, Mr. Chairman, to maybe act on some of those challenges that she just mentioned. Thank you.

Mr. JOYCE. Absolutely. Thank you, Mrs. Hinson.

Recognizing Mr. Cloud for his initial round of questions.

Mr. CLOUD. Thank you so much for being here and sharing your insight with us.

I wanted to tackle—you know, we all certainly want to guard our cyber infrastructure. And, you know, that is a bipartisan goal. A lot of Americans are now concerned about maybe some of the mission creep that has happened recently.

You started, I guess it was in July 2021. And then, shortly after that, not that you did this, but in September there was an effort to start a Disinformation Governance Board, and there was a lot of pushback from that. But part of that memo said that CISA would be involved in flagging content for censorship on social media platforms leading up to the 2020 election.

And then we know that CISA played a key role in working with outside organizations, such as the Election Integrity Partnership, to censor information about the Hunter Biden laptop story.

What are you doing to make sure that that kind of thing doesn't happen again?

Ms. EASTERLY. Yeah. Thank you for the question, Congressman.

Just to be totally crystal-clear, as I think you would want me to be, we don't censor anything. And as someone who served, as a combat veteran that—

Mr. CLOUD. No, but you recommend to Twitter and social media organizations or flag things for them that could be considered—

Ms. EASTERLY. We don't flag anything to social media organizations at all. We are focused on building resilience to foreign influence and disinformation.

So we do not do any censorship. And I just want to make that incredibly clear.

Mr. CLOUD. OK.

On March 7, Biden issued an executive order, 14019, directing all Federal agencies to develop voter registration and voter education plans, to be submitted to the White House and OMB by September 2021.

My understanding is that CISA has submitted a plan to the White House. Is that correct?

Ms. EASTERLY. I need to go back on that. If there is—September 2021? I don't know, sir. I will go back and check on that.

Mr. CLOUD. OK. There has been a number of FOIA requests to get copies of these plans.

Ms. EASTERLY. Yeah.

Mr. CLOUD. And I would like to see if you could—

Ms. EASTERLY. Voter registration—sir, can you help me understand the question?

Mr. CLOUD. Biden issued an executive order directing all Federal agencies to develop a voter registration and voter education plan, to be submitted to the White House.

And my understanding is that CISA did submit one but there have been some FOIA requests, and, government-wide, there has been a lot of non-transparency in delivering on those plans when it comes to FOIA requests.

Ms. EASTERLY. Yeah.

Mr. CLOUD. And would you be able to get us a copy of that plan?

Ms. EASTERLY. Yeah, 100 percent. And, you know, at the end of the day, happy to be completely transparent. Transparency builds trust.

Mr. CLOUD. Yeah.

Ms. EASTERLY. That is our job. Elections and voting is not a partisan issue.

Mr. CLOUD. Sure.

Ms. EASTERLY. We work with all parties, all affiliations. We are just trying to make sure that, whether you are Republican, whether you are Democrat, election officials have what they need to be able to run safe and secure—

Mr. CLOUD. Or neither.

Ms. EASTERLY [continuing]. Elections, as you would want us to.

Mr. CLOUD. Sure.

One of the issues we have when we are looking at budgets is, a lot of the line items we send or we will fund, the line item is great, a lot of bipartisan support for it, but a lot of the action that would be questionable is in the grant-writing process.

But it is hard to have transparency on that, because there is very little transparency on where the grants are going, who the grants are going to, what particular NGOs, what particular—even how the contracting is happening.

Can you work with us on getting us a copy of everyone that has received any sort of grant or contract over the last 2 years through CISA?

Ms. EASTERLY. Yeah. Absolutely. Are you talking about—the grants, the one that we are most directly involved in managing is the State and Local Cybersecurity Grant Program that is really dedicated to State and local.

So, you know, as you can imagine, a lot of those capabilities at the State and local level don't have a lot of resources, and so we want to make sure that the State of Texas or the jurisdictions have what they need to keep their networks and systems secure.

But happy to get you whatever you would like.

Mr. CLOUD. Well, thank you very much.

And I yield back.

Ms. EASTERLY. Thank you.

Mr. JOYCE. Thank you, Mr. Cloud.

I recognize Ms. Underwood for the second round of questions.

Ms. UNDERWOOD. Thanks so much, Mr. Chairman.

Director Easterly, I know you have placed a lot of emphasis on these target-rich, resource-poor critical infrastructure sectors.

In northern Illinois, we have a lot of rural and suburban communities with schools, small businesses, public works facilities, and hospitals that lack the resources to combat the evolving 21st-century landscape of cyber threats. Yet these are vital services for our communities, and we rely on them every day, and they are responsible for a lot of data.



What are some of the most target-rich, resource-poor critical infrastructure sectors and subsectors? And what is CISA doing to help those owners and operators mitigate the specific risks they face?

Ms. EASTERLY. Yeah. Thanks very much for that question.

What we wanted to do was look at those entities that were most targeted by ransomware over the past year and then really focus in a way where we could measurably drive down risk, leveraging the Cybersecurity Performance Goals and then the no-cost vulnerability assessments and some of the tools that we had.

So we chose K-12 school districts, and we wrote—if you haven't seen it, we actually did this great report with the school entities about what are the tools that can most help schools that don't have a lot of resources there. So we are focused on that.

We are focused on public utilities, like water facilities because I am very concerned about that.

And we are focused on hospitals, you know, particularly some of the smaller hospitals. I know you have an appreciation for that. Because making a decision between a surgeon and whether you upgrade your software, you shouldn't have to make those decisions.

Ms. UNDERWOOD. That is right.

Ms. EASTERLY. So we have brought the CEO for Atlantic Healthcare on our board, we have brought somebody that does public utilities in New Hampshire, we have brought somebody who heads a K-12 nonprofit to help advise us and connect us with those communities to drive down that risk using some of these new tools that we have.

By the way, we actually followed up on Waubensee. Thank you for raising that to make sure that they have what they need to drive down risk.

Ms. UNDERWOOD. Excellent. Thank you.

I see small local governments as another example of a target-rich, resource-poor entity. My Resilience Act would target CISA's resources through outreach and pilot programs to rural and suburban communities that don't have the resources to defend against every cyber and physical threat.

Can you provide an update on CISA's current work to help local governments protect themselves from emerging threats?

Ms. EASTERLY. Yeah, absolutely.

The thing I think we are most excited about here is the grant program, the State and Local Cyber Grant Program. Two States opted out of it. We have 54 States and territories that are going to do it. We just received 12 of the first proposals for the first year.

Ms. UNDERWOOD. Yeah.

Ms. EASTERLY. We just approved 10 of them. Info went out to those 10. FEMA is in the process of just validating that. And the money should be out the door within the next couple weeks. And so we look forward to seeing those other 44 by September. And, as you know, that goes for several years.

And there is also a matching component. So we don't want to have this sort of—you know, we understand cyber-poor, but we don't want to have a moral hazard. We want to teach a person to fish, so at the end of the day there is some matching that occurs at the State level.

Ms. UNDERWOOD. Yep.

Ms. EASTERLY. And then we are going to provide assistance to ensure that they are continuing to raise their baseline so that they can drive down risk.

Ms. UNDERWOOD. Excellent.

Now, I understand there has been a larger national conversation and Republican leadership has put forward a plan to involve some cuts.

We received a letter from the Secretary outlining the impact of some cuts, including a note about State and local impacts, which says that budget cuts would lead to a 13-percent reduction in CISA's regional field forces, and the regional workforce is a critical component of CISA's service delivery model.

I am about putting people over politics. And I think that CISA's value and impact for our local communities is unmatched, and would certainly not support this type of devastating cut.

Wondering if you might want to expand on the impact of such a reduction.

Ms. EASTERLY. Thank you. I completely agree. If we have any of the cuts, if we get pushed back to 2022, it will severely negatively impact what we have been able to do with State and local partners and with those smaller critical infrastructure owners and operators around the country.

Over the past 2 years, we have added significant forces—cybersecurity advisors, cybersecurity State coordinators, protective security advisors—that are on the ground, the tip of the spear, providing our no-cost resources, capabilities, and tools to drive down risk to this Nation, in an environment where there are very serious nation-state threats and cyber criminals that are sponsored by those nation-states.

So I would be very concerned about any cuts to those capabilities as well as any capabilities of the things that we asked for. Because that will put us back in a pre-SolarWinds world where we will lose that visibility that we have developed, and that is harmful to our security as a Nation.

Ms. UNDERWOOD. Harmful to our security as a Nation. Limits our ability to meet the demand from our State and local partners, who, as I understand it, are asking for support. And these PSAs and CSAs are oversubscribed as is. And so we can't let a 13-percent reduction move forward.

Thank you so much, Director, for being here.

Ms. EASTERLY. Thank you.

Ms. UNDERWOOD. I yield back.

Mr. JOYCE. Sheriff Rutherford.

Mr. RUTHERFORD. Thank you, Mr. Chairman.

And I want to follow up on that. In my absence, I know Mrs. Hinson talked about our foreign adversaries and Mr. Guest talked about TikTok, so a lot of my questions have already been asked in my absence. And I know Mr. Trone spoke of staffing, as did Ms. Underwood just now, and I want to follow up on that.

Because I will tell you, that is, I think, one of the most important issues we have going forward, is, what are the national staffing needs for cyber-trained individuals, and what are we doing about

it? And what are your needs from a staffing standpoint, and what are we doing about it?

And so can you talk a little—and I guess my question, too, is, is that in your mission, to help develop human capability out there?

Ms. EASTERLY. Yeah. Absolutely.

So, just to talk about CISA specifically, as I mentioned, we have a full-court press on hiring. We are projected to hire up to 600 people this year. That will drive down our vacancies. And, you know, we have grown, I think, 13 percent over the past couple years, given some of the new budgets, so now we are at a place where we are going to be able to drive down vacancies. Because we even asked for, I think, 11 new positions with this budget.

So I am very confident that we will have the capacity and capability to defend the Nation as America's cyber defense agency.

With respect to the rest of the country, so the stats are something like: 3.5 million unfilled cybersecurity jobs globally, 700,000 in the U.S., and about 35,000 in the Federal Government.

So, from a Federal Government perspective, we are working on things like, we run re-skilling programs for people who want to—

Mr. RUTHERFORD. I am sorry, say that again?

Ms. EASTERLY. Like, re-skilling programs. So a 3-month course for people who want to move from what they are doing into cyber and get re-skilling training. So we do that.

We do the Federal Virtual Training Environment, where you can go on and learn about cyber through webinars.

And then we also—importantly, we work across the Nation. Because I think this has to be, frankly, from K—what I call “K through gray.”

Mr. RUTHERFORD. Right.

Ms. EASTERLY. And K–12 is really important. I just saw North Dakota actually mandated cybersecurity in their K–12 education. I think every State should do that, frankly. Because our kids are digital natives, while we are all digital immigrants. They are very facile on their devices. But, quite frankly, they don't know how to protect themselves. So they need to learn at a very young age how to protect themselves.

So we actually have a grantee in Louisiana, Cyber Innovation Center, and we work with them to provide curriculum to train the trainer, for teachers all across the Nation in every State. And I think more of that program is really, really important as we dig in and help our younger folks get more facile on cyber.

It has to be a national thing. It can't just be the Federal Government.

Mr. RUTHERFORD. Uh-huh. Alrighty.

And can you—I want to ask you personally, because I trust you a lot.

Ms. EASTERLY. Thank you, sir.

Mr. RUTHERFORD. This whole TikTok thing, I have to tell you, I am a little torn. I don't like censorship, but I don't know enough about what our full reasons are about going after TikTok.

Can you talk about that a little bit and where you come down on that issue?

Ms. EASTERLY. Yeah. Thank you, Sheriff.

So the data right now from TikTok that a lot of kids use—I think 130 million Americans; that is a lot—basically goes back to China. And, you know, frankly, for those who talked about, you know, we can be more—we can compete economically and this can be a partner, I don't see us turning in that way.

I very much worry about the threat from China to our Nation, and I very much worry about what they are going to do with all of that data to weaponize it—to weaponize it for influence operations. Particularly, I am worried about that, as I have said throughout the hearing, foreign influence operations during our elections.

Mr. RUTHERFORD. Yeah.

Ms. EASTERLY. The Chinese have a well-known doctrine of cognitive domain operations. They are focused on influence operations against the American people to sow discord, to sow distrust, to undermine our confidence in the core foundations of our democracy. This is why I am concerned about so much data that is going right back to an adversary nation.

And I agree with you, we don't censor. You know, I spent 21 years in the Army and three times in combat zones serving the Nation, sworn to protect and defend the Constitution of the United States. We don't censor anything.

What we want to do is to ensure that we are building resilience and securing our Nation from the type of threats that we are going to be dealing with in a really serious way. And China is where we need to be focused.

Mr. RUTHERFORD. Thank you.

I yield back.

Ms. EASTERLY. Thank you, sir.

Mr. JOYCE. Thank you, Sheriff.

Mr. Trone.

Mr. TRONE. I would just like to comment that I think where the sheriff is going there is really right on point. And it is so good to hear, you know, you talk about that and explain that to us. And, you know, I really appreciate that. It really helps me.

And I couldn't agree with the sheriff more on the importance of building that pipeline of workers to get into cyber. And if we see we are falling behind, like we have fallen behind on addiction specialists, therapists, psychologists, a lot of folks in the medical fields—we are doing things to help fill those needs, but if we see the problem here, you have to come to us. And we can think about ways we can put tax credits, tuition refunds, get our kids in this area that are going to be such great jobs in the future that really pay well.

And the other comment would be, I really thought Mr. Guest had some great comments about, you know, maybe some tax credit ideas on our small business. You know, a bigger business, like myself, we get it; we are all in. But these small businesses, you know, I was there one time, and you always think short-term. You are just working on getting payroll Friday. And you have to think long-term, you know, when you look at cyber, because it is going to devastate you. You won't be able to recover.

So, if we give them some sort of credit, that kind of gets them in the swimming pool, so to speak, and gets their feet wet, and

then all of a sudden they realize, wow, this could be bad. Then they are going to figure out how to get some of their own resources, go to places like the chamber, we talked about earlier and be successful. And we can support those small businesses, which are—the future of our country is small businesses in America.

So we should continue to think about that, Mr. Chairman, and ideas. I think this should be very bipartisan and we would all support that.

The last thing I want to mention was on TikTok. You had talked to me a little bit about how TikTok looks differently in China and how it works in China versus how TikTok works here and how the, I think you said, dumbing-down of 130 million Americans, so they are just dumbed down, looking at dogs and cats and animal tricks, versus thinking about reading a book, you know, about philosophy or English literature, you know, some things that really could help us.

So talk about that, how it is different in China.

Ms. EASTERLY. Yeah. And my friend Tristan Harris, who was one of the founders for the Center for Humane Technology, actually talked about this, I think it was on “60 Minutes,” several months ago.

It is this idea of “spinach TikTok,” so the controls that are placed by the Chinese on how TikTok is used within their nation. Restricted time. There is not the—you know, I am not ideologically opposed to cat videos, but, at the end of the day, cat videos versus videos about museums and Nobel Prize winners.

So this is really different from what our kids here are seeing, versus what kids in China are seeing.

Mr. TRONE. The kids in China are seeing what?

Ms. EASTERLY. Seeing much more educational videos. And they are restricted in terms of timing.

And so, you know, when you think about what our kids are seeing here versus there, it is, I think, part of an overall strategy to impact how our kids are being educated. And I worry a lot about it, both as the Director of CISA but also as a mom.

And I think we all, as parents, as citizens of this Nation, we all need to be focused on, really, how to be a good ancestor, frankly. What are my great-grandkids going to think about, you know, these, what I call, “weapons of mass distraction” and all of the, sort of, tools—which, frankly, we should, you know, read a damn book, right, at the end of the day.

And so I am with you. And, again, there is some cool stuff going on in this technology, but I think we need to be very mindful about how it is impacting the next generation.

Mr. TRONE. You nailed it. Thanks for your insights.

I yield back.

Mr. JOYCE. Thank you, Mr. Trone. And I agree that reading books allow one’s imagination to flourish.

Ms. EASTERLY. Yes, sir.

Mr. JOYCE. And taking my second question of this round: Hypothetically, what would a full-fledged nation-state-actor attack on our critical infrastructure look like? And what are we doing to prepare for that worst-case scenario?

Ms. EASTERLY. Yeah. Thank you for asking. You know, I often get asked what keeps me up at night.

Mr. JOYCE. Yeah.

Ms. EASTERLY. This is part of it. A lot of things, is the answer.

So, you know, you saw, I am sure, the intel community assessment that came out a couple weeks ago. And it is very clear in there, you know, we are still focused on the threat from Russia. We are still vigilant, we are still keeping our shields up, knowing that we are not out of the woods in terms of retaliation on our infrastructure.

But, to me, the focus needs to be on China. China is the pre-eminent threat. And so what I worry about is a scenario where, in the next 3 to 6 years, China decides to reunify with Taiwan, whether that is an invasion or a blockade of the straits. But, at the same time, I think we are very likely to see attacks here in the homeland.

Remember, China is looking at Russia and Ukraine, and they are learning lessons just as we are learning lessons, and I think they are costing in the impact of what an escalatory attack would look like. And so I think we would see attacks against pipelines, because the big lesson of Colonial Pipeline is, what a great way to create panic, to incite societal panic, to, you know, essentially upend how Americans are thinking about their safety and security.

So I would see attacks on pipelines, attacks on transportation, attacks on water facilities, all of which, again, induce societal panic, delay mobilization of our military forces, and really get the American people to say, "Look, I don't want to worry about that place out there. I really just want to worry about getting to work and getting my gas and getting my healthcare and being able to communicate."

And so I think that is the kind of thing that we can see. I think that is a more-than-likely scenario and certainly if you read in the intel.

So what are we doing? We are aggressively doing everything we can, working with our partners, our industry partners, our partners in every sector, to ensure they understand the threat and that they are taking aggressive measures to drive down risk.

If they are some of the smaller entities, it is using some of the no-cost tools and the capabilities like our Cyber Performance Goals to drive down that risk. If it is some of the bigger companies, we are working with them to ensure that we are sharing information to allow us to have a consolidated threat picture so that we can actually drive down risk to the Nation.

But this, to me, sir, it is not about prevention, at the end of the day. It is about resilience. Because in this highly connected, highly vulnerable world, it is very hard to prevent bad things from happening. We need to expect disruption. We need to ensure that we have redundant communications, that we are prepared to recover, that we have manual overrides, that we can actually withstand an attack and then get back up and have the country running in a very short period of time.

That is the mentality and the culture that we all need to be focused on across the Nation to be able to deal with these threats.

Mr. JOYCE. Thank you. And Godspeed in getting to that.

Ms. EASTERLY. Thanks, Chairman.

Mr. JOYCE. Without any further ado, members of the subcommittee may have some additional questions. I know both Mr. Harris and Mr. Cloud have asked for some responses from you. Would 15 business days from today give you enough time to respond?

Ms. EASTERLY. Yes, sir, Chairman.

Mr. JOYCE. OK. Thank you.

And anybody else who would like to send a written question in a timely manner, get their responses during that time.

But I also want to thank you again for being here today.

And this subcommittee stands adjourned.

Ms. EASTERLY. Thanks, Chairman.

Thanks, everyone.

[Answers to submitted questions follow:]

Questions for the Record  
Subcommittee Homeland Security  
U.S. House Committee on Appropriations  
Director Easterly  
March 28, 2023

CSD:

QFR 1. Compliance with OMB Memo on TikTok  
OMB Memo M-23-13 ([https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance\\_final.pdf](https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf)) required federal agencies to remove the TikTok application from the mobile devices of federal employees by March 27<sup>th</sup>.

**Question:** What steps has CISA taken to be in compliance with this OMB deadline?

**Answer:** On December 23, 2019, CISA proactively implemented a block to prevent federal and contractor users within CISA systems from downloading and installing TikTok or any successor application or service of TikTok developed or provided by ByteDance Limited onto their government-managed mobile devices; removing the applications and services from all devices prior to January 2, 2020. As a result, the agency positioned itself to ensure compliance by the stated OMB deadline.

On March 2, 2023, CISA's Office of the Chief Information Officer (OCIO) disseminated agency-wide communications to federal and contractor CISA employees to reiterate the OMB guidance and on March 6, 2023, CISA implemented a block to prevent users from accessing the TikTok URL from their government-issued mobile devices.



Questions for the Record  
Subcommittee Homeland Security  
U.S. House Committee on Appropriations  
Director Easterly  
March 28, 2023

CSD:

**QFR 2. Compliance with OMB Memo on TikTok**

OMB Memo M-23-13 ([https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance\\_final.pdf](https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf)) required federal agencies to remove the TikTok application from the mobile devices of federal employees by March 27<sup>th</sup>.

**Question:** To what extent does CISA acknowledge that removing the TikTok app from federal mobile devices is just the first step in preventing the data stored on these devices from being shared with apps and IP addresses originating in China?

**Answer:** CISA is highly concerned about the potential for sensitive data sharing with adversarial nation states, including China. We continue to work closely with OMB and federal agencies to identify any necessary steps to most effectively protect information stored or processed by federal agencies on behalf of the American people.

Questions for the Record  
Subcommittee Homeland Security  
U.S. House Committee on Appropriations  
Director Easterly  
March 28, 2023

CSD:

**QFR 3. Compliance with OMB Memo on TikTok**

OMB Memo M-23-13 ([https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance\\_final.pdf](https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf)) required federal agencies to remove the TikTok application from the mobile devices of federal employees by March 27<sup>th</sup>.

**Question:** What assistance is CISA providing federal agencies in terms of both removing the TikTok app and ensuring that mobile endpoint security solutions are being used to prevent federal data stored on mobile devices from being shared with the Chinese Communist government?

**Answer:** CISA provides technical capabilities, implementation guidance, and advisory services to agencies to support their cybersecurity posture and manage the overall risk in the federal enterprise. For example:

- CISA's Protective Domain Name System (DNS) resolver provides visibility into Federal Civilian Executive Branch DNS queries and traffic originating from on premises networks and destined for TikTok infrastructure. It additionally provides agencies with an ability to block such traffic. Several protective DNS customer agencies are already implementing block policies for multiple domain names used by TikTok infrastructure. The service is currently focused on on-premises networks and is being expanded to mobile, roaming, and nomadic devices.
- CISA provides Enterprise Mobility Management (EMM)/Mobile Device Management (MDM) solutions through the Continuous Diagnostics and Mitigation (CDM) Program. These solutions, where deployed, allow agencies to easily identify installed TikTok applications and take immediate action to remove them from affected mobile devices and prevent future installation. Additionally, when an agency partners with the CDM program to deploy this technology, the information is incorporated into the CDM Dashboard for CISA analyst visibility. This enables CISA operators to see across the federal enterprise to detect instances of this application and follow up with agency personnel for further action, when appropriate. Finally, CDM offers a Software Management capability that can inventory installed instances of the software on traditional desktop computing devices and provide the same federal enterprise visibility through the CDM Dashboard.

Questions for the Record  
Subcommittee Homeland Security  
U.S. House Committee on Appropriations  
Director Easterly  
March 28, 2023

CSD:

- The Traveler-Verified Information Protection (T-VIP) program is used to evaluate the post-travel security and integrity of official government devices used in high-threat overseas environments to reduce the likelihood of undetected compromise post-travel.



TUESDAY, MARCH 28, 2023.

**FISCAL YEAR 2024 REQUEST FOR THE  
TRANSPORTATION SECURITY ADMINISTRATION**

**WITNESS**

**HON. DAVID PEKOSKE, ADMINISTRATOR, TRANSPORTATION SECURITY ADMINISTRATION**

Mr. JOYCE [presiding]. Today's hearing will come to order.

This afternoon we welcome the Administrator of the Transportation Security Administration, David Pekoske, to testify on TSA's fiscal year 2024 budget request.

Administrator Pekoske, thank you for joining us today. I would also like to take a moment to congratulate you on being confirmed for a second term as TSA Administrator. In today's political environment, it is quite an achievement to work for multiple administrations.

I have a friend who has been in the U.S. Marshal in Cleveland, and he first got appointed under Bush in 2001, and so he managed—it is always quite an achievement. You must be really doing your job if you can survive administration after administration. Thank you for your leadership and service.

TSA's mission is vast and imbedded in the principle that transportation security is national security. Establishing the immediate aftermath of September 11, 2001, TSA works to combat dynamic threats across the Nation's transportation systems and protect the traveling public.

In order to carry out that mission in a robust and effective manner, the resources this committee provides to TSA must prioritize innovative and transformative solutions to security challenge we face today.

Of course, Administrator, I am not sure the President's 2024 budget request meets that mark. The budget request for TSA is nearly \$1.6 billion above the fiscal year 2023 enacted level. The single largest line item increase in the budget request is \$1.1 billion for pay increases for the TSA workforce.

I appreciate the dedication and service to our Nation that these officers show each and every day and believe they should be paid fairly, but I also recognize the significant budgetary challenges that this poses, especially in the current fiscal environment.

The budget request also woefully underfunds investment in new, more capable technology in airport checkpoints. For example, computed tomography technology is able to render 3D images of carry-on baggage, provide TSOs with a greater ability to identify potential threats at checkpoints while increasing the speed and efficiency of passenger screening.

However, the budget request includes only \$70 million for this technology, which is \$35 million less than the amount that was provided in fiscal year 2023. At the current rate, in this budget, TSA will not be able to fully deploy these systems across the United States until 2042.

Compounding these budgetary challenges is the administration has, yet again, resorted to budget gimmicks, assuming unauthorized fees that are offset for TSA's appropriation. Coupled with the \$1.1 billion in pay increases, this administration has created a huge hole in TSA's budget to the tune of \$2.8 billion.

The committee will need to take a hard look at the entirety of TSA's and the Department's budget and balance the proposals against other funding requirements.

Administrator Pekoske, today I look forward to your testimony and working with you throughout the fiscal 2024 appropriations process.

Before I turn to the witness for his statement, I would like to recognize our ranking member, my friend, Mr. Cuellar, for his opening remarks.

Mr. CUELLAR. Mr. Chairman, again, thank you so much. And, again, congratulations on your chairmanship.

Mr. Administrator, again, good talking to you again and welcome back. You are no stranger to this committee, and we appreciate the good work that you and your folks have done.

We are here looking forward to hearing about the President's budget request for TSA for fiscal year 2024, and I think we understand the very important work that you all do.

We rely, the public relies on making sure that flights take off on time, and it is a lot of work. And certainly, with the growth that now post-pandemic, we certainly know that those numbers are going to go up on that.

We also understand and we want to talk to you a little bit more about the fiscal year 2023 funding bill that is part of TSA's effort to provide parity to the TSA workforce, and an effort to bring TSA employees on par with their peers on the rest of the Federal Government. We do know that there is some work to be done legislatively and appropriations.

And again, we appreciate the work that you have done.

One of the things that also we want to talk to you a little bit about in some of the questions is the procurement process, the hiring process itself also, and also customer service. I am a big believer in customer service. Certainly, I appreciate the work that your folks do. Very important work. But again, customer service, how we treat, how we talk to people is very important.

So, again, we look forward to working with you. And, again, welcome back to the committee again.

Thank you, Mr. Chairman.

Mr. JOYCE. Thank you, Mr. Cuellar.

Administrator, without objection, your written testimony will be entered into the record. With that in mind, we would ask for you to please summarize your opening statement in 5 minutes.

**STATEMENT OF HON. DAVID P. PEKOSKE**

Mr. PEKOSKE. Thank you, Mr. Chairman, Chairman Joyce, Ranking Member Cuellar, and distinguished members of this subcommittee. Thank you for the opportunity to appear before you this afternoon on the President's fiscal year 2024 request for TSA.

Let me begin by recognizing that our operations are conducted by an incredible team of TSA employees and contractors and with the enormous security contributions of all the stakeholders in the aviation's surface transportation industries.

To put the scale of our operations in context, in calendar year 2022, 736 million travelers were screened in our checkpoints at over 430 airports across the country. This is an average of over 2 million travelers and their 5 million carry-on bags per day.

Last calendar year, we stopped 6,542 firearms, an all-time record, at our checkpoints. 88 percent of those firearms were loaded.

We expect that passenger volumes will continue to grow. Therefore, we need the additional staff requested in the fiscal year 2024 budget to continue to meet our passenger wait time standards of 30 minutes or less in our standard lanes and 10 minutes or less in our PreCheck lanes. We met these standards for over 99 percent of passengers last year.

And with this subcommittee's support, we continue to upgrade all of our primary screening technologies for identity verification, carry-on bag screening, and on-person screening. These critical technology investments accomplish all three of these key goals to improve security effectiveness, to improve security efficiency and to enhance the passenger experience.

I am very grateful for the funding we received in the fiscal year 2023 Omnibus Appropriations Act that places TSA employees on an equal-pay footing with every other employee in the Federal Government. This action is absolutely fundamental to our long-term success.

As I travel to airports and offices around the country, I find that our recruiting is stronger already, and our attrition rates are coming down as a result of Congress including fair pay in our fiscal year 2023 appropriation. It is having an enormous positive effect on our workforce, and it is coming just in time to ensure we are ready to face the changing threats to our transportation system and the increasing demand for air travel that all of us see evidence of every time we fly.

The TSA workforce performs a critical national and Homeland Security function. Here are some examples of outstanding performance: At Cleveland Hopkins International Airport, TSA's Alan Borocz and Joshua Guysinger found a knife hidden in a passenger's cast during screening.

At the Lehigh Valley Airport in the Allentown, Pennsylvania area, Transportation Security Officer Vance Hamilton and Nick Apostolou detected an explosive in a checked bag.

At Austin-Bergstrom International Airport, TSO Angel Ayala and STSO, Supervisor Transportation Security Officer Emmett Street detected a stuffed animal with over 50 rounds of 9 millimeter ammunition sewed inside of it.

And just this month, while assigned to a Visible Intermodal Prevention and Response deployment in the Charlotte Douglas International Airport, two Federal air marshals were called to assist the Charlotte-Mecklenburg police in approaching and apprehending a known felon in possession of a handgun in the airport's parking garage.

These and many more examples prove that TSA cannot be successful without a professional, vigilant, engaged, and properly staffed workforce.

I thank you in advance for your continued support of our workforce. That, in addition to fair pay, includes assuring that they have the tools and technology needed to do their jobs.

The cybersecurity of our critical transportation infrastructure is much stronger today than it was just two years ago, and that is urgently needed because the cyber threats we face are significant.

We have worked very closely with pipeline, rail, and aviation critical infrastructure owners and operators. Together, we have begun to build cybersecurity protections and improve the resiliency in these sectors that are so critical to our national well-being. The private sector and non-Federal Government entities that own and operate the majority of the transportation infrastructure have been terrific partners and have made significant and necessary investments in cybersecurity.

Similarly, the President's fiscal year 2024 request will provide the resources TSA needs to continue to fight this threat and support our stakeholders' efforts.

I appreciate the challenge of identifying the resources needed to fund TSA's operations. TSA's gross discretionary budget request is offset every year by revenues generated by a fee paid by all passengers when they purchase an airline ticket. This fee is called the September 11th Security Fee, and its only original purpose was to fund aviation security.

But since the 2013 Bipartisan Budget Act, a significant portion of these fee revenues, nearly \$1.6 billion or 38 percent of the total fees collected in fiscal year 2024 will be directed towards deficit reduction, not aviation security. The President has submitted a legislative proposal again this year to end this fee diversion and provide that \$1.6 billion in additional offsetting collections to TSA's budget.

I will do all I can to provide information to you and our authorizing committees to enact this legislative proposal and the fee diversion, and put the funds to their intended purpose, as the President has requested.

Thank you for the opportunity to testify, and I look forward to your questions this afternoon and to working with all of you over the coming years to ensure that TSA has the funding needed to continue to provide for our transportation security.

Thank you, Mr. Chairman.

[The information follows:]





TESTIMONY OF

David P. Pekoske  
Administrator  
Transportation Security Administration

BEFORE

House Committee on Appropriations  
Subcommittee on Homeland Security

ON

"Fiscal Year 2024 President's Budget Request for the Transportation Security Administration"

March 28, 2023  
Washington, DC

Good morning Chairman Joyce, Ranking Member Cuellar, and distinguished Members of the Subcommittee. Thank you for inviting me to testify on the President's Fiscal Year (FY) 2024 President's Budget Request, which includes a \$10.4B request for the Transportation Security Administration (TSA). I am honored to be here and am grateful for the longstanding and constructive partnership TSA enjoys with this Subcommittee and all the support you have provided over the years.

First and foremost, I would like to thank the Committee and Congress for the funding to support our workforce in the FY 2023 Omnibus Appropriations Act. This was not only the right thing to do by our workforce, but we believe it will help with retention and recruiting in ways that will have a measurable impact on mission performance.

I would also like to thank Congress for the authorities it has provided to TSA through the *TSA Modernization Act of 2018* as well as appropriations that have enabled us to execute our mission and make significant progress on our strategic priorities. Additionally, I would also want to take this opportunity to acknowledge the superior efforts of the entire TSA workforce, convey what they have accomplished, and explain our future goals and objectives. During the last year, TSA:

- Screened 736 million travelers, an average of more than 2 million passengers per day, with 99.4 percent of passengers waiting less than 30 minutes at airport security checkpoints, and 99.4 percent of TSA PreCheck® passengers waiting less than ten minutes. We need to maintain our wait time standards while ensuring security in light of increasing passenger volumes.

- Deployed an additional 534 Credential Authentication Technology (CAT) units and 191 Computed Tomography (CT) X-ray scanners, which significantly improve security while reducing physical contact.
- Enrolled 9 new airlines and 3 million individuals in the TSA PreCheck® Application Program. Just this month, on March 2, 2023, we achieved the milestone of exceeding 15 million enrolled members in the TSA PreCheck Program and are working to onboard two additional enrollment vendors to expand enrollment options. Taking into account TSA's partners, such as U.S. Customs and Border Protection's Trusted Traveler Programs, there are over 30 million Known Traveler Number holders with access to TSA PreCheck expedited screening. These programs provide more efficient screening and a better checkpoint experience, while also maintaining the required level of security for passengers by allowing TSA to allocate resources to areas of the greatest risk. TSA also recurrently vetted over 30 million individuals across transportation worker populations on a daily basis.
- Prevented more than 6,542 firearms—a record number—from being carried into the secure area of airports or airplane passenger cabins, the majority of which (88 percent) were loaded. This is a testament to the security proficiency of our screening officers.
- Trained 4,409 flight crew members in Crew Member Self-Defense training to address increasing trends in unruly passengers and partnered with the Federal Aviation Administration to rescind TSA PreCheck eligibility for passengers who are disruptive aboard flights or during security screening. In especially egregious situations, TSA has taken action to limit individuals from flying in the future if they are assessed to pose a threat to aviation security.

- Expanded the Transportation Security Officer (TSO) new hire training from two to three weeks, providing additional instruction on image interpretation, TSA culture, enhancing the passenger experience, and improved cognitive performance. Additionally, TSA launched TSA Academy West adjacent to Harry Reid International Airport. With this additional training capacity, TSA trained over 9,000 TSO new hires in FY 2022, with almost 1,000 of them attending training at Academy West.
- Established the first outcome-focused cybersecurity-related Security Directives and Security Program Amendments that require mandatory incident reporting and the adoption of mitigation measures to the most critical owners and operators of transportation infrastructure. TSA is committed to enhancing and sustaining industry's resilience to cybersecurity attacks. TSA is working on a rulemaking that will permanently codify critical cybersecurity requirements for pipeline and rail modes.
- Published Information Circulars to Transportation Systems Sector stakeholders with recommended actions to reduce vulnerabilities associated with cybersecurity-related threats.
- Published the Innovation Doctrine—the first of its kind in government, which lays out agreed upon current best practices and establishes mechanisms like Local Innovation for TSA (LIFT) Cells across the country to foster a culture of innovation, provide resources and pathways to solve local-level problems, and expand the innovation ecosystem around transportation security. It also creates an Innovation Pipeline, a disciplined, repeatable, and scalable process for innovation across TSA to out-innovate those that threaten the traveling public, and leverages the TSA Innovation Task Force's expertise in the evaluation and demonstration of promising technologies.
- Continued several programs and initiatives to recruit and retain TSOs, including:

- A performance-based rewards program called the Model Officer Recognition that provided 19,478 monetary awards or pay increases to top-performing TSOs in FY 2022;
- Authorized TSO retention incentives at 143 airports, benefitting more than 10,000 employees nationwide. Although these are still needed in certain locations moving forward, the changes in TSA pay structure afforded by the FY 2023 enactment will dramatically reduce the need for these incentives.
- Expanded digital identity technologies that securely enhance the customer experience, including testing TSA PreCheck touchless identity solutions, collaborating with Apple and other private sector partners to incorporate mobile driver's licenses (mDL) into security checkpoint operations, and publishing an Identity Management Roadmap which lays out a comprehensive end-to-end strategy for identity management at TSA.
- Established two Unmanned Aircraft System (UAS) Test Bed Programs—one at Miami International Airport and the other at Los Angeles International Airport—to test and evaluate detection, tracking, and identification technology for UAS that enter restricted airspace. TSA continues to collect data on performance of these various technologies to share with industry and government partners.

TSA's vision is to remain agile, embodied by a professional workforce that engages its partners and the American people to address current and future challenges and threats to the Homeland. To that end, within the first year of my term as Administrator, I issued the "TSA Strategy" and established three strategic priorities to guide the agency's workforce through its 25<sup>th</sup> anniversary: (1) Improve Security and Safeguard the Nation's Transportation System; (2)

Accelerate Action; and (3) Commit to Our People. I have twice published Administrator's Intent documents delineating and updating the short and medium-term goals and objectives to achieve those strategic priorities. I will publish the third iteration of the Administrator's Intent, in close consultation with your staff and our stakeholders, which will focus on the 20 most critical cross-cutting issues that require collaboration across the entire agency with senior executive accountability. The Administrator's Intent 3.0 is aligned with the Department of Homeland Security's priorities as well as national strategies and directives including the National Security Strategy, the National Cybersecurity Strategy, and the Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.

We have also strengthened our partnerships across the spectrum—from private industry, to foreign partners and international organizations, advisory committees, academia, state and local governments, and our federal partners—in order to increase collaboration, security, information sharing, and maximizing the customer experience in the new travel environment while minimizing negative impacts on travelers and commerce.

Securing and safeguarding the Nation's transportation system requires innovative tactics to address cybersecurity threats and risks associated with the continued integration of advanced electronic and networked systems. The FY 2024 President's Budget includes an increase of \$10.4M for cybersecurity staffing, as well as the development and implementation of enhanced cybersecurity-related measures to improve cyber resiliency across the U.S. Transportation Systems Sector. Across the transportation sector, TSA continues to help partners build cyber resilience and improve incident response, focusing on the surface, rail, and aviation sub-sectors. With those stakeholders, TSA hosts a variety of planning meetings, intelligence briefings, and

tabletop exercises to ensure partners are aware and prepared to respond to emerging issues. I have personally visited pipelines and other critical infrastructure operators to discuss the evolving cybersecurity threat, and to understand the challenges and successes of implementing the current security directives and program amendments.

This year, as required by Congress, TSA will deliver for the first time an unconstrained Capital Investment Plan that describes an ideal future state in which TSA is able to buy down more risk to the transportation sector with additional resources. It is imperative that TSA continues to invest in, acquire, and field new technologies to strengthen transportation security.

The transportation sector will remain a top target for malicious actors including international and domestic terrorists due to the prevalence of soft targets within the sector, the public accessibility of many transportation modes, and the importance of transportation infrastructure to the Nation. The agency carefully monitors this evolving threat environment and the need to strategically manage risks. Risk-based decision making is inherent to the TSA mission of protecting the Nation's transportation systems to ensure the freedom of movement for people and commerce. The challenges and risks TSA encounters will foreseeably become more complex, and the agency needs to position itself to be both more strategic in responding to risks and in developing solutions. A critical dependency in risk mitigation is sufficient funding that would allow TSA to continue to evolve transportation security in high-risk areas.

In conjunction with the FY 2024 President's Budget, the Administration offers two proposals to increase availability of funding to resource TSA's strategic priorities and help TSA address emerging threats. First, it includes a legislative proposal to terminate TSA's deficit reduction contributions from Passenger Fee collections, which, if enacted, will provide an

additional \$1.6B to directly offset TSA's appropriated funding and return the funds to use for their intended purpose. Second, the Budget includes a legislative proposal to transition access control at exit lanes to airport authorities and commercial airports under federal regulatory authorities, which will result in a projected savings of \$111.0M. If approved, TSA will work with airports to integrate exit lane security into their perimeter security plans and assess those plans regularly. The proposal will enable TSA to better focus its resources on screening functions and risk-based security measures.

TSA's level of success is influenced by the help of Congress as well as our professional, vigilant, and engaged workforce. That is why "Commit to Our People" is one of our three strategic priorities. The initial funding the Committee provided in FY 2023 to TSA allows for that continued commitment. The FY 2024 President's Budget includes \$1.4B to fully support the TSA workforce pay initiatives started in FY 2023.

The strategic priority of "Commit to Our People" also entails ensuring that we provide our workforce with the necessary advanced technology to be successful. Today's evolving threats require a dynamic and responsive TSA. Access to greater technology enables our passenger screening workforce to assess potential threats quickly and efficiently and also supports a more seamless experience for the traveler. To that end, the FY 2024 President's Budget includes \$70.4M and \$11.0M to procure additional systems within the Checkpoint Property Screening System (CPSS) and Credential Authentication Technology (CAT) programs, respectively, to address capability gaps to detect new and evolving threats to civil aviation in current property screening technology reliably and efficiently, while improving the customer experience. Our field officers have done a tremendous job being diligent by monitoring the



threats at the checkpoint. However, it is imperative that we equip them with the necessary tools to combat those persistent threats. As of today, TSA needs a total of 3,585 CAT and 2,263 CT machines to reach Full Operational Capability (FOC). Currently, CPSS procurements are an estimated 35 percent of FOC, which puts deployments at approximately 28 percent for CPSS and 57 percent for CAT. Based on past, present, and current projected funding, TSA will meet FOC for CAT machines and CPSS in FY 2049 and FY 2042, respectively. Full and dedicated funding for CPSS and CAT are imperative for our nation's security at the checkpoint.

Furthermore, there are a number of investments in Operation and Support that require sustained funding to ensure the transportation sector stays secure. Some of these investments include:

- \$251.0M to provide the TSA workforce a 5.2 percent pay raise.
- \$39.0M for Transportation Security Equipment Maintenance to fund anticipated maintenance costs of TSA's checkpoint and checked baggage screening technologies based on current contractual requirements.
- \$19.0M and 24 Positions for the implementation and expansion of the REAL ID Program.
- \$11.3M for maintenance, technical support, and engineering contracts for Credential Authentication Technology.
- \$10.0M to properly support the National Deployment Office Travel increases.
- \$4.5M and 45 Positions to establish a dedicated pipeline security assessment team to conduct inspections and assessments on the Surface Transportation System.
- \$3.8M to enhance TSA's Insider Threat Program.

- \$2.7M and 6 Positions to support Executive Order 14058 to enhance Customer Experience Strategic initiatives.

As you know, TSA was established by the *Aviation and Transportation Security Act* in the wake of the September 11<sup>th</sup> attacks and was given the urgent task of protecting our nation's transportation systems. Since that day, we have remained steadfast in our commitment to provide the highest level of security across all modes of transportation and work with our partners to stay ahead of evolving threats. In the years since 9/11, and specifically over the past fiscal year, TSA has not only had to address ever-present physical threats to aviation, but also dynamic and emerging cybersecurity threats to our nation's aviation, rail, as well as hazardous liquid and natural gas pipeline infrastructure. TSA works closely with the transportation industry to provide agile and responsive security across all modes of transportation through passenger and cargo screening, vetting and credentialing personnel in critical transportation sectors, law enforcement, regulatory compliance, and international cooperation.

Today, within the aviation network, TSA is responsible for the security of over 430 federalized airports, with screening services forecasted this summer for over 22,000 domestic flights (at pre-pandemic levels) and nearly 2,300 outbound international flights per day. With travel volume rebounding, TSA routinely screens more than 2 million passengers, 5 million carry-on bags and 1.4 million pieces of checked baggage daily for explosives and other dangerous items, and in many locations across the nation. TSA expects passenger volume to eventually exceed our pre-pandemic FY 2019 levels, which averaged up to 2.3 million per day. The FY 2024 President's Budget includes \$197.1M to enable TSA to continue to recruit and retain a workforce able to meet increasing demands of passenger travel volume and maintaining

security effectiveness. In addition to these core security functions, we also ensure regulatory compliance in aviation through the work of more than 1,285 aviation, cargo, and surface transportation security inspectors.

In the surface realm, TSA works closely with transportation system owners and operators to protect the critical surface transportation systems that connect cities, manufacturers and retailers and power our economy through more than 4 million miles of roadways; nearly 140,000 miles of railroad track; more than 470 tunnels; and over 2.8 million miles of pipeline. TSA's security inspectors conduct approximately 8,000 surface inspections annually in pursuing a risk-based approach for securing a large and complex network of transportation systems and critical infrastructure.

Since TSA's creation, the modes and methods of terrorist attacks have become more decentralized and opportunistic, and aviation and other transport hubs remain high-value targets. Threats to aviation and surface transportation are persistent and constantly evolving. To meet these challenges, we must continue to be responsive, innovate, rapidly deploy new solutions, and maximize the impact of our resources.

The FY 2024 President's Budget aligns with TSA's strategy to improve security and safeguard the nation's transportation system, accelerate action, and reinforce TSA's commitment to advancing its strategy. Thanks to Congress' support for TSA through the FY 2023 enactment, the FY 2024 President's Budget honors commitments to our workforce by providing appropriate compensation and other benefits while addressing capability gaps to ensure that the nation's transportation security remains the safest in the world.

Securing our nation's transportation system is a complex task that requires robust partnerships and a well-trained, dedicated workforce. Funding in the FY 2024 President's Budget will have a positive impact on all TSA employees—from Transportation Security Officers, Federal Air Marshals, inspectors, canine handlers, analysts, and management to administrative and professional employees—as well as on transportation security and the passenger experience. To achieve the priorities reflected within the FY 2024 President's Budget, we will continue to engage with industry and stakeholders, invest resources in our employees and technology, and encourage the public to be part of the solution. Finally, through constructive oversight and dialogue, we seek to continue to partner with Congress as we work to secure all modes of transportation for the public.

Chairman Joyce, Ranking Member Cuellar, and members of the Subcommittee, thank you for the opportunity to testify before you today. I strongly believe that the TSA priorities outlined in the FY 2024 President's Budget are not only necessary but timely and vital to our economy. As always, we will be very responsive to addressing any questions that you might have throughout this budget process and I look forward to this discussion and your questions. Thank you.

Mr. JOYCE. Thank you, sir.

I will start with questions, and I will start with myself.

I mentioned in my opening statement my concern with the requested level for technology procurements, including computed tomography machines. CT machines apply sophisticated algorithms to detect weapons, explosives, and other prohibited items.

Can you describe how this technology impacts the aviation's security system and what benefits they provide to TSOs and the traveling public and how this is critical to the technology—how this is important technology to the aviation security?

Mr. PEKOSKE. Mr. Chairman, thanks for the question.

The computed tomography, or CT scan x-rays that we are installing in our checkpoints are medical grade x-ray systems. What they provide more than anything else, is they provide the ability to detect a very small amount of explosive, which we know we need to detect and prevent a catastrophic event with an aircraft in flight at 35,000 feet.

So the detectability is very consistent with our requirements for detection in our checkpoints, and it has other benefits of providing additional speed and also providing additional convenience for passengers.

For example, with the computed tomography x-ray technology, passengers don't need to take out laptops or liquids, aerosols, and gels out of their carry-on bags if they are a PreCheck passenger because the technology can actually see around those items with the way it works from a detection standpoint.

So this project has been critically important to us. We have got CT x-rays deployed at about 40 percent of our checkpoints nationwide. So we are not quite halfway there, but with the funding levels to the points that both you and the ranking member made in your opening statements, this program will not be completed until 2042. That is a further delay from where it was just last year.

Last year, at last year's funding levels, we thought we could get this completed in 2036. Now, with the funding levels that are reduced to the top-line constraints, this is going to be moved out to 2042.

Mr. JOYCE. Fair to say in those 40 airports where it has been deployed, that it has sped up the process of passenger handling?

Mr. PEKOSKE. Where it has been deployed, Mr. Chairman, at 40 percent of the airports already, or 40 percent of the lanes, more properly, in our system, yes. In fact, the large systems, which have a technology called an Automatic Screening Lane imbedded within the x-ray system, five passengers at the same time can take things out of their carry-on bags and put them into bins if they need to be taken out.

That is much better than doing it one passenger after the other. In other words, you don't have to wait for the passenger or two or three passengers in front of you.

We found significant improvements in the ability of that technology, combined with those automatic lanes, to process passengers compared to what we currently can do.

Mr. JOYCE. It is fair to say that under the current funding plan, it would take two decades to roll this out. If, in fact, we, the committee, were to fund the technology to the requested level, does

TSA have a strategy in place to accelerate this plan in future years?

Mr. PEKOSKE. Mr. Chairman, this is one of the rather unique situations in the Federal Government where the agency requesting the funding not only knows exactly what it wants to buy and has tested it both from a, "Hey, does the technology work perspective," but also does the technology work in our environment perspective.

So we tested it. We know what we want to buy, and we have contract vehicles already in place. And so, you know, we could spend, with our current contract vehicles, and successfully install. So it is one thing to be able to buy a lot and store them. That is not what I am saying. We could buy about \$350 to \$380 million worth of CT technology. That would accelerate this project by many, many years.

So, you know, we are in a position where we know what we want. We have tested it. We have had operational experience with it. We have contract vehicles in place, and we have an implementation plan.

Mr. JOYCE. Has TSA performed an analysis on impacts to TSO's staffing requirements as more capable screening equipment is deployed to the airports? And do you anticipate this will reduce the number of TSOs needed to staff a checkpoint and maintain the same passenger throughput?

Mr. PEKOSKE. Yes, sir. We have started that. We started extensively. It would reduce the rate of growth for screening officers because, you know, what we expect to see over the next many years, we are already seeing it from fiscal year 2022 into 2023. We will certainly see it from 2023 into 2024 is a return to increases in passenger volumes.

Pre-pandemic, it was about 4 percent year over year. We expect to see that beginning in fiscal year 2024. So, you know, from our perspective, we won't need to grow the workforce nearly as much as we would have had we not had this technology in place.

Mr. JOYCE. Thank you.

I will notice my dear friend, Ranking Member Henry Cuellar, for any questions he may have.

Mr. CUELLAR. Thank you, Mr. Chairman.

Mr. Administrator, under the 2010 law, there was a 2010 law that called for every agency to make sure they set up their strategic plans, their performance measures, their mission, their vision, their goals, their objectives. And I have looked at your strategic plan and the performance measures, and one of the things we said earlier today is at the State level, State legislature, there is this working collaboration with the agency and the legislatures.

And one of the things I would ask you is if you would be willing to work with us on reviewing some of this because the way the Federal Government does it is that you all set up your own performance measures.

And with all due respect, not you all but there are some agencies that just put performance measures so they can pat themselves in the back. They look good.

But measuring activity is one thing. Measuring results, which is what I think you are looking at, is a little harder.

So I would ask you later on, once we get past this appropriation process, sit down with us to go over some of the work that you all have done on that.

The other thing is what the chairman was asking. On the procurement acquisition part, it is going to take a long time, and I think this is a problem that we have with almost every agency. It is, you know, we buy things and it costs the taxpayers dollars. You don't have enough competition at times, and we have got to find a better way.

So one of the things that, you know, we would ask you is, you know—and I am sure, you know, to improve it, some of the steps are you have to have some clear goals, a metrics as to what you want to do, look at the—streamline the acquisition process. If you can do it in 1 year, instead of 5 years, let's do it because I think waiting until 19—what is it, 2042 or whatever, that is a long time.

You know, making sure that we are working with the stakeholders, which means, you know, the private sector also. And, of course, making sure that you have the right procurement or acquisition professionals because if the people that you hire—and I am not saying that, but if an agency hires some people that don't know and the other side knows more, you know what is going to happen there.

So, we certainly want to work with you on the procurement process, and any ideas that you have, any authorities that you think you might have besides money, because it is money and authorities, we want to go over that.

Mr. PEKOSKE. Yes, sir. And thank you for your comments, and I agree with everything that you said.

And let me go back to the strategy piece for a second, if I could. When we developed our strategy, which we published in 2018, we intentionally made it a longer-term strategy, because I wanted to bring some stability to the agency in terms of an strategic direction. But it was especially important that we included the inputs of all of our stakeholders, members and staff up on Capitol Hill, members of the industry, other Federal partners, our international partners.

So we got a lot of very robust input, and what you see is that strategy document that goes out into our 25th anniversary in 2026.

To go with it, there are documents that I publish every 2 or 3 years called Administrator's Intent documents, and these documents are basically looking at the strategy. What do we need to accomplish in a 2-year window? Because things are going to change every couple of years. What do we need to accomplish in a 2-year window to be able to achieve the strategy, which should be relatively stable?

So we are now developing the third version of that Administrator's Intent. We have already shared it with your staff.

So we have done a robust industry engagement, because I agree with you. I mean, getting as much input as we possibly can is going to get a better product, and it is going to make sure that we have more people buying into what we collectively need to do, because we are not a single actor in this environment.

The other thing I would offer, in addition to the great things that you mentioned with respect to acquisition, is having a steady level

of funding. If I am a vendor and I am looking at an agency as a customer, knowing that that agency is going to have a relatively steady level of investment or a predictable level of investment means that I am willing to spend a little bit more money up front on our research and development, for example.

Or it means that, hey, if I might be sitting at the sidelines saying, "Hey, this is a short-term acquisition or it is only going to go to a couple of vendors," I might sit on the sidelines. But if I see a pot of money out there that is an addressable market for me, I might come into that market.

And, for us, what we want is more competition. More competition develops a better product, and it generally reduces price.

The other thing I would add to your list, and we are doing this with our CT investments, is making sure that we buy things based on widely-accepted standards, that we aren't developing proprietary systems. Because if you develop standard-based systems, and our standards are based on standards that are established internationally and domestically, not established necessarily by the agency, you are going to get more vendors that are going to participate in what you are doing as well. And plus, you are going to have more flexibility in the long-term.

Mr. CUELLAR. And the cost will go down.

Mr. PEKOSKE. Cost will do gown.

Mr. CUELLAR. Thank you.

Thank you, Mr. Chairman.

Mr. JOYCE. The chair recognizes Mr. Cloud.

Mr. CLOUD. Thank you, Administrator, for being here.

I wanted to see if you can help us clear up something kind of on another issue that TSA has been dealing with.

At some point, were migrants flowing through our traffic system, through airports, going through TSA?

Mr. PEKOSKE. Yes, sir. Migrants, on any given day, do travel domestically in the United States.

Mr. CLOUD. Still?

Mr. PEKOSKE. Yes, sir.

Mr. CLOUD. A lot of that is transferred to private carriers now, or charter flights?

Mr. PEKOSKE. There are so charter flights, but they also do some commercial flights.

Mr. CLOUD. Okay. Could you speak to the identification that is required for those?

Mr. PEKOSKE. What we do is we have an application on the smartphones of the airports that we know that migrants will typically fly from. It is called CBP One, and it is an application developed by Customs and Border Protection.

Mr. CLOUD. That is really new, though.

Mr. PEKOSKE. It is new, right, and we have been using it robustly. In fact, you know, 99.7 percent or so of all the migrant travelers use the CBP One app for identification.

Mr. CLOUD. Okay.

Mr. PEKOSKE. So it is a biometric match.

Mr. CLOUD. Yes. And how do they—well, up until now you have used arrest warrants, right? Warrants for removal and deportation,



order of release and recognizance, or supervision notice to appear in arrival departure forms as well?

Mr. PEKOSKE. Not exactly. And to explain that, a migrant that might not be able to use the CBP One app, which are very, very small numbers—so to give you a sense of scale, on average, we verify the identity that CBP has established when these immigrants cross our border.

Mr. CLOUD. How do they establish the identity? That was going to be my next question.

Mr. PEKOSKE. Sure.

They have their own process where they capture biometrics. They take the identity information that the individual has on his or her person and go through a process of—

Mr. CLOUD. Which usually isn't anything?

Mr. PEKOSKE. That is CBP's process.

Mr. CLOUD. Right.

Mr. PEKOSKE. And they are in the best position to speak to that.

Mr. CLOUD. Yes, I realize that is not your doing. You are going with what they are giving you, the information they are giving you.

Mr. PEKOSKE. Right. But what they have decided, though, is they have decided to admit legally this person into the country, and they have established their identity upon admission coming into the country.

What we check is, is this the same person that CBP encountered, and that biometrics match does that.

Mr. CLOUD. Right.

Mr. PEKOSKE. To your question on the civil arrest—

Mr. CLOUD. But there is still a loophole as to whether that person is actually who they are saying they are when they come, but that is not your purview.

But the point is that there are people potentially flying on our flights that might not be who they say they are. Not because of TSA. I want to clarify.

Mr. PEKOSKE. We trust the identity that CBP has provided to us.

But to go back to the civil arrest warrant question you had for just a second, on any given month, there are—in the month of March, there were nine individuals to date that have come in with one of those forms. And what we do is you can't just present that form and say, "Hey, this is my identity," and then you are processed through our screening process.

What that does is it has on it a file number, and what we do is we take that file number, and we call CBP and get the information from that file number, including identifying characteristics of that person to satisfy ourselves. The same idea, that this is the same person that CBP encountered at the border.

The other really important thing to keep in mind, sir, is that every single person, whether it is a U.S. traveler or a non-U.S. traveler who doesn't have the identity credentials that we established, goes through enhanced screening.

So, you know, we do full-bag searches. We do on-person searches of all of these individuals, irregardless of where they are coming from.

Mr. CLOUD. Now, during COVID, thankfully we are past that, but there were COVID restrictions on U.S. citizens coming into the

country but not on migrants coming into the country, I guess, through CBP.

Mr. PEKOSKE. Well, title 42 was established. That limited the number of migrants coming into the country. And again——

Mr. CLOUD. Well, yes, but that is—anyway.

Mr. PEKOSKE. Right. But folks coming into the country——

Mr. CLOUD. Moving on, I wanted to ask you about—just to get your take on data collection. What data does TSA collect? What do they do with the data? How long do they store it? Do they share it with other agencies? What is your general policies on——

Mr. PEKOSKE. The data we collect on any passenger, sir?

Mr. CLOUD. Yes.

Mr. PEKOSKE. Sure.

So for any passenger, we collect their name, their date of birth to verify their identity. And we also verify that they have a flight that day from that airport. So those are the two things we look at is, “Hey, is this the person that we vetted through our systems that we are going to permit to travel today?” And, you know, have they changed their flight reservation that might be different than a paper boarding pass?

It also prevents any boarding pass fraud that we might have seen in past years.

Mr. CLOUD. Right.

There was some talk of—I guess I saw a headline that you are working to implement facial recognition. Could you speak to that and how that will be used?

Mr. PEKOSKE. We are in an operational assessment phase for facial recognition, and basically, this is, at this stage, primarily one-to-one facial recognition.

So if you go up to our screening checkpoints, there is a technology that we are investing in. We have had great support from this subcommittee for this investment. That allows the passenger, rather than the officer, to insert their driver’s license or their passport into the technology.

What that technology does is it takes from the driver’s license, let’s say in this case, the name, the date of birth, and the digital photo, and then takes that digital photo and displays it on a larger screen for the officer. And so the officer looks at the passenger, sees if what is on the screen matches the enlarged photo that is there. If so, then that passenger’s identity is verified.

There is a further enhancement to technology where we have a camera system now that we are prototyping in the second version of this identity technology that the camera takes another photo. And then there is a one-to-one comparison of the photo the camera takes digitized and the photo on the driver’s license or passport that is digitized.

What we have found in our testing is that that is much more accurate than a human. And of course, you know, I think most people would assume that would be the case. It is very hard to look at, you know, a photo and do a quick match.

Mr. CLOUD. It is usually the worst picture of all.

Mr. PEKOSKE. Right, right. Yes. Yes. Yes.

And then we are, for PreCheck passengers, testing out a one to small number comparison where we would pre-load—for PreCheck

passengers, when you enroll in PreCheck or Global Entry, you voluntarily provide your passport information, and we have your passport photo, or your driver's license photo. And what we do is we pre-load those photos onto our technology for the people that we know have a reservation for a flight that day.

And when they walk up to the technology, there could be just a no exchange of a credential, but a match of the photo that is stored in the gallery with the photo that the camera takes.

Mr. CLOUD. Okay. And that information would stay within TSA, I guess?

Mr. PEKOSKE. Yes. In fact—thank you. All the information that we do on processing people operationally for biometrics, as soon as that passenger walks away from our technology and the next passenger comes up, we erase that data completely. We don't retain it.

Mr. JOYCE. Thank you.

Ms. Underwood.

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Mr. Pekoske, thank you for being with us today. It is nice to see you again.

Mr. PEKOSKE. Thank you.

Ms. UNDERWOOD. So I fly in and out of O'Hare a lot, and I can tell you on my trips following the fiscal 2023 omnibus bill being signed into law, the TSOs were very excited, and they told me how relieved they felt knowing their pay raise was included in the bill, the new law.

And I am excited, too. It has been a long time coming, and it is thanks to these officers who have been unionizing and advocating for the past 20 years that Congress is able to get this across the finish line.

As you have explained already, pay equity will have an immense impact on employee morale, workforce retention, and job satisfaction, and it will allow the TSOs to develop their careers at TSA instead of leaving for other jobs that can offer higher pay.

Now, this is no small feat, and it needs to be celebrated. I believe in putting people over politics. I know that House Republicans have put forward a plan that would involve some cuts, and we cannot be rolling back these well-fought, important pay increases as part of this larger debate.

I know that TSA personnel still do not have full collective bargaining rights, and we know that collective bargaining is good for workers. It raises wages, increases benefits, and makes workplaces safer.

Can you tell us more about why collective bargaining would be beneficial for the TSA workforce specifically? And, from your perspective, why is it a necessary next step following pay equity?

Mr. PEKOSKE. Thank you very much for your comments.

And, yes, collective bargaining is an absolute critical part of our effort to improve the workplace environment, and to improve our ability to attract and retain talent in the Transportation Security Administration.

Full collective bargaining was approved. The resources were approved in last year's budget. And once those resources were approved, I approved full collective bargaining for the screening work-

force in TSA. We have been very diligent about working and getting a collective bargaining agreement negotiated and in place. That work is going on very, very well.

But to the points that you made, this is making an enormous difference in our workforce. You know, one of the things that I looked at very carefully when I was going through my confirmation hearing for TSA were the Federal employee viewpoint survey results for the TSA workforce. I mean, this is a survey that Federal workers take every single year, and it gives you a year-to-year comparison as to how we are doing in workplace environment, how people feel about their promotion potential within the agency, how they feel about the way they are treated within the agency.

TSA's results were—well, let me put it this way, had room for improvement.

Ms. UNDERWOOD. Yes, sir.

Mr. PEKOSKE. And I tried everything in my first 3 or 4 years as the Administrator, to put programs in place to, first, address the pay issue, but I could only do a very small part because I was on a very limited budget.

As I looked at it, it became really clear to me that, one, we need to fix the pay. To have a portion of the Federal workforce that has critical national security responsibilities not getting the same pay as their Customs counterparts that are literally in the same airport is unconscionable, right? And no surprise we were losing a lot of people as a result of that.

Secondly, we need to make sure that we do everything we can to have people view TSA as a career of choice.

Ms. UNDERWOOD. Right, but I asked about collective bargaining, sir.

Mr. PEKOSKE. Sure. And collective bargaining will give all of our screening workforce more of a voice in what is going on—

Ms. UNDERWOOD. Right.

Mr. PEKOSKE [continuing]. And much better communications.

Ms. UNDERWOOD. Thank you.

Mr. PEKOSKE. And we can make improvements there.

Ms. UNDERWOOD. Okay. Thank you so much. I look forward to working with you to fully implement the collective bargaining rights.

Mr. PEKOSKE. Thank you.

Ms. UNDERWOOD. Now, you and I share the priority of keeping the TSA workforce safe, as well as passengers and airport employees. Our Nation's gun violence epidemic has a direct effect on the security of our skies.

Can you tell me how many guns were discovered in airports by TSA last year and how many were loaded?

Mr. PEKOSKE. Yes, ma'am. 6,542, and 88 percent were loaded.

Ms. UNDERWOOD. 88 percent were loaded.

How does that number compare to previous years?

Mr. PEKOSKE. It is higher than every previous year, and the next highest year was the year before.

Ms. UNDERWOOD. What other trends or novel threats are you seeing related to firearms?

Mr. PEKOSKE. We are seeing firearms just being carried much more commonly across the entire system, and we have done a lot of things to deter that behavior. It is not having a big effect to date.

Ms. UNDERWOOD. What are you seeing in terms of long guns?

Mr. PEKOSKE. We rarely see long guns. Although, we see them on occasion. Recently, we have seen two, which is unusual.

Ms. UNDERWOOD. Two? In this fiscal year?

Mr. PEKOSKE. So far in this calendar year.

Ms. UNDERWOOD. In this calendar year. Yes, sir.

No one should have fear of mass shooting at work. Hard stop. No one should fear a loaded gun being on a plane with them either. And thanks to screeners, like our TSOs, 5,642 guns have been prevented from making their way onto planes full of passengers, but we need to do more as policymakers to see this trend go down.

Thank you, Mr. Pekoske.

I yield back.

Mr. PEKOSKE. I appreciate it.

Mr. JOYCE. Thank you.

Mrs. Hinson.

Mrs. HINSON. Thank you, Mr. Chairman.

Administrator, it is great to see you again. Thank you so much for coming before our committee again and for all you do to help keep Iowans and Americans safe while they fly.

I wanted to just share a quick story with you. And this man was actually my State of the Union guest this year, but his name is Sergeant Trent Dirks. And he brought a challenge to my attention that he faces when he travels, because he flew out here to Washington, D.C., and he flies with his service dog, Tracer.

Sergeant Dirks, obviously, served our country valiantly. He came back from that service with PTSD. And, unfortunately, that is an affliction facing many of our servicemen and women when they come back.

But Sergeant Dirks founded an organization in Waverly, Iowa. It is called Retrieving Freedom. It paired him with his service dog, Tracer, and he has been able to improve his quality of life and get out and travel and share the good word.

So, unfortunately, what he flagged for me was that they are facing some challenges when they travel with their service dogs, a lack of consistency. Sometimes the collars have to come off. Sometimes they don't.

It can place our veterans in a position where they are, again, re-traumatized, and it is confusing for the service animal as well. So it provides additional barriers and complications when they are trying to go through TSA security.

So I think that when you look at that added stress and anxiety-inducing situation, I think that there may be room for improvement there. So I would ask today would you commit to working with me to improve that process so there is consistency across all airports for our veterans flying with service animals?

Mr. PEKOSKE. Yes, ma'am. I appreciate your advocacy, and I am absolutely willing to work with you.

We do have a passenger support specialist program that you can call and ask for assistance prior to arrival at the checkpoint, and

that is something that we are trying to expand and make more available throughout our system.

But absolutely willing to work with you and look forward to it.

Mrs. HINSON. Yes, I think consistency is the biggest challenge here, right. We want to make sure that every veteran can count on the same process, no matter what airport they are flying through.

Another area, and it is kind of a pivot here, but to drugs and looking at and trying to counterdict those drugs. When we look at the fentanyl crisis facing our country, I think we need to be looking at true, meaningful solutions, and I think you are on the front end of fighting a lot of that.

We have to control this mass flow of illicit drugs through our systems, and I think some of it is on increasing penalties for traffickers in our homeland. And it is our, obviously, responsibility as members to enact legislation to do that.

But can you maybe speak to some of the increases you may have been seeing in terms of illicit drugs, fentanyl, synthetics, counterfeit drugs? What are the latest tactics that you are employing at TSA to help counter the traffickers and the drug cartels?

Mr. PEKOSKE. Thank you for the question.

You know, we see drugs transported through our system in checked baggage sometimes, on persons sometimes, and certainly in carry-on bags. One of the things that we do, and this is where we find a lot of drugs, is on a person. And sometimes we get criticized for the pat-down process we have, but the pat-down process, we know from our own testing, is absolutely critical to detect where people might be able to secrete something on their person. So, you know, a lot of progress there.

But also, in the carry-on bags, we see good quantities of fentanyl coming through our screening checkpoints. Our process is to identify it, call the local law enforcement officials over, and then they take care of the situation from there.

Mrs. HINSON. How frequently are you encountering folks traveling with fentanyl?

Mr. PEKOSKE. We see fentanyl every single day. So it is not an uncommon occurrence.

Mrs. HINSON. Is it mostly the pills? Is that the—

Mr. PEKOSKE. Mostly the pills, yes, ma'am.

Mrs. HINSON. Okay.

Mr. PEKOSKE. And sometimes in pretty large quantities.

Mrs. HINSON. So I know I was in Chicago a few months back, and there was a drug-sniffing dog, obviously, going around our gate. Is that a situation where they might be able to get something on the second sniff, so to speak, if it doesn't get caught in the initial screening process?

Mr. PEKOSKE. Our dogs are explosive detection screening canines. So they are not trained to screen for any drugs whatsoever. But local law enforcement dogs can be trained in that regard.

Mrs. HINSON. And do you partner with them inside the airport, or is inside the airport—

Mr. PEKOSKE. We do. Inside any airport, I mean, there is just not enough capacity to go around between local law enforcement and the Federal law enforcement agency, CBP and TSA, generally.

Mrs. HINSON. All right. Thank you, Administrator. I appreciate you. Thank you.

Mr. PEKOSKE. I appreciate it. Thank you.

Mr. JOYCE. Thank you, Mrs. Hinson.

I recognize Mr. Trone.

Mr. TRONE. Thank you, Mr. Chairman and ranking member.

Mr. Administrator, thank you for being here today. We appreciate your help.

As someone who grew a business from employee one to 12,000 employees, I get it that you have got to recruit the best folks, the best talent for your team. You need pay equity, and, hopefully, better benefits and better pay than your competitors to get the best folks.

So, Mr. Administrator, as you are preparing to implement these new salaries July 1 of this year, which is fantastic, to get equivalency, the President's budget includes sufficient funds to continue that new pay plan in 2024.

If this committee does not provide that level of funding, what would be the consequence?

Mr. PEKOSKE. Thank you for the question.

The consequences would be pretty dire for passengers in particular because it will force us to, arguably, furlough a good number of people. And I can see a situation where if we don't get the pay, the funding we need to continue the pay into fiscal year 2024, that we will have wait times in major airports of 2 hours or longer.

And that creates, obviously, the inconvenience of passengers, all of us here included, but also a security problem, because you have got a lot of people in a public area of an airport that are easy targets for somebody that might want to do some harm. So I hope it doesn't come to that.

But, you know, to your point, I think paying people fairly and paying people for—that recognizes the importance of the position that they hold, and how hard a job it is—I mean, people don't realize that is a hard job to do. I get tired sometimes just watching 15, 20 minutes of video that I review on occasion for our operations, and I am in our checkpoint operations all the time personally.

So I appreciate the comments, and it will have very, very significant impacts on travel.

Mr. TRONE. Tough job on your feet the whole time, dealing sometimes with difficult folks.

Mr. PEKOSKE. And you know you can't make a mistake, right.

Mr. TRONE. I think that is part of the problem because when you have got a line there for 2 hours, versus a normal line, all of a sudden, sometimes shortcuts get taken, and you can't afford, or your team, to take a shortcut because it puts major risk out for the population.

Mr. PEKOSKE. Well, and the other thing that happens, too, is as an officer, you might not be able to work just a 40-hour week. You know, you might be working 60-hour weeks, week after week after week. That induces a lot of fatigue as well.

And, plus, that is a big detractor for somebody wanting to stay with the agency. Because as you know from your own business experience, keeping your great employees with you is a key objective of any organization.

Mr. TRONE. Would you be forced to return to the old pay scale?

Mr. PEKOSKE. No. I would not return to the old pay scale. I don't think that is right. I fundamentally believe that people ought to be paid a fair wage for the work that they do, especially when they have a national security position in place.

Mr. TRONE. I absolutely agree with you 100 percent.

As you stated, the transportation sector certainly is a high value target for international, domestic threats due to the number of easy public access, not much protection. How would the proposed budget cuts affect the technology that you deployed to significantly improve safety and security while minimizing the negative impacts on travelers and commerce?

Mr. PEKOSKE. Yes, sir, a great question. And you already see the impacts of it to a degree in the fiscal 2024 request. I mean, our technology request the chairman mentioned in his opening statement is less in fiscal 2024 than it was in 2023. That is a top-line constraint issue. It is not the ability to contract. It is not the ability to identify what we want to buy.

What it also does is it allows us to continue known security vulnerabilities. I mean, our technology is designed to close vulnerabilities. That is the number one reason why we buy it.

Thirdly, you have got a lot of people waiting in line, arguably, and you have old technology, which means it is going to be slower, and they are going to have to go through more motions to get through our screening process, where the new technology eliminates some of those steps.

Mr. TRONE. What is the exact fee that you charge a passenger for passage?

Mr. PEKOSKE. Yes, sir.

The 9/11 security fee is \$5.60 in each direction, \$11.20 round trip.

Mr. TRONE. \$5.60, 11.20.

So what is the thinking of that number times the number of passengers should be the budget? I am not quite sure I am on the same page on that one because it seems like that is a capricious number that you leverage up as you drive more throughput with more efficiency. And probably that number ought to be thoughtfully reduced and charge the passengers less long-term. Or we are just simply charging people to pay down the budget.

Mr. PEKOSKE. Yes, sir.

You know, arguably, you could get the same amount of revenue just with the natural growth in the traveler population, which, as I mentioned earlier, we are starting to see already. So 4 percent growth year over year would increase the fee by 4 percent. That is sort of baked into the budget as it exists today.

But the increase in the budget that was made in 2013, was quite significant. It went from \$2 and something up to \$5.60, but all of that money went to deficit reduction, not to aviation security.

Mr. TRONE. I yield back. Thank you.

Mr. JOYCE. Thank you, Mr. Trone.

I recognize Mr. Newhouse.

Mr. NEWHOUSE. Thank you, Chairman Joyce, Ranking Member Cuellar.



Administrator Pekoske, it is a pleasure to have you with us. Thank you for being here.

And let me just say that, you know, all of us come in contact with your folks on a regular basis, and I have got to tell you, the patience, an example of patience, I should say, by most of the members of your agency, I could never do that job. It would be hard.

But with the increase in air travel that we are seeing, growth over the next several years projected, it is going to tax an already-taxed system.

Just a couple of questions about security improvements. I noticed the exiting—I don't know if I can call this correctly, but the exit lane doors that we walk through now, those were required a couple years ago, 10 years ago, I guess, but now in place most everywhere I think. And so that displaces some individuals.

I am just curious about the funds for the FTEs at those displays. Were those being directed to help facilitate the entrance of passengers coming through the system? Tell me a little bit about that change that you are making in your budgets?

Mr. PEKOSKE. Yes, sir. And thank you and thank you for your comments as well. I greatly appreciate it. And all the officers are listening to this hearing. So they appreciate all of your comments as well on their performance.

For exit lane staffing, I mean, we all would like to get to the point where we don't staff exit lanes. To your point, there is technology in place. It is in place in most airports already. It is more efficient in the long-term, easier for a lot of people, and it doesn't generally make any—it can't get overwhelmed by large numbers of people.

We have in the budget a proposal to reduce exit lane staffing for about the 25 percent of airports that we currently staff the exit lanes. So there are some TSOs staffing exit lanes at 25 percent of the airports, about 109 airports nationwide.

Basically, that number was the number that existed in 2013 when the bipartisan budget agreement was passed. And part of the agreement was that it would require TSA to continue staffing those exit lanes for the foreseeable future.

As we all look at this, I mean, it doesn't make any sense because it costs more money in the long run to do it that way, and really it is not the best application—

Mr. NEWHOUSE. Put those resources to better use somewhere else.

Mr. PEKOSKE. Correct.

Mr. NEWHOUSE. And you want to do that?

Mr. PEKOSKE. We do.

Mr. NEWHOUSE. So maybe you can—in the couple minutes I have left, two things I wanted to ask you about. Some of the technology and modernization that you are looking at, you talked a little bit about the face-to-face recognition thing. So some of those things that you are anticipating.

Then, also a question about the collective bargaining agreements. And help us feel better that the original mission of TSA when it was set up to be responsive to emergent situations, to be able to be flexible and be able to change in a moment's notice, is that impacted by bargaining agreements?

Or how can you make sure that there is flexibility in those agreements so that we can be—you know, do as good a job as possible keeping travel flowing smoothly and safely?

Mr. PEKOSKE. A vision of TSA is to be an agile security agency. In the cornerstone that established our agency, it lists innovation as one of the key attributes of TSA.

You know, we have limited collective bargaining now with our screening workforce. We are about to go to full collective bargaining. In limited collective bargaining, we have been able to maintain that agility. In our efforts, as we negotiate a collective bargaining agreement, we will be able to ensure that because the agility is in the best interest of our workforce as well.

Mr. NEWHOUSE. Agility. I like that word. You have got to be agile.

Mr. PEKOSKE. You do because your threat actors are agile, right. You have got to be more agile than they are.

Mr. NEWHOUSE. So that will be a primary goal?

Mr. PEKOSKE. Absolutely.

Mr. NEWHOUSE. Okay.

Mr. PEKOSKE. And officers are going to want to see that agility. They want a technology solution to a problem we have to be put in place as quickly as it can, because that way they don't have to do a manual process on something, you know, 150 times over on a given day.

Mr. NEWHOUSE. So then any other technology modernization you are looking at?

Mr. PEKOSKE. There are several. One of them is on the on-person screening technology that we use. That is the technology where you walk into a machine and put your hands above your shoulders. We are just now deploying a new software upgrade to that technology that will improve its ability to detect anomalies on a person's body. So security gets better.

It also reduces by about 50 percent, so a big, big reduction in the false alarm rate. Because that technology was very new when we put it out. We knew it had a false alarm rate. We knew we needed to get a software solution to fix that. Well, that solution is being installed right now.

So a 50 percent reduction in false alarms for officers. That is a 50 percent reduction in pat-downs. And for passengers, same thing. So that is going to be a fairly significant improvement.

The other thing that we are working on with respect to identity verification are digital identities. Right now, we have worked with Apple. We have also worked with Google and Samsung to have State DMVs have the ability, if they choose to, to allow one of their license holders to download their driver's license into their wallets on their smartphones.

And then while you do—you know, I use an Apple iPhone, and I am a Maryland resident. So Maryland participates in this program. All I do when I go to the screening checkpoint is I literally tap my iPhone on a reader. It comes up and asks me if I want to transmit the following fields in my driver's license to TSA. I double click it. It gets transmitted electronically. And then there is no exchange of credentials whatsoever.

It is much more secure. A lot more convenient. People will leave home with—will leave some things at home, but they will not leave their smartphone home.

So it also helps us in the process. But we are trying to, you know, get to less friction. So that is a lot less friction in the check-point.

From a health perspective, much better from, you know, just a seasonal flu perspective, to say nothing of the pandemic.

And then digital identity is very, very hard to counterfeit.

Mr. NEWHOUSE. Very good.

Again, thank you for being here and for the work you do.

Thank you, Mr. Chairman.

Mr. JOYCE. You are welcome, Mr. Newhouse.

I am glad to hear we are making some upgrades on that technology. From a guy like me with a replaced titanium knee, I am in there every week.

The budget request includes an increase of \$1.1 billion to pay for the increase of the TSA workforce that we have been talking about. As I said in my opening statement, I support paying TSA employees fairly and taking care of our front-line officers. But the total cost of across-the-board pay increase presents a significant funding challenge.

In 2019, the TSA blue ribbon panel noted that low pay and difficult nature screening jobs were key challenges in the transportation security office retention. However, the panelists specifically recommended against implementing across-the-board pay increases. It also noted that increasing pay alone will not resolve the other leadership, human capital, and IT issues that were identified by the panel.

TSA has long struggled with TSO officer retention. Did TSA consult with any other DHS components or any outside organizations on strategies to improve morale and increase retention that did not involve across-the-board pay increases?

Mr. PEKOSKE. Sir, we looked into all kinds of things. I, as the administrator, had a lot of flexibility under the law that governs TSA to adjust pay as I saw fit. I just needed the funds to be able to do that.

We put a number of programs in place that we thought were going to have an impact, but whenever we did that—and it really goes to the premise of your question—we had a very limited amount of money to do this with. And so, you know, I could provide maybe a \$2- or \$300-a-month bonus for a certain level of activity, but it was fairly limited. And what we saw was it really didn't move the needle at all on recruiting or retention.

When we came out of the pandemic, one of the things that is very fortunate about the United States system is that we have a Federal system, and we were able to maintain our workforce throughout the pandemic. Our workforce was not furloughed. And so when we came out, we already had a good number of people in the workforce.

But we had a really tough time recruiting people to come into TSA because literally they could work for Chick-fil-A for the same amount of money we were willing to pay them, and they weren't

showing up at 4 a.m. In the morning and weren't working 60 hours a week without any discretion.

So, you know, I think there is a whole menu of things you need to look at, and I absolutely agree that pay is not the cure-all for everything.

But one of the things that the Fed survey says unambiguously about TSA, and it says it uniquely about TSA, and basically what the Partnership for Public Service said is pay is always something that any employee is going to say, "Hey, I wish I got more pay." And so we sort of factored that into some of the Fed's evaluations that we do.

But when we analyzed TSA's Fed results over many, many years, pay was a driving factor in dissatisfaction within the agency. And until you fix that, you aren't really going to fix any of the underlying issues either. So, you know, I think that is a fundamental starting point, but it is not the only thing that we are doing.

Mr. JOYCE. The panel also recommended against switching TSA employees to the GS system, but TSA is adopting a system that pretty much exactly mirrors GS scale. Why did you adopt this approach?

Mr. PEKOSKE. We adopted the approach, sir, because we weren't asking for any more or any less than any other Federal employee. And the General Schedule pay system was that template.

What we did was we looked at our counterpart agency in DHS, the Customs and Border Protection Agency, and we said, "Hey, how do they pay their folks?" And we basically used the model that they had for our own workforce.

And really, in marketing that effort and convincing people that it was the right thing to do, it was very important for us to say, "Hey, we are not trying to be any different than anybody else from a pay perspective. We just want to be able to be on equal footing for the work that we do."

Mr. JOYCE. Aside from increasing pay, what other steps did you take to address the low morale and high attrition, particularly within the TSO workforce?

Mr. PEKOSKE. A number of things. You know, we put all kinds of leadership programs in place. They are starting to have an effect. We are trying to make sure that we have the right staffing at our checkpoints because if you can't take vacation time or you can't count on being done with your shift on time, that is a big dissatisfier for our people.

The other thing, sir, that is really important is pay is critical, and when you throw a bunch of incentives onto a person's compensation, those incentives don't count towards your retirement calculation. They don't count towards your Thrift Savings Plan and your 401(k) equivalent contributions with respect to agency or government matches.

So we just really felt we were significantly disadvantaging our workforce by not having the pay the same.

Mr. JOYCE. Thank you.

Excuse me. Mr. Cuellar.

Mr. CUELLAR. Thank you, Mr. Chairman.

And I understand this thing about the pay reform and we certainly—I know we might have some questions, but we want to

work with you to make it work somehow on that and address any concerns that some of the members have.

Let me talk to you about some of the trends impacting TSA, and that affects your budget and that affects the way you do it. And, again, I am looking at your strategic plan.

Continuous threat. You know, bad guys always trying to find a way. Emerging technology. How you can have interconnected technology that will enable a security model to work better. Passenger experience. People want to have the best experience, and it is always difficult. The changing workforce, which is tied into pay. You know, how do you recruit and retain talent with some of the skills that you need nowadays. And, of course, the transportation system and economy.

So, talk to us about how those trends are impacting your work and your budget?

Mr. PEKOSKE. Sir, I will start with the threat. I mean, the threat is changing. We didn't have anywhere near the cyber threat today that—or 5 years ago that we have today. So that is a significant change in the threat factor. We put a considerable amount of effort into cyber protections for transportation sector owners and operators. So that is a big threat change.

With respect to the foreign base, foreign-inspired threat, that still is very much a concern of ours. And, you know, what I think about all the time is on 9/11, it took 19 people to kill thousands of people in this country. And so even though ISIS and al-Qaeda might be smaller, they still exist, and they still want to attack the American system.

We also are concerned with the domestic terror threat, and we see manifestations of domestic violence in this country, in our aviation system in particular and our surface systems every single day at levels that we never saw before.

We look, too, at emerging threats. We have an incredible system of national laboratories in the United States that really look at, "Hey, what can an adversary develop that you just need to be aware of so you can start putting mitigations in place to be able to arrive with a prevention before the adversary is able to use it."

And then the incredible growth in transportation overall, particularly in aviation, I mean, you know, aviation, as we all know, and I said it in my opening statement, when you jump on a plane today, it is full, and all the flights are booked. There is an incredible demand for aviation. There has been a tremendous investment and there will be more with airport improvements, new terminals, new checkpoints. You see it at Reagan Airport, a brand new checkpoint here, for example, that many members travel out of. So there is just a lot of work in the transportation sector.

And the other thing that we are paying very close attention to is how do we strengthen our partnerships internationally? Because we have hundreds of flights that come in every single day from international locations, and one of the things that Congress gave us the authority to test is this concept called One-Stop Security, which means if you are coming from a trusted last point of departure airport internationally that we have an agreement with, that when you land in the United States, unless they have a follow-on

domestic flight somewhere else in the United States, you don't need to get rescreened in this country.

You know, the screening that you receive at your departure airport internationally is equivalent to U.S. standards. That has made inbound flights and will make, as we continue the prototyping of this, more secure inbound to the U.S.

So there is just a whole menu of things going on.

Mr. CUELLAR. Let me ask you, before my time is over, on the back end of the procurement, how we improve the procurement process. What happens to the technology? I know some years ago TSA had some technology, and they said we are not using it anymore. So I suggested, Well, maybe give it to some of the local jails that they can use. And they contacted the local jails, but there was an agreement where they had to pay. And the sheriffs were saying, well, we don't want to pay whatever the large amount is.

So TSA was keeping that technology, paying rent, paying on that contract, paying on the equipment they were not using.

So on the procurement part of it, I certainly want to ask you that you all look at working out better deals for the taxpayers' dollars. Because I remember that particular situation. I said, I have got a solution for the local jails that they can use that, and it didn't work out because they had to pick up this contract on that.

I even tried to work it with some other countries, you know, work with the State Department. They didn't want to pick up the cost.

So I would ask you to look at those.

Mr. PEKOSKE. Okay. Sure.

Mr. CUELLAR. Mr. Chairman, thank you so much.

Mr. PEKOSKE. Okay. Sure.

Mr. CUELLAR. Yeah. Mr. Chairman, thank you so much.

The CHAIRMAN. You are welcome, Mr. Cuellar.

Dr. Harris.

Mr. HARRIS. Thank you very much.

And thank you for being here in front of us. I have a few things I want to touch on.

One thing—and I am sorry, I apologize, I came from another hearing—there is a diversity inclusion chief at TSA. Now, I am kind of puzzled because I think minorities actually are overrepresented in the TSA.

So, first of all, how much is this costing in your budget? And what are they going to do? Are they going to hire different—I mean, you already have 55 percent, I understand, of the workforce minority. So what are you going—are you going to hire Asian-Pacific Islanders because they are underrepresented? Are you going to go out and hire more Caucasians because they are underrep—I don't understand. Why would you be spending security dollars on a diversity inclusion chief that doesn't seem to be necessary?

Mr. PEKOSKE. We would spend security dollars because it is better security, pure and simple. And we do have a Diversity, Equity, Inclusion, and Accessibility Officer that reports directly to me. That is how important I think this program is.

For me, you know, my goal is to make sure that all the different perspectives that we need to have to make good decisions in TSA are represented around the table, both at the front line in rede-

signing things that we do and in our policy decisions in our headquarters. So diversity of thought, diversity of perspective, diversity of culture. And really, you know, when I think of TSA, I can't think of another Federal agency that has more interaction with the public than TSA.

Mr. HARRIS. Sure. So are you going to hire more Asian-Pacific Islanders? Because when I go to the airport, I don't see them in the T—I mean, they are very rarely seen among the TSA staffing. Is that what this diversity inclusion chief is going to do?

Mr. PEKOSKE. What we are trying to do is to create the environment where we have wide range of choice on who we hire coming into TSA, that we have equal opportunity in who we can bring into the agency. And very, very importantly is that—you know, you mentioned that we have a very diverse workforce, and really that is at the front line of our workforce.

Mr. HARRIS. Sure. No, no. And good for you.

And so let me move on from that, because I guess—I don't know. Like I say, I can see where it is important that those—but at the front line it would appear to me that maybe you should be just hiring people who aren't there. Like I said, you are already overrepresented with minorities. That is all I can say. I get it. That is what this administration wants to do, but this administration, we are \$1 trillion in the hole. Your mission is to keep the skies safe.

Mr. PEKOSKE. Right.

Mr. HARRIS. And that is it.

Mr. PEKOSKE. And, you know, sir, that I served——

Mr. HARRIS. So I appreciate that.

Mr. PEKOSKE. I served in both administrations. I have the very same perspective.

Mr. HARRIS. Okay. Thank you very much.

Now, in terms of the budgets, you know, there is a \$1.1 billion increase in pay reform, but your budget depends upon us terminating the diversion of passenger security fees to the Treasury General Fund, and instead you assign them to TSA.

Now, if we don't statutorily do that, how do you fill that hole?

Mr. PEKOSKE. You appropriate the funds, so that is the hole that we are asking you to fill.

Mr. HARRIS. Us to fill?

Mr. PEKOSKE. Yes, clearly. And, really, let's think about this for a second.

Mr. HARRIS. Sure.

Mr. PEKOSKE. Passengers are paying money every single trip they make for aviation security. It is not going for that purpose. That seems wrong to me.

Mr. HARRIS. But you have taken that money and you have added it to your budget. I mean, it is not like you have said, Okay, give us, you know, \$1.56 billion less because we are going to divert these funds. You have just inflated the budget by that. Your budget counts on \$1.56 billion transferred. Is that right?

Mr. PEKOSKE. I disagree——

Mr. HARRIS. Okay. Thank you.

Mr. PEKOSKE [continuing]. With the characterization that we inflated the budget. The budget is what we need to operate the agency, and it is a bare-bones budget.

Mr. HARRIS. Sir, believe me, every hearing I am in, that is what everyone says: This is what we need. The President's budget is what we need.

We are \$1 trillion in deficit, so just pardon me if I am going to dissect whether you really need a thing like a diversity inclusion chief and things like that.

Finally, and hopefully on a high point, the Federal Flight Deck Officer and Crew Training Program—and I think it is an important program—what is the number of flight crew who have been trained in the program already?

Mr. PEKOSKE. We have about 7,200 Federal Flight Deck Officers. It is a really great program. I agree with you.

Mr. HARRIS. And they are—because it says flight crew. Now, I am assuming it is flight—it is basically flight deck. Is that where you are starting?

Mr. PEKOSKE. It is the FFDO Program, Federal Flight Deck Officer Program.

Mr. HARRIS. So when you say flight crew members, you mean in the cockpit?

Mr. PEKOSKE. Pilots and first officers.

Mr. HARRIS. And you have 7,200. So that is not a very high percentage, though, is it? Is it enough to be a deterrent?

Mr. PEKOSKE. No. We would like it to be higher.

Mr. HARRIS. Correct. And what is your goal? What percent of the flight crew do you—the flight deck officers do you think would be amenable to this kind of training?

Mr. PEKOSKE. Candidly, I would like to have as many as we possibly can. I mean, if we had 100 percent, that would be great, because we would know every single cockpit was secure.

Mr. HARRIS. Oh, look, I couldn't agree more.

And that 7,200, that is only a very small percent of the flight deck officers right now?

Mr. PEKOSKE. It is. These are all volunteers. There are about 2,000 people in the queue that—

Mr. HARRIS. Okay.

Mr. PEKOSKE [continuing]. Have raised their hand that want to join, and we are processing them.

Mr. HARRIS. And your increased funding request would train how many of that waiting list?

Mr. PEKOSKE. It would probably train about 500, so it is chipping away at it. It is not as fast as I would like. But, you know, I am really heartened by the fact that we have pilots and first officers that volunteer their time to do this program, so I want to bring them in as quickly as we can.

Mr. HARRIS. I am heartened by the fact too. I think it makes for a much safer airliner. Thank you very much.

I yield back.

Mr. CUELLAR. Chairman—

Mr. JOYCE. Mr. Cuellar.

Mr. CUELLAR [continuing]. I don't mean to interrupt, but I don't know if this is the right time to ask Mr. Harris what he meant twice by they are overrepresented by minorities. And I don't know if you want to do this privately or I can ask him now, but—



Mr. HARRIS. No. If the gentleman would yield, I would be more than happy. I mean——

Mr. CUELLAR. Yeah, I would be happy to.

Mr. HARRIS. The statistic I saw is that 55 percent of the workforce is minority, which actually, if you go through a TSA screening point, you——

Mr. CUELLAR. But you almost made—your tone made it sound like it was not good.

Mr. HARRIS. No. That is great. But, again, if the gentleman would yield, my question is, what is your diversity and minority officer going to do? I mean, we are spending administration dollars when minorities are already represented in the workforce.

Mr. CUELLAR. Uh-huh, uh-huh. Well——

Mr. HARRIS. That was my point.

Mr. CUELLAR. Yeah. Okay. Well——

Mr. HARRIS. In some workforces in the Federal Government, they are not. This one they are.

Mr. CUELLAR. This one they are.

Mr. HARRIS. Thank you. Thank you for yielding.

Mr. CUELLAR. But you did ask the same question of CISA this morning, so I assume you are going to be asking every agency—by the way, Border Patrol is 51 percent Hispanic, so I want to lay that out before we go any further.

But I don't want to disrupt, Mr. Chairman, but I just would like to keep a certain level of—work together with the members. And if we have any other particular questions, I will be happy to talk to you in private if we have to.

But sorry to interrupt, Mr. Chairman.

Mr. JOYCE. That would be a much better place for those discussions, Mr. Cuellar.

Mr. CUELLAR. I agree. I agree.

Mr. JOYCE. Thank you very much.

Mrs. Hinson.

Mrs. HINSON. Thank you for your patience with a second round of questions.

I just wanted to follow up actually on something that we talked about a little bit last year with the CT scanning technology, computed tomography technology. I think we can all agree it is essential. We talked about all the fentanyl that you are able to catch and things like that.

So I just wanted to flag, obviously your budget proposal cuts this account by 33 percent over last year. So what is your rationale for this reduction specifically? And what are you doing to accelerate the implementation of these systems?

Mr. PEKOSKE. Yes, ma'am. Thank you very much. The rationale is the top line. I just don't have the top line room to—as I said earlier, I have contract vehicles in place I know I want to buy. With more money, I would buy more, and I could install more so they wouldn't be put in storage. So we would put them into use right away.

My goal is to get this acquisition done as quickly as we can. The good news with the acquisition is that we have more and more competition in it as well. We have multiple vendors in each one of the sizes of CT technologies that we are buying in. We buy a base

size, a mid size, and a large size. So now we have robust competition within there, and we will see more competition over the coming years.

Mrs. HINSON. I certainly hope that drives prices down so you can buy more and get them in sooner.

I think a major concern that I have is, when you look at the time that it is taking to implement these systems, technologies advancing quickly, we are already talking about, with the machines that you have to put your hands over, the fixes that have happened there.

So, I guess, what are you doing to ensure that taxpayer-funded new technology is deployed in a timely manner? And are you concerned about it being outdated by the time we get all of this in place?

Mr. PEKOSKE. Yeah. One of our hedges against that being outdated is that open architecture piece that I mentioned, is that, hey, when we buy the technology, it produces data that is in a very standardized format so that we can rapidly change the software packages that have all the detection algorithms in them.

And, for example, if we have a new threat that manifests itself, rather than rewrite the entire package, we would just place a layer on the existing package. So that is a way to future proof.

Mrs. HINSON. Okay. Real quick followup on the digital driver's license. We are working on it in Iowa, I know that, and I can't wait to have it on my phone as a frequent flyer.

How many States currently are participating in that program? And what kind of enrollment have you seen?

Mr. PEKOSKE. Thank you. We have seen pretty good enrollment. We are still in the testing phase. We are still testing to make sure that it works as planned. So far, the tests have gone really well. Arizona, Maryland, Colorado, and now Utah are participating. And Utah has their own digital identity.

So, you know, we have allowed a lot of variation how States do this, all tagged to a standard. It kind of goes back to that open architecture piece is, here's the standard you need to achieve, and that means that you can go at it from a different perspective, but as long as you meet that security standard that is there.

Mrs. HINSON. Do you see any efficiencies in time getting passengers through using a digital ID?

Mr. PEKOSKE. Huge, huge. It takes——

Mrs. HINSON. Can you quantify that?

Mr. PEKOSKE. Well, every second counts in a checkpoint. So if you shave 2 seconds off, it counts. Because if you multiply that times, you know, 2.5 million people every day going through a checkpoint, that is a lot of time.

Mrs. HINSON. Absolutely. Thank you.

Mr. PEKOSKE. Thank you.

Mr. JOYCE. Thank you, Mrs. Hinson.

Recognizing Sheriff Rutherford for basically his first round here.

Mr. RUTHERFORD. Thank you, Mr. Chairman. I will try and be quick.

Thank you for being here this afternoon. Is there somewhere that I can go to get results from VIPR operations and BOD deployments?

Mr. PEKOSKE. Yes, sir. You have done it. We will get those to you.

Mr. RUTHERFORD. Okay. And can you tell me how many States we are running VIPR operations in?

Mr. PEKOSKE. So we have 31 VIPR teams for the entire country, and so we move them around as we need to. For example, when we have a national special security event, we move more VIPR teams to that event. But we also—you know, part of the reason that VIPR teams were put in place was to provide that visible presence of police and working very closely with State and local police in that effort.

Mr. RUTHERFORD. Okay. And so there are 31 teams. And how many individuals on each of those teams?

Mr. PEKOSKE. There are seven or eight people on each team.

Mr. RUTHERFORD. Okay. All right. And if you can get me that information on their results, what they have done.

Mr. PEKOSKE. Sure.

Mr. RUTHERFORD. How do you measure results on that operation?

Mr. PEKOSKE. We measure results in one way that I think is particularly powerful—and as a sheriff, you would appreciate this—is how many operations do we do jointly with our law enforcement partners? I mean, how much of a force multiplier, how much coordination occurs between the law enforcement agencies so we have the best coverage of a transportation hub that we possibly can.

We also look at the interactions that VIPR teams have had to ensure compliance with regulations or with law in different jurisdictions. And we have that data. We would be happy to share it with you.

Mr. RUTHERFORD. Okay. And are they still doing the BOD deployments also, the behavioral observation performance?

Mr. PEKOSKE. So we don't have a dedicated behavioral detection program any longer. That was ended by the Congress, actually, many years ago.

Mr. RUTHERFORD. Okay.

Mr. PEKOSKE. But what we do is we train every person on the front line with behavioral detection techniques. So we accomplish a similar thing, but it is across the entire workforce. I think it is actually more powerful that way.

Mr. RUTHERFORD. But there is no special deployments for that purpose any longer?

Mr. PEKOSKE. No, sir. Right.

Mr. RUTHERFORD. Okay. Thank you.

If you will just get me those numbers, I would greatly appreciate that.

Mr. PEKOSKE. Sure.

Mr. RUTHERFORD. And if we can do that fairly quickly, because we are trying to move through this process fast.

Mr. PEKOSKE. No. We will get them to you very soon. Thank you.

Mr. RUTHERFORD. Thank you very much.

I yield back, Mr. Chairman.

Mr. JOYCE. Thank you very much.

For those get-back questions of the members from the subcommittee today and any other ones that they may come up with,

we ask that you try to respond in 15 business days so that we have an opportunity to do this in a timely fashion. There may be additional questions—

Oh. Welcome. Let me back up.

Mr. Guest, I recognize you for your—I apologize for having put you right on the spot. I can't give you any breathing room because we were just about to close. So this will be technically your first round of questions, any questions you have.

Mr. GUEST. Thank you. And, Mr. Chairman, I apologize. I was just coming back from an Ethics Committee meeting, so I apologize for my tardiness.

Mr. JOYCE. The one that I missed that both you—

Mr. GUEST. That is right.

Mr. JOYCE [continuing]. And Mr. Rutherford were covering for me on.

Mr. GUEST. That is right.

Mr. JOYCE. Thank you very much.

Mr. GUEST. Yes, sir.

First of all, I want to thank you. I know you came by, visited with us earlier. I had a couple of questions on a couple of things.

First, I want to talk to you about REAL ID. I know REAL ID originally was implemented in 2017, I think July of 2017. REAL ID was implemented with the intended rollout to be 2020, giving roughly a 2.5 year period for individuals to comply with that. I know that REAL ID has since been moved—the implementation date has been moved. I think now it has been pushed back until sometime in 2025, if I am not mistaken.

Mr. PEKOSKE. Right.

Mr. GUEST. And so I guess my question and concern is—and I am assuming that REAL ID is a very important part of us being able to verify and screen those individuals who are getting on planes to make sure that they are using a State identification that you can rely upon.

Outside of COVID, why has it taken now or will take some 7-plus years to implement REAL ID?

Mr. PEKOSKE. So the Secretary just extended the deadline for REAL ID enforcement to the 7th of May 2025, as you mentioned. The reason he made that decision was because when you look at REAL ID compliance across the States—in other words, how many of the driver's license holders hold a REAL ID compliant driver's license—that number is about 53 percent. Operationally, we can't implement a program when just 53 percent of the license holders have the credential they need.

I agree with you 100 percent. I mean, it does create a much stronger credential. That is the reason for the effort.

Mr. GUEST. And so is this a State issue, the fact that States are not complying and issuing the driver's license quickly enough? I am just trying to see if there is a way that maybe, as Congress, that we can push back on some of the States to make sure they implement this quicker.

Again, I think it is an important screening method and important screening tool, but I do have some concerns at the continual delay in getting REAL ID implemented. And so is the delay on the State level? Is that what I understand?

Mr. PEKOSKE. The States issue the driver's licenses. And so, you know, we see great variability across the States in terms of the amount of compliance.

There is also, you know, a role that we play in terms of enabling individuals that are going to go get a REAL ID driver's license to electronically transmit some of the documents that are needed. That rulemaking is in process right now. So it is not all on the States, but the States have a significant responsibility here.

We do have a very good working relationship with what is called AAMVA, the American Association of Department of Motor Vehicle Administrators. They have been very cooperative with us. I think we all want to get to the same point, but continued emphasis on the part of Congress would be helpful.

Mr. GUEST. Okay. And then the other question I have is, at one time, there were some reports about illegal immigrants who were being able to fly without photo ID, I think actually using paperwork that DHS had issued those individuals.

I know that you testified before the Senate in July of last year, said that roughly—I think you said somewhere under a thousand illegal immigrants had been allowed to board planes using those warrants as identification.

One, is that process still in existence? Are immigrants able to use that as an identification? And then, two, do you have an approximate updated number? Again, it was under a thousand 9 months ago. Do you know what that number would be today?

Mr. PEKOSKE. Yes, sir. With respect to the civil arrest warrants, that document is not the identification document. What that document has is it has a file number. And what we do in all those cases when a passenger presents that civil arrest warrant is we take that file number and then call Customs and Border Protection and use the information we get from them to verify the identity of that individual.

Mr. GUEST. So do they present that paperwork and a photo ID at the same time?

Mr. PEKOSKE. Well, that paperwork, and then, you know, we can—Customs and Border Protection, if they have a photo of the person, can send it to us. We can look at it, or we can describe the individual and be more sure than not that this is the person.

To give you a number, so far in the month of March, nine people have presented that document as not an identification again but as a reference to a file that will allow us to further verify their identity.

The other thing, sir, just very quickly, is they all go through enhanced screening, any passenger that doesn't have the proper form of identification, whether it is somebody that is a migrant in the country or a U.S. citizen.

Mr. GUEST. And last question. I am running out of time. I know that there has been legislation introduced in the Senate that would ban these documents from being able to be used as travel documents.

Would you support the ban of those documents and require these individuals, just like everyone else, to present some sort of photograph ID, State-issued ID, again, driver's license, passport, something of that nature?

And I will let you answer. And then I yield back.

Mr. PEKOSKE. Yes, sir. I haven't seen the legislative text. I would like to see that legislative text to see what it requires.

From our perspective, you know, we want to be sure that the person that we are encountering is the person that we vetted, so that that person gets the right level of screening and is not a person that is on a no-fly list, for example. And so I would look at it from that regard is to make sure that our security protections are in place. We don't make decisions as to who is allowed to enter the country.

Mr. GUEST. Thank you.

Mr. PEKOSKE. Thank you.

Mr. GUEST. I am sorry. I yield back, Mr. Chairman.

Mr. JOYCE. No problem. I mean, you also missed a second round. If there is one burning question that you would like to get off, I mean, feel free.

Mr. GUEST. All right. One last question—and we talked about this in the office as well—is the rollout of the CT scanners, the importance of that to protect the traveling public. I know that, I think in our conversation, that there was going to be, under this budget, some delay in maybe those scanners being rolled out as quickly as they could be. I know that there is a limit in how quickly that those scanners can be installed in airports.

But can you talk about the importance of the CT scanners, what they do for your agents as being able to be able to better identify what they are seeing, move passengers through more quickly, and then the importance of us being able to outfit airports as quickly as possible with those scanners?

Mr. PEKOSKE. Yes, sir. Those scanners are critically important to allow us to detect the level of explosive weight that we need to detect to make sure that if an IED, an improvised explosive device, went off in an aircraft at altitude, that it would not be catastrophic for that flight. So there is a driving security concern to get the CT technology in place, and it is critical for our overall security.

Additionally, the CT X-ray allows the officer a much better view of what is in a carry-on bag. And so what that generally means is that things that normally we ask people to take out of their carry-on bags we don't need to with the CT technology, like liquids, aerosols, and gels, like laptops and iPads, and things of that nature.

So what that does is it is more convenient for the passenger. It is actually better for us because we can resolve any discrepancies that we see in the bag on the screen rather than having to do a bag search. So we are not going into somebody's property nearly as often as we were before.

To your point about speed, originally, this program—if we looked at last year's budget, you know, the fiscal 2023 budget, the budget that we are executing now, that project would be completed in 2036. So that is already a long time. With the reduced funding, which is basically reflective of our top line constraints, we don't have enough room in our budget to fit more of this in, it is now out to 2042. So that is a very long way into the future for a security vulnerability that we need to close as quickly as we can.

The last point, sir, is that we have contracts in place. We have robust competition amongst all sizes of this technology that we are buying. So we are ready to buy and we are ready to install.

Mr. GUEST. Thank you. That is all I have.

Mr. Chairman, I yield back.

Mr. JOYCE. As a former prosecutor, Mr. Guest, you will appreciate the fact that I opened my questioning with those questions, and I really wanted to give you the asked and answered, but that is okay.

Mr. GUEST. Great minds think alike.

Mr. JOYCE. And reminding you, for the members of the committee—or questions that the committee members will submit to you, 15 business days if you could respond to us, so we could.

Again, I would like to thank you for being here today, Administrator.

And, with that, this subcommittee is adjourned.





WEDNESDAY, MARCH 29, 2023.

**FISCAL YEAR 2024 REQUEST FOR THE DEPARTMENT OF  
HOMELAND SECURITY**

**WITNESS**

**HON. ALEJANDRO MAYORKAS, SECRETARY, DEPARTMENT OF HOMELAND SECURITY**

Mr. JOYCE. The Subcommittee on Homeland Security will come to order.

Welcome, Secretary Mayorkas. I sincerely thank you for joining us today as we discuss the Department's fiscal year 2024 budget submission.

First, I want to recognize DHS' 20-year anniversary. The Department was forged in the wake of the horrific attacks on September 11, 2001, and it was tasked with the critical mission of protecting our Nation against those who would do us harm.

On behalf of the committee, I would like to convey my sincere appreciation for the tireless, and often thankless, work done by the men and women of DHS on a day-to-day basis.

Turning our attention to the fiscal year 2024 budget request, this proposal is, unfortunately, more disappointing than it is promising. The budget is full of gimmicks that mask the true cost of protecting the homeland and make our job as appropriators that much more difficult.

The administration's fiscal year 2024 budget request for the Department is \$60.3 billion, which is nearly equal to the current fiscal year. However, after accounting for the \$1.6 billion in unauthorized TSA fees and the \$4.7 billion in emergency funds for border management activities, the real request is nearly \$6 billion above the fiscal year 2023.

Now is not the time for budget gimmicks. For over 2 years, we have seen skyrocketing illegal migration at the border. The policy-driven crisis continues for one reason and one reason alone: This administration is unwilling to publicly dissuade migrants from coming to the border and to back that up with the action and authority it already has on the books.

Bad policy drives bad outcomes, and the Biden administration's policies are undoubtedly driving our border security crisis. It is our job as appropriators to be good stewards of the taxpayer dollars, ensure we are not wasting money by supporting bad policies that don't result in desired outcomes.

Despite your public statements to the contrary, the border is not secure. If it was, we wouldn't have 2.7 million encounters, a record level, last fiscal year; we wouldn't have an estimated 600,000 illegal migrants who got away from agents and made it into our country; and we wouldn't have our law enforcement professionals stuck

administratively processing migrants when they should be patrolling the border.

On top of all this, the title 42 public health authority that the Department has relied on to turn back migrants at the border will likely expire on May 11. When that tool goes away, the border security operations will be profoundly impacted. As we consider resources, it seems clear that the combination of losing title 42 will easily cause a surge and overwhelm our dedicated officers and agents at the border.

The Biden administration has responded to the situation with a proposed rule entitled the "Circumvention of Lawful Pathways," which is being touted as an effective border security measure. However, this does not solve the problem at hand, and instead, it abuses the parole system by allowing tens of thousands of migrants with no permanent lawful path to citizenship into the country.

The administration's response also includes taking out crucial funding for addressing the border crisis out of its own base, and instead, funneling it into a slush fund that will have little impact on mitigating the border chaos.

The proposed emergency \$4.7 billion Southwest Border Contingency Fund will only ensure that we will spend more hard-earned tax dollars to achieve the same results and less oversight from Congress. Conditioning additional funds to worsening conditions incentivizes this administration to not solve problems and do their job in the first place.

Building more soft-sided facilities for processing and then releasing migrants into the interior hasn't worked. Decreasing detention capacity hasn't worked. Border security operators have been clear. Without consequences, the illegal flow will continue unabated. We cannot manage our way out of this crisis with a blank check for processing capacity and nongovernmental organizations. These actions will only facilitate lawlessness and encourage more migrants to make this dangerous journey north.

A lack of transparency in this budget proposal is frustrating. Today, I would like you to be more specific on funding and outcomes, what has worked, what hasn't, and how we can sufficiently resource the Department to carry out its important missions.

I look forward to working with you and the Department to seek solutions to address the border security crisis at hand and combat the many threats facing our Homeland.

I now turn to my distinguished colleague, Mr. Cuellar, for his opening remarks.

Mr. CUELLAR. Thank you, Mr. Chairman, Madam Chair, it is a pleasure, members of the committee.

Mr. Secretary, thank you so much for being here with us. I do have a prepared statement, but I am just going to summarize it, because I want to give you the opportunity to provide your statement on this.

But Homeland is very important to me. Like I always tell my friends, I don't go visit the border, I actually live there. My family lives there, and we work there and we live there, go to church and everything.

So the border is very important. And trying to find that balance between security, that is, providing security there at the border is

very important, but at the same time, allowing trade and tourism, which are so important to our area. You know, Laredo, the largest inland port, we get 17,000 traders a day.

So it is not only the men and women in green that are important, but also the men and women in blue. And so, not only hiring new officers are important, but now the support staff, the border processing coordinators are very important.

So one of the things that I want to focus on and I hope that we all focus on are what are the facts. For example, if we talk about drugs coming into the U.S., there are times where people will say, Oh, migrants are bringing in the drugs.

But when you look at the numbers from the Office of Field Operations at a port of entry, as of January of fiscal year 2023, 98 percent of the meth came through ports of entry; 97 percent of the fentanyl, port of entry; 87 percent of the cocaine, port of entry; 94 percent of the heroin, port of entry; 58 percent of the marijuana, ports of entry.

And yes, Border Patrol does catch what comes in. But I want to make sure that we put resources, that technology at the ports of entry, whether it is canine officers, support staff, working with our counterparts.

And one of the good things when we went with Senator Cornyn a delegation to Mexico, Mexico is now, for the first time, buying some of the same technology, same companies that we use at the ports of entry. So that way they can talk to each other, the technology can talk to each other. So that is very important.

Now, one of my concerns is procurement, how long it takes. We will put in the money, but it takes a long time to get the technology. So we have got to find a way to streamline the procurement process.

And on top of that, it is not only adding money for the technology, but the footprints of the bridges are very important. And a lot of times, we don't appropriate money to make sure that we can put the machines where they have to be. So that is one of the things that we have to focus on.

And talking about who brings in the drugs. According to the Sentencing Commission, the latest numbers we have, fiscal year 2021, 86.2 percent were U.S. citizens that are used by the criminal organizations.

So I just want to make sure that we put the focus and the monies where we need to look at, and look at, you know, not 14th-century solutions, but 21st-century solutions. We know the drones that the bad guys are using and we need to counter the drones that they are using, the tunnels and other ways.

But I am also concerned about what happens on May 11. You and I have had conversations. I am one of the ones that supports the new rule that will be coming out. I do support Title 42, but I do understand that it is coming to an end.

And I am one of those that I feel that Title 8, if we do expedited work process and deportations when the case calls actually works better than title 42, because title 42, you expel people, you don't deport people. There are no bars for somebody that is expelled under title 42. But title 8, you have 5 years, 10 years, 15 years,

20 years or lifetime bars, depending on the facts. So that is actually more I think provides teeth than title 42.

So we look forward to working with you on this new rule coming in, again, provide the law and order, the border security, but at the same time, respect the rights of the asylum folks.

Finally, to conclude, let me just say this: One of the things that Mexico, we spent 4½ hours with the President and his Cabinet. There are some ideas that I want to follow up. For example, the fentanyl, you know, what is the agreement, you know, what are we doing. They are basically saying, we will work with you on fentanyl, but stop the guns from going back over there. So those are things that I am hoping that we can explore.

And, with that, I say thank you so much to your men and women that work for you across the agency.

And, Mr. Chairman, thank you so much.

Mr. JOYCE. Thank you, Mr. Cuellar.

I would now like to recognize the chairwoman of the full committee, Ms. Granger, for her opening statement.

The CHAIRWOMAN. Thank you very much. Thank you, Chairman Joyce.

Thank you, Mr. Secretary, for being here. Since the last time you testified before us, the situation at the border has not improved. And living in Texas, I have been there many, many times.

Last year, a record 2.7 million migrants attempted to cross the border, 2.7 million. This year, they are telling me it is even worse. We have already had more than 1 million migrant encounters.

In May, title 42, you talked about, the Congressman talked about that. We want the thing that works best, and Title 8 will work better than that.

The cartels or the traffickers, they have no fear. They are not afraid of what we are going to do or where we are going to send them or fined. They are not doing that. They are coming across our border and drugs are coming across our border in huge numbers. Drugs are affecting all the communities, not just the Southwest, but all over.

You said you have operational control on the border. I would say this, I don't agree. The administration must reverse course on the situation, or it is going to get worse. We can't imagine it getting worse than it is now, worse than it is now. And now, some that have been able to go into the area can't even come close to it now because of the danger.

You have to have a strong voice in this. The border isn't open. And if you try to cross illegally, you will be quickly sent home. We have to be clear and we have to work together on this. It is not going to work any other way.

But when we are seeing what has happened, what has happened to our border, what has happened to our schools, what has happened to our freedom, it is just a tragedy. And I have done this many, many times over many, many years, and have friends that have on both sides of that border. And now no one goes there.

Mr. Secretary, the administration has to acknowledge what we all know, and that is the wall does work. And I have explained that to so many people. And it wasn't the wall, that we will have a wall that will stop it. It is what is inside that wall. It is inside the wall

so that we will know when people are trying to come across that. And so that technology was so important. I think it was a step—and as soon as it was built, I went down there and visited whatever. And now, it is just sitting there.

To close, I want to extend my appreciation to the men and women of the Department when they are trying to fix this. I will do everything in my power, everything in my power to be helpful, but we can't just live with what is here now. Thank you.

Mr. JOYCE. Thank you, Chairwoman Granger.

Secretary Mayorkas, without objection, your full testimony will be entered into the record. With that in mind, I would ask you to please summarize your opening statement in 5 minutes.

#### **OPENING STATEMENT OF SECRETARY MAYORKAS**

Secretary MAYORKAS. Thank you very much, Chairman Joyce, Ranking Member Cuellar, Chairwoman Granger.

On Sunday, I traveled to Rolling Fork, Mississippi, to assure the residents there and others in Mississippi devastated by the tornadoes that had just struck that the Department of Homeland Security will support their recovery in the days, weeks, and months ahead. More than 20 people lost their lives, and many more lost their homes and all that they possessed.

On Monday, I spoke with Senators Blackburn and Hagerty and with Governor Lee and Mayor Cooper and offered our Department's response to the too tragic and senseless murder of children and adults at St. Paul Christian School in Nashville, Tennessee. Our thoughts, prayers, and support are with all who are suffering today.

Over the past 20 years, the Department has evolved and responded capably to an increasingly dynamic threat landscape. We have done this through the unflinching dedication of the Department's 260,000 public servants, the third largest workforce in the Federal Government.

Every day these heroes work to: ensure the safety of Americans in the skies and on the seas, secure our borders; promote lawful trade and travel; provide relief when disaster strikes; advance the security of cyberspace and critical infrastructure; stop cartels from trafficking illegal drugs into our communities; combat human trafficking and online child sexual exploitation; protect our interests in the Arctic and the Indo-Pacific, and much more. The threats and challenges facing the homeland never have been more complex or dynamic.

The President's fiscal year 2024 budget for DHS was crafted to meet these threats and challenges strategically and responsibly, ensuring that our Department has the tools that it needs to keep our communities safe.

The displacement of people across the region is greater than at any time since World War II. I have visited the Southwest border approximately 16 times as Secretary, to meet with our personnel and to see firsthand the challenges that they face and the tools that they need to do their jobs.

The fiscal year 2024 budget proposes the hiring of more than 1,400 additional personnel to secure the Southwest border, including 350 additional U.S. Border Patrol agents and 310 additional

U.S. Border Patrol processing coordinators, to get more agents back into the field performing their critical law enforcement mission.

The budget proposes \$535 million in new funds for border technology, \$305 million of which is to deploy new technologies and capabilities in our fight against the trafficking of fentanyl through our ports of entry.

The threat environment that we face along the southwest border is dynamic, and the annual appropriations process does not provide the flexibility to address challenges that often change, from sector to sector, and from month to month.

We propose that Congress create a fund that can be spent for specific purposes when certain migrant encounter thresholds are met. This would equip our personnel with the tools that they need to meet migration surges if and as they occur, like transportation resources, soft-sided facilities for processing, and grants to support State and local community reception.

The budget also will enable the Department to process the increasing number of asylum cases, to address the backlog of applications for immigration benefits, to support the Citizenship and Integration Grant Program, and to improve refugee processing to meet the goal of admitting up to 125,000 refugees.

Our schools, hospitals, businesses, local governments and critical infrastructure are increasingly the targets of cyber attacks launched by transnational criminal organizations and hostile nation-states, including China, Russia, Iran, and North Korea. This budget invests in personnel, infrastructure, and enhanced tools and services to increase the cybersecurity preparedness and resilience of our networks and critical infrastructure.

We also must continue to build a culture of preparedness so that communities on the front lines of climate change and increasing extreme weather events are informed, ready, and resilient. This budget provides \$20.1 billion for FEMA to assist individuals and State, local, Tribal, and territorial partners affected by major disasters, and funds whole-of-community efforts to build climate resilience.

The U.S. Coast Guard provides critical capabilities and broad authorities to defend our national interests in the Western Hemisphere, the Arctic, and the Indo-Pacific. This budget makes strategic investments in the U.S. Coast Guard's fleet of Offshore Patrol Cutters and Polar Security Cutters that will advance our safety, security, and economic prosperity.

Finally, the men and women of DHS who serve our Nation are our most important and vital resource. We cannot expect to recruit and retain a world-class diverse workforce if they are not compensated fairly. We are asking for \$1.4 billion to honor the promise of pay fairness for our TSA workforce.

This budget will enable the Department to respond to the threats of today and to prepare for the threats of tomorrow. Thank you very much, and I look forward to answering your questions.

[The information follows:]

INSERT FOR THE RECORD



TESTIMONY OF

Alejandro N. Mayorkas  
Secretary  
U.S. Department of Homeland Security

BEFORE

Committee on Appropriations  
Subcommittee on Homeland Security  
United States House of Representatives

ON

"Fiscal Year 2024 Budget Request for the Department of Homeland  
Security"

March 29, 2023  
Washington, DC

## Introduction

Chairman Joyce, Ranking Member Cuellar, and distinguished Members of the Subcommittee:

I appreciate the opportunity to appear before you to discuss DHS's FY 2024 President's Budget.

This month marks the 20<sup>th</sup> anniversary of the Department's creation, which brought together 22 agencies and 180,000 public servants from across the Federal Government in a determined national effort to safeguard the United States against foreign terrorism in the wake of the devastation wrought on September 11, 2001. DHS remains the largest reorganization of the Federal Government's national security establishment since 1947 and a testament to the grave threat that we faced as a Nation from terrorism brought to our shores by foreign actors and foreign terrorist organizations.

Twenty years ago, Americans seeking a way to serve their country joined DHS to make meaningful contributions to the safety and security of the homeland. These first employees assembled chairs and desks in front of elevators, drew up initial plans and organization charts, and fought for a seat at the table. More than 32,000 of those early employees, whom we admirably refer to as "plank holders," still are serving proudly with the Department. Their service built the Department into the fit-for-mission organization that it is today.

Over the past 20 years, the Department has responded to an increasingly dynamic threat landscape with leadership, new programs and capabilities, cross-component collaboration, and unflinching dedication to mission. Today, we are the third largest department in the Federal Government with a 260,000-member workforce. Every day, our personnel interact with the U.S. public more than does any other federal agency as we: ensure the safety of Americans in the skies and on the seas, promote lawful trade and travel, ensure the protection of our critical infrastructure, provide relief when disaster strikes, advance the security of cyberspace, combat human trafficking and online child sexual exploitation, protect communities from illicit drugs and weapons, stand watch at our borders, defend the United States' interests in the Arctic and the Indo-Pacific, guard our federal buildings, and more.

Through all of our work, the Department is guided by 12 priorities that I established to ensure that we are ready to address the threats of today and to prepare for the threats of tomorrow. With these priorities in mind, I will share how we are confronting these threats and challenges, and how the President's Budget will ensure that the Department has the resources to do so effectively.

The FY 2024 President's Budget for the Department, totaling \$103.2 billion, will ensure that DHS has the resources to execute its mission to safeguard the American people and our homeland while also preserving our values. Of the \$103.2 billion requested, \$60.4 billion is discretionary funding, \$20.1 billion is for the Disaster Relief Fund (DRF) to support response, recovery, and resiliency during major disasters, and \$22.7 billion is mandatory funding and fee collections. In addition to the \$103.2 billion, this year the Department is proposing up to \$4.7



billion in emergency designated funding for a Southwest Border Contingency Fund to provide additional resources to DHS in the event that increased migration along the Southwest border exceeds pre-identified encounter thresholds.

Collectively, we may not have predicted today's diverse and complex threat environment when our Department first was created, but our mission never has been more vital, our agencies and officers never have collaborated more closely, and our Nation never has been more prepared. DHS was born out of tragedy and necessity. But in that necessity, we evolved and grew, and we attracted and retained the very best talent that America has to offer to solve its greatest challenges. This FY 2024 President's Budget will enable the Department to continue fulfilling its critical mission for the American people.

#### **Securing the Border and Building a Safe, Orderly, and Humane Immigration System**

Violence, food insecurity, severe poverty, corruption, climate change, the Coronavirus Disease 2019 (COVID-19) pandemic, and dire economic conditions all have contributed to a significant increase in irregular migration around the world. In our hemisphere alone, failing authoritarian regimes in Venezuela, Cuba, and Nicaragua, along with an ongoing humanitarian crisis in Haiti, have driven hundreds of thousands of people to migrate to the United States and other countries. These movements often are facilitated by numerous human smuggling organizations that exploit migrants as part of a billion-dollar criminal enterprise. The depth of suffering that these migrants are willing to endure speaks to the desperation that they feel about their prospects in their home countries.

Over the last several months, DHS has announced new processes for Cubans, Haitians, Nicaraguans, and Venezuelans and their immediate family members that combine an accessible, streamlined opportunity for eligible individuals to come to the United States via a lawful pathway, with consequences for those who do not avail themselves of this pathway and instead cross the Southwest border without authorization. Nationals of these countries who do not avail themselves of this process and who attempt to enter the United States without authorization generally will be returned to Mexico.

The coupling of these measures has led to a dramatic reduction in the numbers of Cubans, Nicaraguans, Haitians, and Venezuelans seeking to cross the Southwest border without authorization. Encounters of nationals from these four countries between POEs at the Southwest border declined from a 7-day average of 1,231 on the day that this policy was announced on January 5, 2023, to a 7-day average of 46 on February 28, 2023—a drop of 96 percent. This reduction represents a decline of 99 percent from the early December 2022 high of 3,546 daily encounters, and occurred even as encounters of other noncitizens began to rebound from their typical seasonal drop.

While encounters of Cubans, Haitians, Nicaraguans, and Venezuelans between POEs at the Southwest border have plummeted, thousands of nationals from these countries have followed the process successfully for lawful entry. As of March 1, more than 66,000 Cubans, Haitians, Nicaraguans, and Venezuelans, after being screened and vetted thoroughly, have received travel authorization. More than 45,000 individuals have arrived lawfully through commercial air travel at POEs to unite with supporters already in the United States, including

more than 9,500 Cubans, more than 8,000 Haitians, more than 2,700 Nicaraguans, and more than 25,000 Venezuelans. The successful use of these parole processes and the significant decrease in illegal crossing attempts clearly demonstrates that noncitizens prefer to utilize a safe, lawful, and orderly pathway to the United States if one is available, rather than putting their lives and livelihoods in the hands of ruthless smugglers. Combining accessible legal pathways with consequences for those who fail to use those pathways works.

*A Fair, Orderly, and Humane Immigration System*

The Biden-Harris Administration is committed to improving the Nation's immigration system and safeguarding its integrity by adjudicating requests for immigration benefits efficiently and fairly. The FY 2024 Budget includes \$865 million for U.S. Citizenship and Immigration Services (USCIS) to process increasing asylum caseloads, to address processing times for immigration benefit requests, to support the Citizenship and Integration Grant Program, and to improve refugee processing to support the Administration's goal of welcoming up to 125,000 refugees in FY 2024.

The Budget also includes \$165 million for the Department's Management Directorate to support the design and construction of a third permanent Joint Processing Center along the Southwest border. This facility, with dedicated operating space for multiple agencies and organizations, will make processing more efficient and will enable co-location operations, as appropriate. These projects will provide an integrated, whole-of-government solution for the processing of noncitizens encountered along the Southwest border.

*Enhancing Border Security*

DHS is leading the implementation of a whole-of-government effort to secure the Nation's borders and to enforce U.S. immigration laws. U.S. Customs and Border Protection (CBP) is responsible for securing the Nation's borders to protect the United States against terrorist threats, to combat and deter transnational crime, and to facilitate lawful travel, trade, and immigration. U.S. Immigration and Customs Enforcement (ICE) enforces more than 400 federal statutes and stands at the forefront of our Nation's efforts to strengthen border security and to prevent the illegal movement of people, goods, and funds into, within, and out of the United States. The FY 2024 Budget provides almost \$25 billion for CBP and ICE, demonstrating significant investments in personnel and technology. For example, the Budget funds an additional 350 U.S. Border Patrol agents, \$535 million for border security technology at and between POEs, and an additional 460 processing coordinators and assistants at CBP and ICE to ensure further that U.S. Border Patrol agents are in the field performing their critical law enforcement mission. The FY 2024 Budget also supports CBP's efforts to reduce reliance on Department of Defense (DOD) support along the Southwest border.

*Southwest Border Contingency Fund*

The annual appropriations process makes it difficult to adjust operationally to changes at the Southwest border throughout the year. In recent years, the Department has relied on supplemental funding and internal funding realignments to respond to fluctuating levels of migrant encounters that strain appropriated resources. The FY 2024 Budget includes a

Southwest Border Contingency Fund of up to \$4.7 billion, an emergency funding source to respond to migration surges along the Southwest border that only becomes available if migrant encounters reach predetermined thresholds. Each fiscal year, the fund will receive appropriations quarterly if the number of encounters exceeds the pre-identified thresholds. The contingency fund can be used only for certain border management costs incurred by CBP, ICE, and FEMA, to include requirements such as soft-sided facilities, transportation of migrants, medical support, surge staffing, immigration detention beds, Alternatives to Detention, and the Shelter and Services Grant Program. When the specified encounter rates have been met, the Department will notify this Committee of its intent to use the resources made available through this Fund.

The Contingency Fund will help to relieve pressure on CBP's U.S. Border Patrol stations, to facilitate ICE's enforcement of our immigration laws, and to provide humanitarian assistance. To avoid potential operational risks created by realigning funds from base budgets, CBP and ICE will use the Southwest Border Contingency Fund for emergent border management requirements associated with potential migrant surges. The Fund also will allow FEMA to provide critical humanitarian resources and relief to local governments and nonprofit organizations to help to manage better the costs of noncitizen arrivals in their communities.

#### **Investing in Cybersecurity and Infrastructure Security Protection**

The Department continuously evolves to counter emerging threats and to protect Americans in our modern world. DHS will implement the President's vision outlined in the National Cybersecurity Strategy, working with partners across sectors and around the globe to provide cybersecurity tools and resources, to protect critical infrastructure, to respond to and recover from cyber incidents, and to pave the way for a more secure future.

Our interconnectedness and the technology that enables it—the cyber ecosystem—expose us to a dynamic and evolving threat environment, one not contained by borders or limited to centralized actors, and one that affects governments, the private sector, civil society, and every citizen. As a result, cyber threats from foreign governments and transnational criminals remain among the most prominent threats facing our Nation. Hostile nations like Russia, China, Iran, and North Korea, as well as cybercriminals around the world, grow more sophisticated and create more adverse consequences. The Department continues to make significant strides to address these threats, including the work of the Cyber Safety Review Board, pursuing international partnerships such as expanding the Abraham Accords to defensive cybersecurity, promulgation of the cybersecurity performance goals, and creating more mature public-private partnerships to secure and defend civilian critical infrastructure, including those upon which the DOD may rely.

In March 2022, the President signed into law the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which requires the Cybersecurity and Infrastructure Agency (CISA) to develop and implement regulations requiring "covered entities" to report "covered cyber incidents" to CISA no later than 72 hours after the covered entities reasonably believe that a covered cyber incident occurred, and to report ransom payments within 24 hours after a

payment resulting from a ransom attack is made. The information derived from these reporting requirements will increase CISA's ability to deploy resources rapidly and to render assistance to victims suffering cyberattacks, to analyze incoming reporting to identify trends, and to share that information quickly with network defenders to warn other potential victims. The FY 2024 Budget includes \$98 million to help to ensure that CISA has the staffing, processes, and technology in place to implement and utilize successfully the information gained through CIRCIA.

The FY 2024 Budget is the first to request the transitioning of portions of the National Cybersecurity Protection System to a new Cyber Analytic and Data System (CADS). Over the past 2 years, Congress provided CISA with additional authorities and resources that in turn enabled unprecedented access to cybersecurity data across both federal and nonfederal systems. This data will allow CISA to decrease significantly the time required to identify potential intrusions or vulnerabilities and to take action to minimize potential harm, for example, by rapidly determining that threats identified across multiple agencies or companies are part of the same campaign or by assessing quickly the breadth of a compromise to contain impacts more effectively. This data will increase exponentially with the successful deployment of CIRCIA. Effectively leveraging this data requires new analytic capabilities and associated infrastructure, which CISA is implementing through CADS. CADS will provide a robust and scalable analytic environment capable of integrating mission visibility data sets and of providing visualization tools and advanced analytic capabilities to CISA's cyber operators, allowing more rapid analyses to inform more rapid actions, and, in turn, reducing the prevalence of intrusions and exploitable conditions across federal and critical infrastructure networks. This \$425 million request will allow CADS to expand the cyber mission systems engineering, mission information technology infrastructure, and cyber operation tools and services needed to enable CISA cyber operators to achieve their mission objectives fully.

### **Countering Fentanyl**

CBP and ICE work together to combat transnational criminal organizations (TCO) and to counter narcotics trafficking and other threats. For example, CBP's use of advanced analytics and targeting capabilities at the National Targeting Center allows CBP and partners to identify critical logistics, financial and communication nodes, and areas of weakness in illicit opioid trafficking networks. This information is shared with ICE's Homeland Security Investigations (HSI), which employs a suite of comprehensive criminal investigative techniques to combat drug trafficking into the United States, which primarily happens at POEs rather than between POEs. Investigative techniques deployed by HSI include physical surveillance and authorized electronic surveillance, defendant and witness interviews, the use of confidential informants and sources of information, and Special Agents embedded with host country law enforcement. HSI investigates land border narcotics seizures and contraband smuggling events as part of its strategy to disrupt and dismantle the capabilities of TCOs and to target sources of supply. Information resulting from these investigations is shared further with CBP to assist in locating and interdicting these smuggling attempts.

The shift in the illicit drug market toward synthetic opioids, primarily fentanyl and its analogs, led CBP to develop and implement the CBP Strategy to Combat Opioids. With the

support of Congress, CBP continues to make significant investments and improvements in drug detection and interdiction technology. CBP's extended border and foreign operations missions involve collaborating with U.S. and international partners to conduct joint maritime operations in the source, transit, and arrival zones of the Western Hemisphere. In collaboration with Joint Interagency Task Force South, CBP operates aircraft throughout North and Central America, conducting counternarcotics missions to detect and thereby facilitate the interdiction of bulk quantities of illicit narcotics by partner countries and agencies. CBP seized 11,200 pounds of fentanyl in FY 2021 and 14,700 pounds in FY 2022. This compares to 2,804 pounds seized in FY 2019.

Analysts continue to assess that the vast majority of fentanyl that enters the United States moves through U.S. POEs. At our POEs, CBP's nonintrusive inspection (NII) program deploys technologies to inspect and screen cars, trucks, rail cars, sea containers, and personal luggage, packages, parcels, and flat mail through either X-ray or gamma-ray imaging systems. CBP officers at our POEs use NII systems to help to detect drugs, unreported currency, guns, ammunition, and other illegal goods, as well as human smuggling attempts, while having a minimal impact on the flow of legitimate travel and commerce. CBP officers and agents currently utilize more than 370 large-scale systems and more than 3,500 small-scale NII systems to scan cargo and vehicles. In FY 2021, CBP executed FY 2019 funding to procure 123 additional large-scale NII systems to reach the current goal of 493 total systems. These additional units are expected to increase scanning to 40 percent of passenger vehicles and to 70 percent of cargo vehicles along the Southwest border land ports of entry. These increases will represent a 2,000-percent gain in scanning capacity and will enhance our enforcement and deterrence efforts dramatically. CBP will continue to utilize risk-based analysis to screen the remaining 60 percent of passenger vehicles and 30 percent of commercial vehicles through its existing layered enforcement strategy. The Budget request of more than \$305 million in FY 2024 will allow CBP to identify, procure, and deploy enhanced inspection capabilities to interdict emerging threats in the land and mail environments, specifically within civil works activities for drive-through NII deployments, enhanced narcotic detection with a primary focus on fentanyl detection, inspection technology at mail and express consignment facilities, chemical analysis to enable interdiction of opioids, and systems integration.

HSI is the principal investigative arm of DHS and plays a critical role in countering narcotics trafficking by exchanging information, by coordinating investigations, and by facilitating enforcement actions with law enforcement partners abroad to deter the ability of TCOs to smuggle drugs, people, and contraband into and out of the United States. HSI has matured into one of the premier criminal investigative agencies in the world. In FY 2022, HSI conducted 11,535 narcotics-related criminal arrests and seized roughly 1.87 million pounds of narcotics, which included 20,981 pounds of fentanyl. Additionally, HSI agents seized more than \$210 million in total currency and assets through their narcotics enforcement efforts.

The FY 2024 President's Budget includes \$40 million to support the Monroe Project operations along the Southwest border to combat illicit drug operations. The Monroe Project is a recent DHS-wide effort aimed at targeting criminal organizations responsible for distributing illicit fentanyl that killed more than 77,000 Americans last year. A key component of the Monroe Project is the consolidation of information to enable better data-driven decision-making.

This funding also supports capacity enhancement for HSI Mexico and its Transnational Criminal Investigative Unit, which is a critical component in the DHS strategy to disrupt and dismantle TCOs specializing in the production and distribution of fentanyl.

#### **Combating Human Trafficking and Preventing Child Sexual Exploitation**

Combating the abhorrent crimes of human trafficking and child sexual exploitation and abuse (CSEA) is a top priority for the Department. These crimes target the most vulnerable among us, offend our most basic values, and threaten our national security and public safety.

Almost every office and agency in the Department plays a role in our counter-human trafficking mission. The DHS Center for Countering Human Trafficking (CCHT) coordinates the counter-trafficking efforts of 16 offices and component agencies, reflecting our commitment to combat this heinous crime from every angle: investigations and enforcement, intelligence, public education and prevention, policy innovation, victim protection and support, and more. HSI leads criminal investigations into sex trafficking and forced labor, making 3,655 human trafficking-related arrests during FY 2022, an increase of more than 50 percent from the previous fiscal year. Our human trafficking investigations led to 638 convictions, an increase of more than 80 percent from the previous year.

The FY 2024 Budget includes \$24 million for HSI Child Exploitation Investigations Unit (CEIU), an increase of \$17 million, to enhance HSI's capability to investigate international and domestic child exploitation. CEIU will utilize these resources to develop additional specialized sections within CEIU to focus on new and emerging threats, as well as on the development of an online undercover program to ensure that HSI is utilizing all tools available to combat CSEA around the globe. CEIU employs the latest technology to collect evidence and to track the activities of individuals and organized groups who sexually exploit children using the open internet, DarkNet, chat rooms, peer-to-peer trading, and other app-based platforms. The Budget also includes \$22 million for HSI's CCHT, a \$2 million increase. These additional resources will increase the number of investigators working to combat child exploitation and human trafficking.

#### **Modernizing Coast Guard Operational Capability and Presence in the Arctic Region**

As a maritime nation, the United States depends on a strong and agile U.S. Coast Guard to enhance the Nation's maritime safety, security, and economic prosperity. For 232 years, the U.S. Coast Guard has applied its broad authorities and capabilities to save lives, to protect our waters, and to defend our national interests. As challenges to our national security and global influence grow more complex, the need for a more adaptive and connected Coast Guard never has been greater. By confronting threats to the homeland wherever they emerge—from the Arctic to the Indo-Pacific—the U.S. Coast Guard secures our borders, saves lives, counters malign state behavior, prevents terrorism, and reduces physical and cybersecurity risks.

The FY 2024 Budget provides \$12.1 billion in net discretionary funding to sustain readiness, resilience, and capability while building the U.S. Coast Guard of the future to ensure that the U.S. Coast Guard has the assets, systems, infrastructure, and support needed to enhance

the Nation's interests in an increasingly complex and connected world. The Budget continues efforts for the U.S. Coast Guard's two highest acquisition priorities, the Offshore Patrol Cutter and the Polar Security Cutter, and advances the Great Lakes Icebreaker acquisition, an asset ensuring America's continued economic prosperity on our domestic waterways.

As climate change and strategic competition increasingly affect the geography, stability, and security of the Arctic region, U.S. Coast Guard presence and leadership never have been more critical. The FY 2024 President's Budget also requests \$150 million to support the acquisition of a commercially available polar icebreaker, including initial modifications, crewing, and integrated logistics support required to reach initial operating capability. The United States has vital national interests in the polar regions and the purchase of a commercially available polar icebreaker is a viable strategy to accelerate U.S. presence in the polar regions in the near-term.

#### **Modernizing TSA Pay and Workforce Policies**

TSA is an intelligence-driven national security organization that combines the skills of its workforce, evolving security procedures, and technology to optimize resource utilization and mission effectiveness. The Nation's economy depends on the implementation of transportation security measures that provide effective security against threats and that ensure an efficient flow of people and commerce. TSA is committed to the highest level of security for the United States across all modes of transportation. Investment in enhanced security capabilities and technology will strengthen TSA's ability to employ risk-based security measures to combat evolving threats actively to critical transportation infrastructure.

The FY 2024 Budget continues the FY 2023 initiative to increase TSA pay levels, making TSA pay comparable to private-sector and Federal Government employees in similar positions, which will assist greatly in recruitment and retention efforts. The TSA workforce deserves to be compensated fairly at rates comparable with their peers in the federal workforce. The Budget includes \$1.1 billion to ensure that TSA employees are paid at a level that is no less than that of their counterparts on the General Schedule pay scale. An additional \$53 million covers the costs of pay systems conversion and establishes a labor relations support capability to manage expanded labor benefits and the right to appeal adverse personnel actions to the Merit Systems Protection Board. Enhancements to TSA pay supports the President's and my commitment to fostering diversity, equity, and inclusion in the federal workforce.

The Federal Government repeatedly has leveraged TSA's unique authorities—including the ability to issue Security Directives and Emergency Amendments within hours of receiving information about a threat—to address cyber threats. This threat has grown dramatically in the past decade and that growth shows no sign of slowing. Accordingly, the FY 2024 Budget includes an increase of \$10 million to conduct critical mission support functions to reduce the cyber threat to American critical infrastructure in both the near- and mid-terms, and in support of both surface and aviation sectors.

### **Supporting 2024 Presidential Campaign Security**

The U.S. Secret Service (USSS) carries out the unique and integrated missions of protecting senior leadership and investigating threats to the Nation's financial system. Best known for protecting the President, the Vice President, their immediate families, visiting heads of state, and other designated individuals, the USSS also protects the White House Complex, the Vice President's residence, foreign diplomatic missions, and other designated buildings. Further, it coordinates security at designated National Special Security Events, such as the State of the Union Address and the United Nations General Assembly, and protects our financial infrastructure by investigating counterfeiting, identity theft, computer fraud, and other crimes related to the financial security of the United States. Every 4 years, the USSS also must plan for the increased requirement related to the Presidential Campaign. The FY 2024 Budget includes \$191 million to ensure that the 2024 Presidential Campaign is resourced adequately for the protection of major candidates, nominees, their spouses, and nominating conventions. The funding supports the enhanced protection, security, travel, and overtime for the 2024 Presidential Campaign and includes resources to train USSS personnel and other federal partner agencies. The President's Budget also continues to invest in USSS staffing, funding an additional 77 positions and bringing the total strength to 8,382, the highest in USSS history.

### **Investing in Climate and Natural Disaster Resilience**

FEMA strengthens the Nation's ability to prepare for and respond to disasters of all types and magnitudes via partnerships with SLTT governments, in part through its grant programs. The Budget includes increased funding for programs and activities that support FEMA's goals to lead whole-of-community efforts in climate resilience and to promote and sustain a ready FEMA and prepared Nation. As part of the Administration's efforts to address climate change, the FY 2024 Budget provides \$4.0 billion for DHS's climate resilience programs, a more than \$150 million increase from the FY 2023 enacted. This is in addition to \$1 billion provided by the Bipartisan Infrastructure Law for FY 2024. The Budget helps SLTT partners to build climate resilience through various FEMA grant programs. The Budget also includes more than \$500 million for flood hazard mapping, including the development of new data to support future flood conditions and their impacts.

The FY 2024 Budget provides a major disaster allocation totaling \$20.1 billion for FEMA to assist SLTT partners and individuals affected by major disasters, and provides a total of \$3.2 billion to promote and sustain a prepared Nation through FEMA grants to improve the Nation's disaster resilience and to implement preparedness strategies. This includes increasing the Nonprofit Security Grant Program by \$55 million to a total of \$360 million for target hardening and other physical security enhancements and activities by nonprofit organizations that are at a high risk of terrorist attack. This also includes \$50 million to establish a critical infrastructure cybersecurity grant program to support risk reduction strategies to protect critical infrastructure from cyberattacks. The Budget also provides \$145 million to support DRF base requirements associated with emergency declarations, pre-declaration surge activities, Fire Management Assistance Grants, and disaster readiness and support activities.



*Sustainability and Conservation*

The Administration remains committed to establishing the Federal Government as a leader in sustainability. The Budget includes \$123 million for DHS, as the third largest department in the Federal Government and the Nation's largest law enforcement agency, to support integrated market-shaping investments into zero-emission vehicles and charging infrastructure. The Budget also demonstrates the Administration's continued support for the strategic investment in the National Capital Region (NCR) for Headquarters and facility requirements at St. Elizabeths. The Budget includes \$264 million for the Department to consolidate its physical footprint across the NCR. In FY 2024, funding will be used for the construction of new facilities, including the Office of Intelligence and Analysis, at the St. Elizabeths West Campus, consolidation of the remaining Management Directorate and FEMA Headquarters from dispersed locations to a consolidated space, and the continuation of utilization improvements at the Ronald Reagan Federal Office Building for CBP.

**Conclusion**

As DHS enters its third decade, the Department will continue to evolve and to rise to the challenges posed by an ever-changing threat landscape. It is a great privilege to represent and serve alongside the DHS workforce, which has time and again demonstrated exceptional skill and an unwavering commitment to keeping our country safe.

The FY 2024 President's Budget includes the necessary funding and authorities for DHS to carry out its wide-ranging mission. I am grateful to this Committee for your continued support and the opportunity to appear before you today. I look forward to working together and to answering your questions.

## BORDER WALL: CONSTRUCTION

Mr. JOYCE. Thank you, Secretary.

I now recognize myself for questions.

Congress provided more than \$5.8 billion in appropriated funding for the border wall, and during the last administration many miles of new and replacement barriers were built. The Chief of the Border Patrol recently told this subcommittee that walls work.

However, this President not only refuses to build additional barriers, but his administration, and specifically your Department, is taking every possible action not to expend the funds Congress explicitly provided for wall construction. There is rusting wall sitting in the dirt in the El Paso sector that taxpayers have paid for that you refuse to put up, and there is no rational reason for that.

So I ask you, do you agree with Chief Ortiz that walls work, and do you believe that additional barriers are necessary to secure the border? And if so, why aren't you building more?

Secretary MAYORKAS. Mr. Chairman, I have approved, I believe it is approximately 129, wall projects to close gaps in the existing wall, to bring technology to the gates to complete those projects.

What we are seeking to invest in is our personnel, our greatest resource, as well as in technology that is an extraordinary force multiplier to help to secure the border.

We believe that technology, and really harnessing the advances of innovation, is the most effective way to secure the border and to add to the tremendous resource and talent that our personnel deliver.

Mr. JOYCE. Thank you. How much money did it cost the Department to cancel the contracts midstream when taking into account the additional work that needs to be done, such as stabilizing roads, drainage, and other mitigation efforts?

Secretary MAYORKAS. Mr. Chairman, if there was a cost in the cancellation of contracts, I certainly would be pleased to provide that to you. I don't have that number at my fingertips.

Mr. JOYCE. Thank you. Fifteen business days after today, I would love to have that.

Secretary MAYORKAS. Most certainly, Mr. Chairman.

## FY 2024 BUDGET: TSA PAY

Mr. JOYCE. While the disaster at our borders is top of my mind for many of us here today, we cannot lose sight of the budget request as a whole. It is over \$60 billion across the Department. I am very concerned with the request of funds being for border management and not for border security. I look forward to having my colleagues dive into this more.

What I am disappointed in seeing in this budget request is a lack of prioritization for another frontline workforce, those working the front line at TSA, including the Transportation Security Officers. For far too long, TSOs' pay lagged behind similarly situated counterparts across the government.

Before someone makes the argument that this is why TSA needs to be moved under title 5, nothing has stopped the Department from prioritizing these workers to get them a pay raise now. Instead, what has been submitted is a budget request to fund an in-

crease for the entire TSA workforce, including those at headquarters.

I would like to see pay increases just for the front line as well as increases in tech investment. Deploying more advanced technology to airports would greatly enhance security. Giving high-paid headquarters execs a raise will not.

Sometimes I think we forget the Federal Government does not have unlimited resources, and we need to be precise and thoughtful on where we spend these limited funds. I tend to think investing in the frontline workers is money well spent.

Secretary Mayorkas, could you explain why this request does not prioritize funding pay raises for only the frontline workforce at TSA who most desperately need it?

Secretary MAYORKAS. Mr. Chairman, I very much appreciate your question. First and foremost, we are prioritizing the much-needed and long overdue pay increases for our Transportation Security Officers at the airports all over the country. They are our front lines, and I am incredibly proud to support them. We also do believe that pay increases for other personnel are warranted.

To address a concern that you articulated, we are, in fact, in this fiscal year 2024 budget, investing in our technology and other innovations. We are harnessing those innovations, including exploring how we can use artificial intelligence to be a force multiplier for our brave and heroic personnel.

We are, indeed, addressing the prioritization that you communicate. We are investing in technology, as you indicate is necessary. We also are providing for pay increases for other personnel who so richly deserve it. They are, in headquarters, but we cannot support the achievements of one without recognizing and rewarding the contributions of all. This is a team effort, and all 260,000 people at DHS contribute to the Homeland Security mission.

#### CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Mr. JOYCE. I want to hit on one other priority, and that is CISA. Over the past few years, CISA's budget has been doubled. They have gained several new authorities. And I look forward to seeing how CISA incorporates industry feedback in finalizing the rule-making for CIRCIA. It was great to have Director Easterly here just yesterday to testify but, Secretary Mayorkas, as the Cabinet-level official overseeing CISA, could you explain where the significant resources CISA has been given are going and how your opinion if CISA is making good use of taxpayer funds?

Secretary MAYORKAS. Mr. Chairman, the threat of cybersecurity is not diminishing. We are seeing cybercriminals only enhance their efforts, predominantly in the world of ransomware, but also in other cyber attacks against our critical infrastructure: schools, hospitals, local law enforcement offices, and so much more.

We also see adverse nation-states—China, North Korea, Iran, Russia—engage in cyber attacks against our country. CISA is on the front line. Its incredibly talented and dedicated personnel work every day to enhance the cybersecurity of our country and to ensure the cybersecurity of our critical infrastructure, the majority of which rests in the hands of the private sector.

We are investing in people. We are investing in technology. We are investing in grant funds to ensure that communities enhance their respective cybersecurity. There are many target-rich and resource-poor elements of this country that have to enhance their cybersecurity. We are doing so much in that regard.

Mr. JOYCE. Thank you. I have exceeded my time limit.

I now recognize my distinguished ranking member, Mr. Cuellar, for any questions.

#### FENTANYL: PROCUREMENT OF TECHNOLOGY

Mr. CUELLAR. Thank you, Mr. Joyce, Mr. Chairman.

Let me concentrate on fentanyl. When you look at the precursors that come in from China to Mexico, you will see that they usually go to two ports, go through the Pacific, end up in Manzanillo and Lazaro Cardenas. And then, of course, then the drug organizations will send them off to different locations in Mexico, store them, change them into fentanyl. And then from there, they will go—and if you look at what makes sense, what is closest, they will go through the areas of California, San Diego, and Arizona, a percentage. And there is a percentage, but—

So if we know that most drugs are coming in through ports of entry, one of the things that concerns me is the major acquisition programs, how long it takes. It moves too slowly. It avoids competition. It avoids opportunities for innovation.

And one of the things that we want to work with you is how do we speed up that acquisition while we still protect taxpayers' dollars? If we know what the problem is and how they are going in, I would ask you to work with us on that part, and then what you all are doing with the Mexican Government, because for the first time the President said, he said, I will officially ask China to stop sending precursors to Mexico.

And then after that, I also read that you all are working with him on—I don't know which Department, working on an agreement. And what they want is, we will help you with precursors, but we want you to stop sending guns, because Texas is the number one source of guns for them.

So I want to see what are we doing to address the issue on procurement to get the technology. And keep in mind, Mr. Secretary, for the first time they are buying—they bought almost \$800 million, and it is the same technology that U.S. Customs is using over here. So that is encouraging for us. So if you can address those issues.

Secretary MAYORKAS. Thank you very much, Ranking Member Cuellar. We are taking a multi-pronged approach to our attack against the cartels that traffic in fentanyl.

I must say, as Congressman Guest knows, we share a past as prosecutors. I served for 12 years as a Federal prosecutor. I have prosecuted cocaine trafficking cases, methamphetamine trafficking cases, and black tar heroin trafficking cases, and we have seen nothing like the toxicity of fentanyl that is killing so many Americans. This is a problem that has been around for too many years. We are taking it to the cartels in unprecedented ways, and we are working with the Government of Mexico in that regard.

I have visited with our Mexican counterparts as well. We are assisting them in securing their ports, because indeed, many of the precursor chemicals and the equipment used to manufacture fentanyl is coming from China, reaching the Mexican ports, and the traffickers, the cartels try to bring it through the ports of entry.

Mr. CUELLAR. And if I can interrupt, and members, if we look at the Chinese investment that we have in Mexico, and we got to be aware that is a different issue, but especially they are very smart. They will do it in the port. So they are there at the ports. They get the legal and the illegal drugs—I mean, products going through there. Sorry.

Secretary MAYORKAS. We are very focused on that element as well.

So with respect to your question about procurement, we have a procurement innovation lab to address precisely the concern that you articulate, which is to be able to harness technology, to harness innovation quickly. We need to be able to move quickly. The procurement process is far too slow.

With respect to the POES, we are surging our personnel to the POES to increase our interdiction and investigative capabilities. The remarkable special agents of Homeland Security Investigations already have begun that effort. I announced Operation Blue Lotus last week, and in its first week of operation, it already is making a significant difference.

Mr. CUELLAR. And that technology, Mr. Secretary, is very important, because if you want to bring marijuana, you can see big old piles. And I have seen some of the technology you have in Laredo and other places. But now you are talking about pills, and it is smaller, and if you don't have the trained officers you won't see those—you can't see them unless if you have the trained eyes. So it takes personnel, it takes canines, and it takes the latest technology and the Mexicans doing that.

So, Mr. Secretary, thank you so much.

Mr. JOYCE. Thank you, Mr. Cuellar.

I now recognize Chairwoman Granger for any questions she may have.

#### BORDER WALL: EXPIRATION OF FUNDS

The CHAIRWOMAN. Mr. Secretary, right now I would say that protecting our border has been a complete failure. And I have been there many times, and it is tragic. It is a tragedy.

Right now, Customs and Border has \$2.8 billion remaining for the funds to complete the wall, \$2.8 billion. A little more than \$200 million of it will expire in the next few months. Are we just going to let that happen? All I hear is words. And see that border, it is a crime. It is terrible what has happened there. So what is going to be real about this?

Secretary MAYORKAS. Madam Chairwoman, as I mentioned to Chairman Joyce, I have approved, I think it is approximately 129 projects, to close gaps and to complete the gates in the border wall. We believe that investing in personnel, investing in technology is the best way to secure the border.

We are focused intensely on securing the southwest border, securing all of the borders of the United States. We are working day

in and day out. I must commend the heroic work of the U.S. Border Patrol agents as well as the Office of Field Operations officers of Customs and Border Protection and the support from throughout our Department. I do not understate the seriousness of the challenge that we face.

The CHAIRWOMAN. What is going to happen to the \$200 million that is going to expire? Are you going to let it expire?

Secretary MAYORKAS. If I may, Madam Chairwoman, the challenge that we face at our southern border, is not exclusive to the United States. We are seeing an increase in migration around and across the entire hemisphere. Let me give, if I may, one example. Venezuela is a country with a population of approximately 28 million people.

The CHAIRWOMAN. My questions were on our southern Texas border.

Secretary MAYORKAS. Yes, but this speaks to the issue. It speaks to the seriousness of the challenge that is gripping the entire hemisphere.

Of those 28 million people, approximately 8 million have fled Venezuela, because of the authoritarian repressive regime there. 2.5 million of those individuals are in Colombia. Hundreds of thousands are moving to Chile.

What we have done, and what we announced on January 5, to address the challenge at the border is we announced an innovative program that provides safe, orderly, and lawful pathways to come to the United States for Cubans, Haitians, Nicaraguans and Venezuelans, and delivers a consequence to individuals from those countries if they don't take advantage of those pathways, and instead come to our southern border.

We have seen a 95 percent, approximately 95 percent—

The CHAIRWOMAN. Sir, that is not the question I asked. That is not the question I have. And I have asked this question over and over and over. We know what is happening, what is happening to our southern border? Texas changed dramatically. Other countries have come there.

But it is pretty simple, and I said there is \$2 million that is going to expire having to do with the wall in a few months. That is a pretty straightforward question. What is going to happen to it? It is going to go away?

Secretary MAYORKAS. As I mentioned, Chairwoman Granger, I have, indeed, approved a number of projects. We will comply with our legal obligations with respect to the funds provided for the wall.

The CHAIRWOMAN. I pass.

Mr. JOYCE. Thank you, Chairwoman Granger.

I believe in a request, though, you said that you had 129 projects that you are going to expend the \$200 million on. We would like a copy of how that is going within 15 business days as well.

At this time, I recognize Mr. Newhouse.

#### MIGRANT ENCOUNTERS: REMOVALS

Mr. NEWHOUSE. Thank you, Mr. Chairman.

Secretary Mayorkas, thank you for being here today.

Secretary MAYORKAS. Good morning.

Mr. NEWHOUSE. We all appreciate the huge challenge at our country's borders.

A couple of questions: Last year, the administration removed—the numbers I have in front of me—72,177 migrants under the Title 8 authority. That does not include the Title 42 expulsions. This past December, over 250,000 people were encountered by the CBP. Well over half of those encountered were single adults. You know all these things.

So in 1 year, the administration removed less than a third of the number of encounters that we see in a single month. And the back-drop of that is in 1 year, 2.76 million people were encountered by the CBP.

So my questions have to do with some of those numbers. I am curious. Of those 72,177 individuals, can you tell me were those people that were arrested in fiscal year 2022 or were they prior arrestees that were being deported? Give me an idea of how quickly people are being removed.

Secretary MAYORKAS. Congressman, you ask a very important question. Title 42 is a public health authority. Title 8 is our immigration enforcement authority. We sought to expand our use of Title 8, because it delivers a consequence, as Ranking Member Cuellar noted, and we were enjoined from doing so.

Last year, we removed and expelled approximately 1.4 million people, the most ever. That is because we were under compulsion to use the Title 42 authority, which allows us to expel people very quickly, and we were prevented from using our Title 8 authority, as we had sought to do so. It is very important to note that 1.4 million people either were expelled or removed from the United States last year.

Mr. NEWHOUSE. So Title 42 is going away. Title 8 you are telling me then will be utilized to a fuller extent moving forward, and so we should see a greater number.

My question has to do with those people that I referred to under the Title 8 removals. Were they arrested in this past year, or how long are people here before they are removed?

Secretary MAYORKAS. I see. Congressman Newhouse, you identify a significant infirmity with our immigration system, strong evidence of why it is so fundamentally broken, and everyone agrees on that.

It historically has taken 4- to 6-plus years in between the time that an individual is encountered at our southern border, and the time that their immigration case is adjudicated with finality for removal.

That is not specific to this Administration, nor the prior administration, nor the administration before that. I learned that when I first entered DHS in August of 2009.

#### ICE: DETENTION BEDS

Mr. NEWHOUSE. So if we could also request that information related to those Title 8 individuals and how long they have been in the country, I would appreciate that.

Throughout your administration, thousands of available ICE detention beds have sat empty. So a simple question: Apart from the

mandate with no discretion that the law provides, do you believe detention is an important part of overall border security?

Secretary MAYORKAS. Yes, I do, Congressman. We seek to prioritize individuals who present a public safety threat or a national security threat.

If I may explain why all the detention beds have not been used. There has been litigation throughout the country with respect to the capacity that we are allowed to fill our detention space.

That has been especially acute in a time of COVID-19, when we have court orders requiring that we not fill a particular facility to its maximum capacity in light of social distancing and the like.

There is a patchwork of litigation across the country that inhibits our ability to use our maximum bed space.

Mr. NEWHOUSE. Well, I do have some further things I would like to learn about, but my time is expired.

Mr. Chairman, thank you for indulging me, and I will yield back.

Mr. JOYCE. It certainly has, Mr. Newhouse.

I apologize, Ms. Underwood. In the spirit of going back and forth, I got ahead of myself. Please.

#### MIGRANT ENCOUNTERS: FAMILY DETENTION

Ms. UNDERWOOD. Thank you, Mr. Chairman.

Mr. Secretary, nice to see you, sir. Thanks for being here with us today. Congress has charged the Department of Homeland Security with an incredibly broad mission, countering terrorism and domestic violent extremism, responding to mass shootings like the tragedy this week in Nashville, protecting our infrastructure at institutions from cyber attacks, leading disaster response and climate resiliency, overseeing our borders with a broken immigration system at a time of historic migration and much more.

And by failing to pass broad immigration reform, like the U.S. Citizenship Act, Congress has not given the Department all the tools it needs to address these challenges.

But leading a Federal agency means being clear-eyed about the political environment and making determined, data-driven choices that uphold our country's values anyway.

So I was horrified to learn that the Biden administration is considering reinstating family detention of migrants. It is not just immoral. It is expensive. It is a bad policy that makes our country less safe. I am a nurse, and I have reviewed the literature myself. The data are clear. Family separation causes long-term damage to kids' mental and physical health, and their parents too. Family detention shouldn't even be an option on the table right now, given the mountain of evidence against it, but reportedly it is.

And so I would like to hear from you what specific data the administration is using that would suggest any justification for going backwards like this?

Secretary MAYORKAS. Congresswoman, you mentioned two things: family separation and family detention. With respect to family separation, the heinous policy of the prior administration, President Biden created the Family Reunification Task Force.

Ms. UNDERWOOD. Right. I am asking about family detention. Family detention, what evidence do you have to reinstate this policy?



Secretary MAYORKAS. No decision has been made, Congresswoman. I try to encourage people to present ideas. I tried to create an open environment where people feel free to do so. No decision has been made.

Ms. UNDERWOOD. So are you aware of any data that would support that option that you are weighing as you are making your decision?

Secretary MAYORKAS. I am aware of data on both sides of the argument, Congresswoman. I can assure you that no decision has been made. We review the data and we review all factors that inform our decision, not just with respect to detention, but with respect to every aspect of our work across the breadth of our mission.

Ms. UNDERWOOD. The evidence against family detention is overwhelming, even within the limits of our current immigration system. The American Academy of Pediatrics finds that there is no evidence that any amount of detention is safe for children. Even the shortest periods of detention can cause trauma and long-term health consequences. There is also no evidence that it meaningfully deters families from coming to the U.S.

Meanwhile, study after study after study has shown that Alternative to Detention programs, or ATD, are generally more humane and more cost-effective than detention. According to ICE, the daily cost to the U.S. Government per participant is \$8 for ATD compared to \$150 for detention. It is also effective. Ninety-five percent of those on ATD appear for their final hearings.

Family detention is immoral, it is un-American, and it is just plain wrong and we have better alternatives available. Reinstating this policy would be unacceptable, full stop. This administration must do better. We have to do better.

And we are here to be partners with you to get that done, sir, and to help build an immigration system that supports our economy, that protects our communities, and that upholds our values.

I yield back.

Mr. JOYCE. Thank you, Ms. Underwood.

Mrs. Hinson.

#### U.S. BORDER PATROL: HIRING

Mrs. HINSON. Thank you, Mr. Chairman.

Good morning, Mr. Secretary.

Secretary MAYORKAS. Good morning.

Mrs. HINSON. Thank you for appearing before our committee and answering our questions.

Your budget request, I believe you have \$77.4 million for border management staffing. Is that correct on my number?

Secretary MAYORKAS. I believe that is correct.

Mrs. HINSON. How many additional Border Patrol agents does that number and that funding level support hiring?

Secretary MAYORKAS. I want to make sure that I speak accurately here, Congresswoman. I don't want to make a mistake, because there are two elements of the budget that go to personnel of our U.S. Border Patrol agents and Customs and Border Protection writ large.

Mrs. HINSON. Who have specifically asked for the agents that are out on the border.

Secretary MAYORKAS. There is a drawdown from Department of Defense, which we calculate separately. Our Department, since 2006, every single year has depended upon that Department—

Mrs. HINSON. I am not asking about 2006, Mr. Secretary.

Secretary MAYORKAS. Oh, I am sorry.

Mrs. HINSON. I am asking about how many agents you are planning to add to your list. I believe the number is 350 Border Patrol agents, if I am correct.

Secretary MAYORKAS. 350 Border Patrol agents in fiscal year 2024. This fiscal year, we added 300, the first time since 2011.

Mrs. HINSON. Is this what CBP is telling you they need to be able to secure the border and provide that operational security? Is that the number, or is it more?

Secretary MAYORKAS. It is 300—remember something, if I may, Congresswoman. There is a limit to how many we actually, functionally can hire in a particular year. We need more Border Patrol agents than 350—

Mrs. HINSON. Which is my biggest concern, because there is 800 or so of those positions that are open right now. So I guess my biggest question is, when you look at 19,000 staff Border Patrol agents, which is what we have right now, funded for 19,800, 800 of those positions are currently open.

So when you are coming to us and saying you need more Border Patrol agents, the policies of this administration have truly affected retention for CBP.

So when we are down 800 currently, how can you tell me realistically that when you are coming to us to ask for these many new positions, you are going to be able to feasibly actually hire this many new people?

Secretary MAYORKAS. Oh, Congresswoman, we are focused intensely on recruiting and retention. As a matter of fact, I spoke with the International Association of Chiefs of Police just last week about the challenges of recruiting and retention, not specific to the Federal Government, but with respect to law enforcement across this country.

We are very focused on filling the positions of the U.S. Border Patrol, of filling the positions of Office of Field Operations, of filling the positions of the United States Secret Service.

#### BORDER SECURITY: CARTELS

Mrs. HINSON. Well, I think it would certainly help if we didn't have defund-the-police rhetoric around the country as well, because law enforcement is struggling. You are right. I hear that from my local law enforcement back in my district. It is why I am so concerned about the security of the border.

When the CBP Chief is saying that you need 22,000 agents total to counter the crisis, that is a total of 3,000 more agents. This request only provides for 350 more, plus I mentioned those 800 positions open.

So I see it as a lack of meaningful work to address the retention challenges. They don't match what CBP is actually asking for. Throwing out increased numbers looks nice, I think, but it does not actually address the reality of the situation at our southern border.

Mr. Secretary, are you aware of how many times in your budget request you mention the word “cartel”?

Secretary MAYORKAS. No, I am not, but I must say that I respectfully disagree.

Mrs. HINSON. It is zero. It is zero, Mr. Secretary.

Secretary MAYORKAS. Oh, Congresswoman, we are——

Mrs. HINSON. In the 100–page document that submitted, you mentioned the word “cartel” zero. You mentioned transnational gangs once, if that is your preferred way of addressing the term, what you call cartels.

I am very concerned when you say you are addressing the cartels in unprecedented ways, the cartel activity along the southern border and in the homeland has escalated. And I can say both times that I have visited the southern border, I have seen that countering the cartel activity was a number one concern for our CBP agents. But it is a clear indication that you are not listening to the men and women on the front lines.

Would you agree that the cartels are a cause of the uptick of the deadly fentanyl surge in our country and the violence at our southern border?

Secretary MAYORKAS. I agree 100 percent with that. I disagree with 100 percent of your mischaracterizations of our commitment to border security, to tackling the cartels, to battling fentanyl. The fact is that we are supporting fully the men and women, the personnel of the Department of Homeland Security.

Mrs. HINSON. Well, the fact is that, Mr. Secretary, with all due respect, we were here a year ago, and it feels a little bit like déjà vu when I was asking you if you were hearing about the morale within the Department at CBP.

When the Chief of the Border Patrol is telling us that the border is not secure and that men and women at the border feel disrespected by the policies of this administration, it is very clear to me, sir, that there is a lot more work to be done and that you need to listen better to the men and women who are putting their lives on the line every single day.

Mr. Chair, I yield back.

Mr. JOYCE. Thank you, Mrs. Hinson.

Mr. Case.

#### FY 2024 BUDGET: FEMA

Mr. CASE. Thank you, Mr. Chair.

Let me just start by agreeing with all of my colleagues on the panel that I believe the situation at the border is a very critical issue, and I think anybody that walks away from that basic statement is not facing the realities.

And I believe that this committee and this subcommittee can be and should be part of the solution as opposed to part of the problem. We have too many in our body and beyond our body who view this in a very binary, polarized approach. And I think that there are eminent solutions that combine the best of all worlds. So I think we should try to focus on how can we come up with a bill that actually solves this problem as opposed to worsens it.

I don't want to focus there. That is what I want to say about the border. It is critical. We need to fix it. But your Department han-

dles a lot more than just the southern border. In fact, Customs and Border Protection is 19 percent of your total budget, as I believe is the case. That leaves 81 percent in an area that you fill critical responsibilities throughout our government.

You are responsible for the Federal Emergency Management Agency. You are responsible for the U.S. Coast Guard. You are responsible for the Immigration and Customs Enforcement, the Citizenship and Immigration Services, the Cybersecurity and Infrastructure Security, the Transportation Security Administration, the U.S. Secret Service, which is not just about protecting our President. It is about financial crimes around the world. You are responsible for Federal Law Enforcement Training Centers that assist our State and local law enforcement. That is 81 percent of your budget.

And so, if all we are going to do is talk about the border, which is critical, then we are doing a disservice to the remaining areas that you are responsible for. So I want to give you a little bit of love in terms of those areas, because we cannot neglect them.

Let me ask you two or three kind of quick questions along these lines. First of all, FEMA, is it sustainable under your budget? Certainly, it has been strained. It is 29 percent of your total budget. We certainly have seen an uptick in emergencies, and we have seen an uptick in the need for FEMA, including just the last few weeks. FEMA is in high demand.

Does your budget provide a realistic, sustainable funding level for anticipated emergencies throughout our country?

Secretary MAYORKAS. Congressman, it does. The President's fiscal year 2024 budget does, indeed, support funding for FEMA. The criticality of funding FEMA has never been more important than it is now.

You speak of the increasing number of natural disasters. It is not only the increasing number of them, but the increasing gravity of them.

I visited, as I mention in my opening statement, Mississippi, on Sunday. The town that I visited, Rolling Fork, Mississippi, where the tornado ripped through that small town, that poor town in about 20 seconds, and the winds moved between 160 and 200 miles per hour, just devastated the community.

We are, in fact, investing in FEMA for fiscal year 2024, and I appreciate the support.

#### FY 2024 BUDGET: TSA

Mr. CASE. Okay, thank you.

The Transportation Security Administration, Americans are traveling much more. Other people from other countries want to travel here. Does the budget address the incredible upsurge in travel post COVID, pent-up demand, and what I think is going to be a sustained level of demand on the TSA?

Frankly, I am not sure it does adequately take care of that load, but I would like to hear your comments on whether this budget addresses what you reasonably anticipate to be demands on TSA.

Secretary MAYORKAS. Congressman, if you have concerns with respect to the funding of TSA in the fiscal year 2024 budget, I would welcome the opportunity to sit down and discuss those concerns with you, because we are very focused on TSA for precisely

the reasons that you express. Not just the opportunity, the economic opportunity of lawful trade, but also, of course, lawful travel, and the security of that travel.

The Fiscal Year 2024 budget invests in our people, our greatest resource, not just in additional personnel, but in pay fairness for them, and critically in technology and other assets. We are harnessing technology in the air environment to facilitate lawful travel and to maintain its security at all times.

#### INDO-PACIFIC PARTNERSHIPS

Mr. CASE. Okay. Thank you. And finally, in the time I have remaining, it is probably going to be a rhetorical question in the time I have remaining, when we talk about Homeland Security, I think we all know that we are not talking about Fortress America. We are talking about Homeland Security in a global context, that we need to be working with our international partners and allies in terms of joint Homeland Security efforts.

I think in terms of my own Indo-Pacific, where you have wide partnerships with others throughout the Indo-Pacific in areas such as human trafficking, financial crimes, cybersecurity, et cetera.

I am just going to make a comment that I hope and believe that this budget enhances those partnerships, because they are going to be critical, given the malign influence out there in the rest of the world.

I yield back.

Mr. JOYCE. Thank you, Mr. Case.

I recognize Dr. Harris.

#### U.S. BORDER PATROL: HIRING

Mr. HARRIS. Thank you very much.

And thank you, Mr. Secretary, for being here.

I am just going to add to the concern that the gentlelady from Iowa had. It is strange the administration wants to hire 350 Border Patrol agents and 87,000 armed IRS agents. Perhaps you should go over to the IRS and see if they will share some of that wealth with you or support our efforts, perhaps, to transfer some of that funding. And that was a rhetorical comment.

I yield the balance of my time to Mr. Guest.

Mr. JOYCE. Thank you, Dr. Harris.

Mr. Guest is recognized.

#### BORDER SECURITY: STATISTICS

Mr. GUEST. Thank you, Mr. Chairman.

Mr. Mayorkas, today's Washington Times headline: "Border crisis questions baffle Mayorkas, Republicans fume." I am sure you would probably disagree with that headline. I know you didn't write that.

But I just want to talk about some statistical data about why Republicans are so concerned about what is happening on our border, specifically the southwest border, but also as we are seeing increased activity on the northern border.

For the last 12 months, we have seen more than 200,000 immigrant encounters along our northern and southern border. For the

last 24 months, expanded out 12 months beyond that, we have seen at least 185,000 immigrant encounters along our northern and southern border. We know that in the month of December of last year, we saw over 300,000 encounters along the northern and southern border.

In addition to that, we see the growing chaos that fentanyl and drug cartels have caused in every community. We know now that the leading cause of death for individuals 18 to 45 is, in fact, drug overdose, the large majority of those associated with fentanyl.

I had the opportunity just 2 weeks ago to be back on the border, my second time this year, but just 2 weeks ago in McAllen, where, as a member of the Homeland Security Authorizing Committee, we had an opportunity to speak with Border Patrol Chief Ortiz. And he also addressed, in an informal briefing, members of this subcommittee, the week prior.

In that hearing, there were some things that I thought came out that were very enlightening, one particularly when I had the opportunity to talk to the Chief about some prior statements made by the administration, not only by you, but by the President, the Vice President and others, about the border being secure.

And, again, looking at statistical data, trying to understand how, with the large increase in immigrant encounters, with the increase of drugs, with the violence that we are seeing on the border, again, much of that on the Mexican side of the border, but we saw four Americans who were kidnapped, two killed, a third shot as they crossed across the border there in the RGV sector, seeking a medical procedure.

We saw the recent rush of over 1,000 immigrants there in El Paso when someone put something out on social media that the border was going to be open. We know that drug cartels have become emboldened in the fact that they are making huge sums of illegal profits off of both human smuggling and narcotics smuggling.

But when the Chief said that five of the nine border sectors were not secure, in his opinion—and he is your Chief of the Border Patrol. He said five of the nine sections were not secure. Now, he didn't specifically mention which sectors. I believe he was probably referring to Del Rio, El Paso, the RGV sector, Tucson, and then the last either being San Diego or Yuma, but I did not follow up with him exactly which sectors that he was referring to.

And he also talked about the number of got-aways that is reported by the administration he believes is actually an under-reporting, and that, in his opinion, that that number is 10 to 20 percent higher.

And so during the 2-plus years of this administration, we have seen over 4.8 million encounters. DHS has reported 1.2 million got-aways. So that is going to be a total of 6 million encounters along the southwest border.

Just looking at the population of the States throughout the United States, that total number, if they were all placed in the same geographical area, that would be the 20th largest State in the United States.

And so, I guess my question to you, Secretary, is, do you still maintain that, with all the statistical data that is out there and

with the statements of your Border Patrol Chief, do you still maintain today that our border is secure?

Secretary MAYORKAS. Congressman, you have covered a tremendous amount of land in your remarks.

I very much appreciate the time that we have spent together addressing the seriousness of the challenge at our southern border. I look forward to meeting with you and to discussing the matters that you have raised in your remarks preceding your question.

I work very closely with Chief Ortiz. Actually, I selected Chief Ortiz to lead the U.S. Border Patrol, and I am very proud of his leadership and very supportive of it.

The seriousness of the challenge at our southern border cannot be understated. We are focused intensely on it. I welcome the opportunity to speak with you about what we are doing about it, the surge of resources, the new programs that we are implementing, and how we are maximizing the resources that we have to deliver the most effective results. I look forward to doing so.

Mr. GUEST. And just yes or no—and I know I am over time. And I apologize, Mr. Chairman.

But yes or no, do you maintain today that, in light of the statements made by Chief Ortiz, that the border is secure?

Secretary MAYORKAS. Congressman, I stand by my prior assessment because, indeed, I define it as maximizing the resources that we have to deliver the most effective results.

Our ability to detect, interdict, and respond to threats has increased over the years because of our incredible personnel, because of our use of technology and harnessing innovation as force multipliers.

Mr. GUEST. Mr. Chairman, I think I am over time. So I will yield back.

Mr. JOYCE. Thank you, Mr. Guest.

The chair recognizes Mr. Cloud.

#### BORDER WALL: CONSTRUCTION

Mr. CLOUD. Thank you, Mr. Chair.

And thank you for being here.

In 1996, we passed the Illegal Immigration Reform and Immigrant Response Act of 1996, as well as the Secure Fence Act of 2006, in part to authorize the construction of barriers along the southern border.

You are aware of that, correct?

Secretary MAYORKAS. I am.

Mr. CLOUD. I will note that was under both Democrat and Republican administrations.

In 2021, we funded more border infrastructure. You are aware of that?

Secretary MAYORKAS. Yes.

Mr. CLOUD. And I am sure, this is basic constitutional, but as the Article I branch, our job is to make the law. Your job is to execute the law. Is that correct?

Secretary MAYORKAS. Oh, most certainly. As a matter of fact, I have been very proud to enforce the laws.

Mr. CLOUD. And yet you canceled contracts for construction of the border wall. Is that true, you have canceled contracts for construction of the border wall?

Secretary MAYORKAS. Congressman, I can assure you that we will comply with all our legal obligations.

Mr. CLOUD. Right now we are paying for border wall to be stored instead of built. Is that correct?

Secretary MAYORKAS. I have approved, as I testified earlier—

Mr. CLOUD. Is that correct, yes or no?

Secretary MAYORKAS [continuing]. Approximately 129 gates in gaps. That project is underway.

Mr. CLOUD. Yes or no, are we paying for border wall to be stored—

Secretary MAYORKAS. We are indeed.

Mr. CLOUD [continuing]. Instead of built? Thank you.

That includes Texas, who is trying to buy it, to build it themselves. You stopped Texas from buying border wall?

Secretary MAYORKAS. Congressman, I am not familiar with that. I will certainly look into that and touch base with you in the days following.

Mr. CLOUD. You keep talking about force multipliers as well. When I talk to the boots on the ground, they talk about the border infrastructure, specifically the wall, the roads that go along with it, the getting—chopping down the carrizo cane, the technology that is involved, all being one of the most effective force multipliers in the sense that you can have two or three people patrol a few miles of border as opposed to dozens.

It is pretty significant that we do this. Yet Biden's border budget request takes the money that we have already allocated and moves it to other directions. Isn't that correct?

Secretary MAYORKAS. I am confused by your question, Congressman. I can assure you that—

Mr. CLOUD. The border that you are here to propose takes money that we have already allocated for the border wall and moves it to other objectives. Isn't that correct?

Secretary MAYORKAS. We are seeking to invest in people.

Mr. CLOUD. It is a yes-or-no question.

Secretary MAYORKAS. Congressman, we are seeking to invest in people and technology.

Mr. CLOUD. It is not an either/or, people or border infrastructure.

Secretary MAYORKAS. No. That is why I am saying I—

Mr. CLOUD. You are taking what we have already authorized, what we have already appropriated for border wall construction, and you are wanting to rescind that and use it for other purposes. Isn't that correct?

Secretary MAYORKAS. Congressman, we will comply with our legal obligations for fiscal year 2023.

#### BORDER SECURITY OPERATIONAL CONTROL

Mr. CLOUD. That is a very well-worded way to get around. You find these loopholes, and you are missing the objective, the overall objective of securing the border by finding these little legal loopholes to get out of things.



For example, the Secure Fence Act of 2006 defines what operational control is as “the prevention of all unlawful entries into the United States, including entries by terrorists, other unlawful aliens, instruments of terrorism, narcotics, and other contraband.”

To be clear, that is the only definition that exists legally of operational control. Isn’t that correct?

Secretary MAYORKAS. I believe that is the statutory definition under the Secure Fence Act of 2006.

Mr. CLOUD. And I understand a point that you have made that it does say “all”, and as long as it says “all” you can never perfectly achieve operational control. You made that point.

But have illegal entries increased or decreased since you became Secretary?

Secretary MAYORKAS. Oh, there is no question.

Mr. CLOUD. Have they increased or decreased?

Secretary MAYORKAS. First of all, you are absolutely correct that under the Secure Fence Act definition, no administration has achieved operational control. It speaks of preventing all unlawful entries. That means, one, get it right.

Mr. CLOUD. Right. But your job should be to be moving us in the proper direction.

Secretary MAYORKAS. Oh, we have——

#### MIGRANT ENCOUNTERS: UNACCOMPANIED CHILDREN

Mr. CLOUD. And we have more illegal entries. We have terrorists coming across our border. And the fentanyl coming across our border has increased. All these things have gotten worse, not better.

So whether you say you have perfectly achieved it, you are certainly not moving toward it. You are moving away from it.

And we all appreciate the boots on the ground who are doing their best to do the job. But I can tell you, I have been down there, they really don’t appreciate the job that they are seeing and the leadership that they see coming out of your office right now.

One other question I wanted to ask you. How many children have been lost between you and HHS?

Secretary MAYORKAS. Congressman, we do not—I don’t know of a single child that we have lost in our responsibility to turn over an unaccompanied child to the Department of——

Mr. CLOUD. To——

Secretary MAYORKAS. Excuse me.

Mr. CLOUD. To HHS, yeah.

Secretary MAYORKAS. To the Department of Health and Human Services within 72 hours, which is our legal requirement.

I am not aware——

Mr. CLOUD. The Biden administration cannot find 42,577 children.

Secretary MAYORKAS. If I may, Congressman, I am not aware of a single child that we have lost in executing our responsibility to take an unaccompanied child in our custody and turn it over to the Department of Health and Human Services.

Mr. CLOUD. Right now the Biden administration cannot find 42,577 children who are going to, quote, “sponsors,” many of whom are connected to cartels. And it astonished me yesterday that you have never seen these.

I personally dug these out of the mud at a gap in the border. It says “coming” and “going” in Spanish on it. On it are digital numbers that the cartels use to track people to make sure they are paying their way both before they get into our country and after they get into our country.

I brought these as a gift to you because I have a number of others, and I will be happy to give these to you.

Last year we were told that we were going to plus up the budget, and because of it, we would be able to secure our border. We would do all these great things, raises for the good men and women, boots on the ground.

And I asked this question. I said the problem is, is we write the check to secure the border and the Biden administration gets it and they say: Yay, more money for human trafficking operations.

How is that going to change?

Yet, what we have seen over the last year is the continued operation of the border being even more a sieve, even more aiding and abetting the cartels in their nefarious actions that destabilize Central and South America, Mexico, and make our communities less safe.

And so if we are going to address the border funding, we have got to see action and we have got to see those trends reversed.

I apologize, Chair, for going over. I yield back.

Mr. JOYCE. Thank you, Mr. Cloud.

Mr. Guest is recognized.

#### MIGRANT ENCOUNTERS: STATISTICS

Mr. GUEST. Thank you, Mr. Chairman.

Mr. Secretary, just getting back to border statistics, when you became Secretary the last month, January of 2021—I understand you were not Secretary for the entire month—there were 95,000 encounters along the northern and southern border. Two months later, in March of 2021, that number jumped to 192,000.

Since that time, there have only been 2 months during your time as Secretary where those numbers have dropped below 192. October of 2022, 187. January of—I guess that would have been—January of fiscal year 2022 would have been 186.

So we have seen those numbers increase very dramatically. Now, we know they are down from the all-time high of December. December they were over 300,000. And we have seen a drop. They still are greater than they were fiscal year last year.

So January of 2023, the numbers still outpaced January of 2022. February of 2023, the numbers outpaced February of 2022. We know last year set a record of 2.7 million, up from the previous record the year before of 1.9 million. And as I understand, we are on track to once again break that record once again.

And so I am trying, by using statistical information, to get back to how this administration can again maintain that the border is secure.

I know you say we do a better job of detecting individuals coming across, but I think we do a poor job of deterring anyone from coming across. It does not appear to me that anyone has any concern about coming across the border and any potential consequences that that may result in.

Let me ask you this, Mr. Secretary. Do you believe that wall construction, or walls in general, that they are an important component to securing the border?

And I understand we are not going to be able to build a wall from sea to shining sea, and that is not what I am talking about. But I am talking about, in particular sectors of the border, have we not seen that walls are effective?

Secretary MAYORKAS. Congressman, may I respond to something that you said preceding your question?

Mr. GUEST. Yes, sir.

Secretary MAYORKAS. There are two things to remember, if I may.

Number 1 is that the level of migration throughout the hemisphere signifies that it is not a challenge specific to our southern border. It is a very serious challenge at our southern border but not exclusively so.

You speak of deterrence, you speak of reducing the number of encounters. On January 5, we issued new policies with respect to some of the most challenging demographics that we were encountering at our southern border, Cubans, Nicaraguans, Venezuelans, and Haitians. We must keep in mind that it is very difficult to remove individuals from Cuba, Venezuela, and Nicaragua because of our absence of diplomatic relations.

What we have said is that we will deliver a safe, orderly, and lawful pathway for you if you avail yourself of it. We screen and vet individuals before they arrive at our border. If you don't use those lawful pathways, we indeed will deliver a consequence to you if you show up in between the ports at our southern border.

We have seen an approximately 95-percent drop in the number of encounters of individuals from those four nationalities in between our ports of entry at our southern border.

That is the type of structure, that is the policy underpinning that we need to pursue, and I very much look forward to doing so with you.

More fundamentally, we need to work together to pass immigration reform because this system is broken.

Mr. GUEST. Well, and I agree the system is broken. I mean, immigration court has over a 2 million-case backlog.

Secretary MAYORKAS. Indeed.

#### BORDER WALL: CONSTRUCTION

Mr. GUEST. We last year adjudicated roughly 300,000 cases. So my math, my public school math from back in high school, if you equate that out, that is a 7-year backlog.

And so as we are talking about we are allowing people to remain in the country, we are not allowing them to remain in the country for days or weeks. We are allowing them to remain in the country for years.

And so when someone has been in the country for 7 years before they have an immigration hearing, that to me is a broken system.

And I understand that that is beyond your control. But clearly our immigration system is broken. Our asylum system is broken.

But we do not have a secure border, Mr. Secretary. And that is where you and I would just have to disagree. I do not see any cir-

cumstance where I can go back to the people that elected me and tell them that our border is secure.

But I would like to know, as it relates to barriers, fences, walls, whatever you want to call them—Secretary Ortiz was here. Again, briefed members of this committee 2 weeks ago. He said that that is an important part of border security, wall construction. He told us in the hearing that we had in McAllen that he disagreed with the administration when they stopped wall construction.

Apparently you must agree that there is at least some benefit of it because you talk about the fact that you have approved 129 projects.

Now, those projects, you say, are to close gaps. So they are not really for new wall construction, for any significant purpose, but at least to close gaps.

So how important are fences? How important are barriers? And why has this administration acted so slowly to incorporate that into the entire strategy?

I mean, we are looking at a border strategy. And it seems to me that this administration, whether it be you or whether it be the people that you answer to, are just saying: We are not going to build any walls. Walls are bad.

I disagree with that. I think that walls are beneficial. I think that they do a great job.

And I know I have gone over time. So I am going to allow you to answer. And then I will yield back.

Thank you, Mr. Chairman.

Secretary MAYORKAS. Congressman, you are correct that the asylum system, as part of the entire immigration system, is broken. They are all broken.

You mentioned that that is beyond anything that we can do. Actually, this is the first administration that has done something about it within its administrative authorities. We issued an asylum officer regulation that enables asylum officers, rather than immigration judges, to make the final asylum adjudication.

We are taking that years-long process that is unworkable and bringing it down to less than a year. That is our objective. I do believe that closing the gaps is important, which is precisely why I approved those projects.

Mr. JOYCE. Thank you, Mr. Guest. My public school math also agrees with you.

Ms. DeLauro, the distinguished ranking member of the whole committee, is here.

#### FY 2024 BUDGET: IMPACTS OF BUDGET CUTS

Ms. DELAURO. Thank you. Thank you so much, Mr. Chairman, and to you, Ranking Member. I said in the last hearing thank you for allowing me to just interlope here. There are about five hearings today and I am trying to get to all of them.

And welcome to you, Mr. Secretary. It is a pleasure to see you.

Mr. Secretary, you recently highlighted to this committee some of the challenges the Department would face if it were to cut, as some Republicans would like, cut fiscal year 2024 to the 2022 levels. Challenges, I think, would be alarming: reducing Customs and Border Patrol frontline law enforcement staffing, reducing the De-

partment's ability to prevent drugs from entering the country, and cutting Federal assistance to States and localities.

Another area that I am going to ask you to comment on is cutting TSA at our airports and what that would mean. And then a quick question about the Coast Guard.

So if you can, describe in further detail how dangerous would the cuts be. What would be the impact of cutting the—going back to 2022 levels in terms of Border Patrol, drugs entering the country, trafficking, et cetera?

Secretary MAYORKAS. Ranking Member DeLauro, thank you very much for your question.

Cutting that budget down to its fiscal year 2022 level would be devastating across the breadth of the entire Department of Homeland Security mission.

Not only would it weaken our efforts to secure the border, not only would it weaken our fight against the cartels and stopping the flow of fentanyl, it would mean longer lines at airports at a time when travel, lawful trade—lawful travel—is rebounding, a source of economic prosperity. The American public would be waiting hours and hours at airports.

Our cybersecurity would be weakened at a time when adverse nation-states are enhancing their cyber attacks and cyber capabilities to do us harm. We would be less protected.

Communities around this country would be less protected against an increasing frequency and gravity of natural disasters. We would not be able to respond as ably and to improve the resilience of communities across the country.

I was just in Rolling Fork, Mississippi, seeing a community devastated by a natural disaster, a vicious tornado. This past Sunday I was there.

So that covers FEMA.

Our United States Coast Guard would not be adequately resourced at a time when securing the Arctic and the Indo-Pacific is more important than ever, given the aggression of Russia and the People's Republic of China.

Our leaders would be less protected given a cut in funding to the United States Secret Service, which also does extraordinary financial investigations that help to secure the homeland.

It would be a devastating move.

Ms. DELAURO. I just would say—and, obviously, you know, I think sometimes we lose track of the breadth of the mission, of the portfolio of the Department of Homeland Security.

And so that if you tracked in each of the areas and you make these extreme cuts that what—and I just say this in all sincerity, that I think the reason why I raise it is because—and this is to all of my colleagues on both sides of the aisle—that it is easy to say we are going to go from—we are going to go—in 2024 we are going to go back to 2022.

But one has to take a look at what the consequences are about areas that you care about. Some that you don't care about, you are happy that it us going back. But those things that you do consider and care about are really going to be at great risk.

And the comments of the emphasis on border and the issue of drugs and the trafficking, and the trafficking of youngsters, et

cetera, would be, according to what you have talked about, is that would lessen our opportunity to be able to deal with that effort.

And I would just say about waiting lines at airports, Americans are not terribly excited about waiting in lines at airports or anywhere else, and I think the repercussions on that would be pretty critical.

I appreciate your testimony today. I really do. But I particularly commend you for the work that you do, not an easy task as the Secretary of Homeland Security. But thank you very, very much for your commitment and dedication to the effort.

Secretary MAYORKAS. Thank you, Ranking Member DeLauro.

Ms. DELAURO. Thank you, Mr. Chairman. Really appreciate it.

Mr. JOYCE. Thank you. And I can't believe for a moment you wait in any lines, Ranking Member DeLauro.

Ms. DELAURO. I do, especially the line that is for either Sally's or Pepe's Pizza in New Haven. You don't jump the line because it is a political disaster.

Thank you. [Laughter.]

Mr. JOYCE. Sheriff Rutherford is recognized.

#### MIGRANT ENCOUNTERS: VETTING

Mr. RUTHERFORD. Thank you, Mr. Chairman.

Mr. Secretary, I was very glad to hear you speak well of Chief Ortiz. I have met him a few times. I think he is a man of integrity, honesty. He speaks his mind. And I think when he spoke of the lack of operational control at our southern border, I think he did that out of a respect for his position, the officers that he works for.

And I certainly hope that there is no pressures brought to bear on him, that he doesn't retire here in 6 months. He is a good man. And I hope we can all continue to support him after this.

I want to bring up migrant vetting. We know that DHS and HHS have facilitated the movement of migrants into the interior of the country without notifying local government agencies. And this is done either through grants to nonprofits or, in some cases, the unaccompanied minors, we even governmentally do that.

And the problem with the lack of vetting, that these migrants are getting popped up in my hometown of Jacksonville, Florida, where we had a case where an illegal immigrant came across the border, lied about his name, lied about his age, was vetted by DHS, turned over to HHS. They still couldn't verify who he was because he was using a fake name and a fake date of birth, a fake date of birth that made him a juvenile.

And so we sent him to the interior of the country. We sent him to his uncle, his Uncle Cuellar in Jacksonville. Not his uncle. They didn't vet his uncle. They just accepted it. They make a phone call, and that is it. They don't vet Uncle Cuellar.

They sent Mr. Ulloa to Jacksonville. He killed Mr. Cuellar. That is because of our system where we are not vetting people properly.

Then, on top of that, this administration is not even confirming the identities of people that we are turning children over to. We have got cases where many children are going to the same sponsors, to the same kids. We are participating in child trafficking, all with the coordination—or all without the coordination or notification of any local government officials, particularly law enforcement.

The non-detained dockets consist of people that have been released to the interior of the country, and they are either waiting for their case to work through the immigration court system or they have an order for removal.

In fiscal year 2022, ICE's annual report, it was indicated that there was a 29 percent increase in that number that is waiting there, their time on the docket.

Another really shocking number to me was that there are 1.2 million people that have had their cases adjudicated, they have gone through that long wait and been adjudicated, and now we have a final order of removal, but they are still in this country, 1.2 million.

The number of people with final removal orders on the non-detained docket continues to grow. ICE is not making this a priority. And deportations are, even though they are up this year, they are way down from where they had been before, even under the Obama administration.

Now, in fact, the last time you testified before this subcommittee we discussed the deportation numbers. And I want to revisit that topic briefly.

In 2022, as I just mentioned, it did go up a little bit, to 72,177 migrants. And that is an increase from 2021 when there were only 59,000 removals. But that is still far below the Trump years. That is even far below the Obama years.

Now, the last time you were in front of this committee you said ICE was removing a higher percentage of criminal aliens in fiscal year 2021, and that was true, but it was a larger percentage of a much, much smaller number.

Now, finally, since we allow people to invade our country because we do nothing to stop them. All we do is process them more quickly.

The whole six-pillar program, that when Title 42 goes away, the entire six-pillar program—I have read every pillar—not one of them is designed to stop somebody from coming to America illegally. It is to process them more quickly so we can get them to the interior of the country. And when we don't vet them properly, they are going to kill more of our American citizens. That is what I am opposed to.

Now, because of the situation at the southern border, as was mentioned earlier by one of my colleagues, now we have a problem at the northern border. In fact, we just saw an 846 percent increase in illegal crossings at the northern border.

President Biden's open border policies have made every town a border town and put our constituents—my constituents—at risk. Every CBP officer, every ICE officer, the cartels, everyone knows it, even Chief Ortiz.

With that, Mr. Chairman, I yield back.

Mr. JOYCE. Thank you, Sheriff.

Last but not least, Mr. Trone. I apologize for the delay.

Mr. TRONE. No problem. We had a couple of—lots of conflicts.

Thank you, Mr. Secretary, for being here today.

Thank you, Mr. Chairman, Mr. Ranking Member.

In this complex and often toxic landscape, we certainly appreciate the challenges you face. And we want to thank you very much and appreciate your service.

Safe and orderly legal migration is in line with our shared American values and good for the communities, good for the economy. In this Nation we do not look down on immigrants seeking a better life, we seek to lift them up, and they become part of the fabric of our Nation.

Extreme Republicans do not want to acknowledge that securing our borders against drug trafficking and fixing our broken immigration system, they are not mutually exclusive.

We know that 90 percent, over 90, is trafficked through official points of entry, driven by U.S. citizens and legal residents, not asylum seekers. Cartels are not packing opioids in backpacks to be carried across the border. That is a myth, and it is harming our ability to develop data-driven and bipartisan solutions.

So, Congress, we need to work with the administration to address this opioid epidemic as a public health crisis, not one linked to immigration, and expanding treatment for substance use disorder, and of course disrupting drug trafficking as we can.

Across the southern border ports of entry U.S. trucks and commercial vehicles are scanned selectively and not too often. The TCOs have long benefited from this. CBP needs to increase their routine scanning of these vehicles at the ports of entry.

The President's budget put in \$305 million for new, nonintrusive inspection technology to increase the efficiency of the 200,000 cars arriving daily without impacting business and critical trade. But without a systemic rollout at all the ports of entry, smugglers will continue to go back and forth and we play whack-a-mole as they move their products elsewhere.

The White House policy of ONDCP has set a goal of 123 scanners, large-scale scanners, up by fiscal 2026. Help us explain why we are 3 years behind.

Secretary MAYORKAS. Congressman, thank you very much for the question.

We are really pushing forward on our implementation of the non-intrusive inspection technology. It is an easy, fast, effective way of detecting contraband of different types, including fentanyl, in passenger vehicles and in trucks and trailers through the ports of entry.

We need the funding to purchase additional technology. We need the funding to hire additional personnel. We are looking to harness artificial intelligence.

We also are critically in need of modernizing our ports of entry, the fundamental infrastructure, which is so antiquated in so many critical areas.

For example, one of the ways that we seek to implement the non-intrusive inspection technology is in the preprimary screening area.

The Nogales port of entry that I visited last week—not my first time certainly—the Nogales port of entry is immediately on the line, on the border, and does not allow for the preprimary inspection that CBP considers to be optimal.

So we have a number of hurdles that we need to cross, and the FY 2024 budget addresses those hurdles most effectively.



Mr. TRONE. And 3 years behind?

Secretary MAYORKAS. Congressman, we are working feverishly. Ranking Member Cuellar noted the challenges of a slow procurement process, which is precisely why we have the Procurement Innovation Lab to cut through that. We are moving as quickly as we can.

Mr. TRONE. Well, we appreciate that. And please keep up the work.

And I yield back.

#### MIGRANT ENCOUNTERS: MARITIME INTERDICTIONS

Mr. JOYCE. Thank you, Mr. Trone.

Upon mutual agreement with the ranking member, we are going to proceed to a second round of questions. And I recognize myself to start.

The Coast Guard is interdicting near record numbers of maritime migrants. Fiscal year 2022, the Coast Guard interdicted 12,500 migrants, primarily in the Caribbean transit zone. At times during the past year, its assets were at capacity for holding migrants.

Discouraging migration along marine routes by prompt interdiction is important both for U.S. border security and the safety of the potential migrants, particularly when the boats on which the migrants travel are often overcrowded and not seaworthy.

The vast majority of migrants interdicted by the Coast Guard are returned directly to their home nation. They are not processed on U.S. soil.

Despite the dangers of marine migration routes, increased security on the land border may push migrants to attempt migration via maritime routes.

How does the budget support the increased number of migrants interdicted along maritime routes?

Secretary MAYORKAS.

Mr. Chairman, we are very focused on the challenge of maritime migration. We saw an uptick in that, given the situation in Haiti, which is extremely dire, and given the authoritarian, repressive regime in Cuba.

We surged U.S. Coast Guard assets in the maritime environment to increase our interdiction capabilities.

We also are critically enhancing our communications in those island countries to ensure that people understand the perils of that journey—too many people perish at sea.

We also are building lawful pathways for individuals to be screened and vetted in advance and to come in a safe and orderly way to the United States, rather than taking that journey.

All of those efforts actually have recently reduced the level of maritime migration that we are experiencing.

With respect to our fiscal year 2024 budget, we are increasing the funding for the United States Coast Guard, which is so vitally important, as well as for other agencies within the Department that contribute to our maritime security.

Mr. JOYCE. My understanding is that Coast Guard assets have been at capacity for the interdictions in holding migrants. What is your plan if the number of migrants continue or increase?

Secretary MAYORKAS. We have surged Coast Guard assets. We also have increased our processing efficiency. We have communicated robustly with individuals who might intend to migrate with respect to the perils of the journey. We have a multipronged effort to ensure that we are minimizing the number of people who take to the seas.

The program that we announced on January 5 with respect to the Cubans, Haitians, Nicaraguans, and Venezuelans also has contributed to a decrease in the number of individuals taking to the seas because we have delivered for them a lawful, safe, and orderly path.

Mr. JOYCE. I would urge you in your position as Secretary to use your bully pulpit to put out the message that you are not going to be processed here, that you are not welcome here, and to stay where they are at. But that is up to you, sir, from here.

I recognize the ranking member, Mr. Cuellar, for any questions he may have.

#### FY 2024 BUDGET: HIRING

Mr. CUELLAR. Thank you, Mr. Chairman.

Again, looking at the Secure Act, just to make sure, the statutory definition says it means the prevention of all unlawful entries, et cetera, et cetera. That means when this got passed under President Bush, he did not have operational control. Same thing under Obama, same thing under Trump, and certainly under Biden now. It is what we do toward that goal that is important. But no President has had true operational control.

Also, just as a point of reference, Mr. Secretary, when you look at the last administration, let's say the second year of funding that Congress provided under the Homeland Security, fiscal year 20—let's look at the second year of the prior administration.

Fiscal year 2018, the Homeland funding was \$47.7 billion. The second year of this administration, it is 86.5, which is fiscal year 2023. So it is almost double the amount of money that we put in.

For CBP, the prior administration, the second year, fiscal year 2018, CBP had \$14.2 billion and ICE had \$7.1 billion. If you compare fiscal year 2023, it is CBP had \$16.7 billion and ICE had \$8.42 billion.

So the money has increased under this administration—or Congress has increased it, should I say—which leads me, we can add money, but it still goes to repercussions.

Again, you treat migrants with respect and dignity. But at the end of the day, if we have to say goodbye, adios, then we have to do that. I mean, otherwise, if we don't have repercussions—and this is something very important to our border security folks that you have.

You agree that repercussions are important, correct?

Secretary MAYORKAS. I do, Congressman. We are a Nation of laws and a Nation of immigrants. We sought to deliver a greater consequence through our title 8 authorities, and we were enjoined from doing so.

Mr. CUELLAR. And, again, just briefly on the wall, because I want to ask you about your parole program that you-all implemented.

But on the wall itself, with all due respect, that is a 14th century solution to a 21st century problem that we have. I can spend \$36 million on a mile for fencing, and all I need is \$100 to buy a ladder to take care of that particular fence.

I think the numbers have changed, \$36 million per mile, depending on the terrain, and you can spend about \$2 million on technology for one mile of fencing. So I think that technology would be a lot better.

And for anybody that is not familiar with Texas, as you know, the boundary is the middle of the river. But the fence has to be, because of certain reasons, has to be—usually it is a quarter of a mile or sometimes longer.

So you can talk about having a fence, but you cross the river, touch the bank, and guess what? They can ask for asylum at that time, or they can use drones to cross drugs itself.

So, again, I want to make sure we have the money for the personnel and the technology. That is very important.

And on the personnel, it is not only hiring agents. I want to hire more agents. I know the Border Patrol chief says that they are behind on the 300 agents that we allotted to.

But it is also the support staff that is there, the analysts and the other folks. And especially for ICE. There might be some people that don't want to hire ICE agents.

I do want to hire ICE agents. But we do need to hire the support staff for ICE so they can track the individuals that they are supposed to.

So if you can talk about the support staff that we need to hire besides Border Patrol agents or CBP agents.

Secretary MAYORKAS. Thank you so much, Ranking Member Cuellar.

It is so vitally important to increase the number of our personnel, including at ICE. The special agents, the Enforcement and Removal Operations officers, do extraordinary work and critical law enforcement work.

They can't do that work without the support of other personnel. It is a process from beginning to end.

We need a tremendous number of additional personnel, which is why the fiscal year 2024 budget provides for increased numbers of those personnel across the enterprise.

#### H-2B VISAS

Mr. CUELLAR. My time is also up, but let me just briefly mention this. And I know Congressman Harris is here.

H-2A, H-2B visas is a pathway that we really need to look at. I have looked at the numbers. And we have got to get this done one way or the other, increase those numbers on that.

Quickly on the parole pathway that you-all implemented on January 5.

And I will close with that, Mr. Chairman.

Mr. JOYCE. Thank you, Mr. Cuellar.

I recognize—

#### PAROLE PROGRAMS

Mr. CUELLAR. Well, can he just say a little bit about the parole?

Mr. JOYCE. You know, of course, he can answer your questions. Excuse me for interrupting.

Secretary MAYORKAS. Mr. Chairman thank you.

Ranking Member Cuellar, the parole programs that we announced on January 5 for the Cuban, Haitian, Nicaraguan, and Venezuelan nationals who are arriving at our southern border in between ports of entry in unprecedented numbers because of the repressive, authoritarian regimes in three of those four countries, and of course in Haiti, the terrible conditions there, we built lawful, safe, and orderly pathways for them to come to the United States. We deliver a consequence for those who don't take advantage of those pathways and who arrive in between the ports of entry.

We have seen an approximately 95-percent drop on the number of encounters at our southern border in between the POEs of those four nationalities. That is the model that we are employing amidst or within a terribly broken immigration system.

Mr. CUELLAR. Thank you.

Thank you, Mr. Chairman.

Mr. JOYCE. Thank you.

The chair would recognize Mr. Cloud.

#### BORDER SECURITY

Mr. CLOUD. Thank you, Chair.

And I apologize. I have to run to help down on the floor really quick. But I wanted to make a couple of points really quick.

And that is, why does that word "all" exist in that statute? I don't think it is so that administrations can come before us and have an out to what their obligation is. I think it there is to emphasize the fact that in whatever discretionary rulemaking you have that you should be doing everything you can to meet this objective.

And what we have seen is the reverse of that, that whatever authorities you have are doing everything you can to create more of a flow, to transport more people into the United States.

And from a larger perspective, yes, I agree, work visa programs, immigration, and border security are related. But they are three distinct issues. We have to secure the border first.

My wife is a naturalized citizen. And at some point we, the vast majority of us, are descendants of citizens at some point.

But half the world's population makes less than \$10 a day. We do not solve those issues by bringing everybody to the United States. We have to secure our border.

And I will just ask you one more question. How many people can fit on a ladder?

Secretary MAYORKAS. I don't understand. I don't understand your question.

Mr. CLOUD. The point is, is that we have thousands of people riding trains. We have seen thousands of people charge our border. And with a wall, even if they can build a ladder, it restricts the flow and helps provide a force multiplier for our people.

They keep asking for border infrastructure, including a wall, including the technology, including the roads. We can build it. And it is modern technology, and we all know it.

And I yield my time to Mr. Newhouse or to the chair.

Mr. CUELLAR. I will take your time. [Laughter.]

Mr. JOYCE. Nice try, Mr. Cuellar.

The chair recognizes Ms. Underwood.

#### DISASTER RECOVERY POLICIES

Ms. UNDERWOOD. Thank you so much.

Mr. Secretary, I would like to talk about disaster recovery. As you know, this is an area where my team and I have been really digging in and working with your staff on big picture questions around equity and resilience.

We know that FEMA wasn't designed with equity in mind. So it has never worked equally for everybody.

Under our current system, disaster recovery can actually make inequities worse than they were before a natural disaster. Studies have found that in counties affected by large disasters, Black survivors saw their wealth decrease by an average of \$27,000, while White survivors saw their wealth increase by an average of \$126,000. And that is on top of the already enormous racial wealth gap in this country.

Bold and deliberate policies are the only way we will be able to combat systemic racism and inequality that is built into our Federal disaster preparation, response, and recovery efforts.

Under Administrator Criswell's leadership at FEMA, I have been pleased to see equity that is being instilled as the foundation of emergency management. It is literally the first goal in FEMA's 2022 to 2026 Strategic Plan.

We are a few months into 2023. Can you share an update on FEMA's work to make disaster response more equitable so far this year?

Secretary MAYORKAS. Congresswoman Underwood, we are focused intensely on this area. If I may share with you an anecdote?

Ms. UNDERWOOD. Sure.

Secretary MAYORKAS. There was an article in the paper following a disaster that struck a very poor Black community, and the individuals in that community were unable to present to FEMA the required documentation of proof of ownership. Therefore, they risked being left disenfranchised and unable to access assistance to which they were entitled because of that lack of documentation.

Our policy back then did not meet their needs because this community didn't have deeds of trust and other documentation because their homes, very, very modest homes—

Ms. UNDERWOOD. Sure.

Secretary MAYORKAS [continuing]. Were passed down from generation to generation.

I read that article and we changed our policies, and we adapted our policies to meet the reality in which people live. We said that perhaps utility bills, an affidavit would suffice to address home ownership so that we can reach an otherwise disenfranchised community.

This issue of fairness, of equality, is of critical importance, not just in FEMA but throughout our entire Department.

## DHS EQUITY ACTION PLAN

Ms. UNDERWOOD. Excellent.

A big picture focus on equity is needed Department-wide, too, not just at FEMA. I know that DHS has a Department-wide Equity Action Plan that identifies programs with the greatest potential on advancing equity.

Can you provide an update on implementing that plan?

Secretary MAYORKAS. We are very, very well underway in that regard, and I have asked every single agency and every single office to execute on that plan.

With respect to details, Congresswoman Underwood, I would be pleased to share with you more specificity in terms of our progress in that plan.

That is indeed one of DHS's organizational priorities.

Ms. UNDERWOOD. OK. Well, I certainly do look forward to getting that information.

I would like to echo Ranking Member DeLauro's comments about the Republican leadership's proposed cuts and how devastating that would be to programs like these, which would be essential to helping every American in the response to a disaster, to make sure that we have equitable recovery in communities across this country.

I put people over politics, and I certainly am not interested in supporting those types of draconian cuts.

Thanks for being here today, sir.

And I yield back.

Mr. JOYCE. Thank you very much, Ms. Underwood.

The chair recognizes Mr. Newhouse.

## FENTANYL: OPERATION BLUE LOTUS

Mr. NEWHOUSE. Very good. Thank you, Mr. Chairman.

Mr. Secretary, just had a couple more things I wanted to talk to you about.

You talked, as well, about fentanyl. I think I can safely say it is destroying our communities throughout the country.

Recently in my district in central Washington I held a roundtable. I had multiple law enforcement representatives, families that were personally impacted by losing children to fentanyl. I had judges represented, prosecutors represented, people that provide services to young people and to drug addicts. And let me tell you, I am sure you have heard, the stories are devastating and truly moving.

So it is not a stretch to say that this drug is destroying our communities. Last year 100,000 people died from drug overdoses, largely from fentanyl. That is more—you and I are both of the age we remember—that is more than all the casualties in the Vietnam war in one year. So it is a huge issue.

I wanted to ask about Operation Blue Lotus. It is a new program, barely a month old. It looks like it is promising. Are there other plans in the administration to address fentanyl? Are there other options?

I think is it Title 32 that provides for the National Guard Counterdrug Program to show a force at, I guess, between the ports of the entry, if that is where the issue is.

I think I can say, if this—if fentanyl was COVID, I dare say the administration would have closed down the country until we had a handle on it. It seems to me that we should be putting all our efforts into this, pulling out all the stops to stop this scourge in our country.

So could you elaborate on some of those questions?

Secretary MAYORKAS. Congressman, I stand with you 100 percent with respect to the scourge of fentanyl, the threat that it poses to our communities, which is why we are focused so intensely on it. I would be very proud to share with you details about Operation Blue Lotus that began last week.

I also, before that, want to assure you that this is not just a DHS effort, but it is an entire administration effort. We have a strategy. In fact, the Homeland Security Advisor of the President led a delegation, consisting of individuals, leaders from multiple departments and agencies, to Mexico to address the fentanyl challenge that we encounter in the United States.

I met with the law enforcement agencies in our Department to review our preexisting all-of-Department strategy against fentanyl.

I never, in my nearly 23 years of public service, have combated a drug as toxic and dangerous as fentanyl.

We decided that what we needed to do was, in addition to the resources that we already were bringing to bear at our ports of entry, which is where more than 90 percent of the fentanyl is brought into the United States, to surge even more resources.

Specifically, Homeland Security Investigations special agents not only display force, they do so much more, because they bring the interdiction capability and the investigative and prosecution capability.

They are at the ports of entry. When we interdict the fentanyl, they can commence an investigation immediately of the individuals apprehended and refer them for prosecution, as is most strategic to the Department of Justice.

It is an extraordinary effort. I believe that we seized 900 pounds of fentanyl in the very first week of Operation Blue Lotus.

We are not stopping at Operation Blue Lotus. I agree with you 100 percent. This caused the death of approximately 70 or more thousand Americans in 2022.

This is a problem that has been building for years. In, I think it was in 2020, during the last year of the Trump administration, it killed nearly 58,000 Americans.

This is not a challenge that is new. It is a challenge that has been increasing year over year. We have to address it. We indeed are bringing an all-of-administration fight to it.

Mr. NEWHOUSE. Is the National Guard Counterdrug Program being utilized?

Secretary MAYORKAS. I will have to get back to you on that specific aspect of it.

Mr. NEWHOUSE. Like I said, it seems like we should be pulling out all the stops here.

So thank you for that, and look forward to the progress in Operation Blue Lotus.

Thank you, Mr. Chairman.

Mr. JOYCE. Thank you, Mr. Newhouse. I think you would have unanimous support for declaring war on fentanyl, wherever it is coming from.

Mr. Trone is recognized.

#### FENTANYL: EFFORTS TO FIGHT

Mr. TRONE. Thank you, Mr. Chairman.

And I appreciate all the efforts of our Republican colleagues and the total unanimous support we do have to work together. This is so bipartisan.

You know, I lost a nephew. He died of a fentanyl overdose in 2016. And since 2014, this scourge has just replaced heroin. And at \$200 a kilo cost versus \$6,000 a kilo cost and 50 times more powerful, it is a losing battle.

And we must do a couple of things. But, most importantly, I was co-chairman with Tom Cotton on the synthetic opioids commission. We spent over a year on this issue with the RAND Corporation on a budget from the NDAA.

And we concluded at the end of the day that, quite frankly, we were not going to stop the precursors from China because China wasn't helping us. We were not going to stop the fentanyl coming across the border because Mexico was doing zero.

And Obrador had adopted, President Obrador has adopted a policy of "Hugs, Not Bullets." You are familiar with that. And he has made a decision not to take on the drug cartels at the top level, other than some few face-saving gestures periodically like before the last visit we had.

So without their cooperation, Senator Cotton and ourselves agreed that we had to focus on the demand side, because we can't win on the supply side without Mexico and China who has just totally turned us down.

And with the cartels controlling roughly 30 percent of the \$1.2 trillion of the GDP in Mexico, they are a force well to be reckoned with and they are armed to the teeth: 56,000 murders, less than 1 percent solved. It is a country that is wracked with murder and corruption at the highest levels throughout the entire country.

So what is going to change? How are we going to change the government to work on the supply side in Mexico when Obrador has just said forget it?

Do you see this new policy as a real chance that something can happen? Because having been there on the ground and met with all of their folks, I just don't see it.

Secretary MAYORKAS. Congressman Trone, let me at the very outset express my condolences for the loss of your nephew. I am very, very sorry to hear of that.

We have to address this on all fronts, both the supply side and the demand side, and indeed we are doing so.

You are correct that too much of the precursor chemicals and the manufacturing equipment are coming from China, and we have to stop that. We are working on that with our international partners, including with Mexico.



I do want to say that we, as a Department and as an administration, are cooperating with the country of Mexico in the fight against fentanyl. We are working with it to help it secure its seaport where the precursor chemicals and the equipment are coming from China.

We have transnational criminal investigative units. Our Homeland Security Investigations personnel are working with their counterparts in Mexico to interdict the flow of fentanyl, to interdict the proceeds from the trafficking of fentanyl. We are increasing our partnership with Mexico. That partnership has improved significantly since you perhaps last addressed it. We are very, very focused.

As I referenced a few minutes ago, the Homeland Security Advisor, Dr. Sherwood-Randall, and the Homeland Security Advisor of President Bush, led a delegation, including the Deputy Secretary of Homeland Security and the Deputy Attorney General of the United States, to Mexico to explore how we can partner more effectively. That delegation was very well received.

A high-level delegation from Mexico is coming to the United States, I believe, in mid-to-late April to advance that partnership further.

We cannot do it alone, and I think we have a cooperating partner, much more so than in the past, in Mexico right now.

Mr. TRONE. I am not going to hold my breath. The Mexican Government has a lot of reasons not to be invested in this, given the power of the cartels in the country and the lawlessness that how the whole country is run.

So good luck. Keep at it. But I think we got to focus on the demand side, because that is where we have a real chance to make a difference.

I yield back.

Mr. JOYCE. Thank you, Mr. Trone.

Mrs. Hinson is recognized.

#### BORDER SECURITY: CHINA

Mrs. HINSON. Thank you, Mr. Chairman.

Mr. Secretary, there have been some extremely concerning reports of increased numbers of Chinese nationals crossing at our southern border. Are you aware of those reports, and are you talking with CBP about them?

Secretary MAYORKAS. I am aware of those reports, Congresswoman. I am working with Customs and Border Protection and other parts of the Department of Homeland Security, and with other parts of the United States Government to address that. We are focused intensely on the security of the border in all respects.

Mrs. HINSON. Does anywhere in your requested budget note those reports or how you are going to specifically address the Chinese Communist Party as they work to exploit our open borders?

Secretary MAYORKAS. Congresswoman, our request for increased funding in support of border security efforts that we have underway, not just at our ports of entry, but in the detection, interdiction, and prevention of illegal entries in between our ports of entry, that request for increased funding gets to this challenge as well as

to the other aspects of the challenge of securing our southern border.

#### MIGRANT ENCOUNTERS: REMOVALS

Mrs. HINSON. I think one of the biggest concerns is a clear lack of communication between CBP and ICE, and this is something that has been ongoing for quite some time. It is apparent in this budget request. And, as said earlier, I think increasing numbers and throwing out catchy names looks nice, but I think there needs to be follow-through.

I mean, we are 2 years into a border crisis, and attempting to muddle through it without accountability or addressing these that these policies have caused, our border is not secure and the Chinese Communist Party is exploiting that.

180,000 fewer removals in 2022 under ICE than in 2017, more than 2.2 million more encounters in 2022 fiscal year than in 2017. I think Iowans and Americans deserve accountability here for their tax dollars and for their numbers. Do you agree with that?

Secretary MAYORKAS. Oh, absolutely. But your data is misleading, if I may respectfully—

Mrs. HINSON. If it is misleading, I am going by data that came directly from the Customs and Border Protection agents. In 2022 fiscal year, 2.76 million encounters; fiscal year 2017, 526,901. My public school math shows that is more than 2.2 million more encounters in that time.

So I have some other questions for you, Mr. Secretary. Are you aware of the number of Americans who have been killed or attacked by illegal immigrants since you took office?

Secretary MAYORKAS. Congresswoman Hinson, last year we removed and expelled approximately 1.4 million people. That is the greatest number—

Mrs. HINSON. But are you aware of the number of Americans who have been killed or attacked by illegal immigrants? It should be an absolute priority for you not only to know that number but to know names of these victims.

Are you aware of the number of CBP agents who have been attacked or assaulted in the line of duty at the southern border since you took office?

Secretary MAYORKAS. So, as I was answering your prior question, we removed and expelled approximately 1.4 million.

Mrs. HINSON. Sir, the number is 1,100 attacks on CBP agents at our southern border from 2021 to 2023.

Secretary MAYORKAS. That is precisely why we are prioritizing the prosecution under title 18, section 111, I believe it is.

Mrs. HINSON. Well, if you look at the number of fewer criminals that were actually deported, at the criminality data, if you look at fiscal year 2019, 247,000 removals. 56.86 were convicted criminals. Again, that number dropped to 67,000 removals. So when you look at the percentages there, clearly you are not prioritizing that, because the criminals speak for themselves.

If you are aware that there have been thousands of known criminals that have crossed our southern border. There have been over 1,000 CBP agents assaulted. Children are being forced into traf-

ficking, as many of my colleagues have said. There are migrants dying every week trying to cross our border.

If you are aware of all these failures and you have done nothing, what will it take for you to resign and step down from this job? Because I see this as a complete failure. What will it take?

Secretary MAYORKAS. Congresswoman, you are mistaken in your citation of statistics. You clearly do not understand the immigration system and how it interplays with the Public Health Order of Title 42 of the United States Code. So what I would—

Mrs. HINSON. Well, what I understand, Mr. Secretary, is that you are failing at doing your job. These numbers from Customs and Border Patrol speak for themselves. The American people understand that border security is national security, and this is a failure.

The policies of this administration have directly contributed to the numbers that I am citing right here, sir. And I am happy to share this document with you too if we need to reconcile our numbers. But, in my mind, it is very clear there has been a complete failure in you doing your job here and we need new leadership, as far as I am concerned.

I yield back, Mr. Chair.

Mr. JOYCE. Thank you, Mrs. Hinson.

Dr. Harris is recognized.

#### BORDER SECURITY: CARTELS

Mr. HARRIS. Thank you very much. And, you know, as the son of naturalized Americans, look, I believe in legal immigration, but not what is going on at our southern border now.

Let me just ask you, do you support naming the cartels foreign terrorist organizations?

Secretary MAYORKAS. Congressman—

Mr. HARRIS. It is a simple answer. It is yes or no. Do you support the bill in the Senate that labels them as foreign terrorist organizations? I have a limited amount of time. That is a very simple question. Do you support it or not?

Secretary MAYORKAS. Congressman, it is not a simple question.

Mr. HARRIS. OK, good. Let's go on to the next one, because you obviously have not made a decision on that. This is clear-cut. You would be much better off if you labeled them foreign terrorist organizations, your ability to control the border. But, as the gentlelady from Iowa suggested, you don't want to control the border. This President doesn't want to control the border.

Now, I am glad you visited the border a month ago. You have a border czar, don't you? Who is the border czar in the administration? Oh, you don't that answer? I will tell you. It is Vice President Harris. I know you want to delay as long as possible. It is Vice President Harris.

When was the last time she was at the border? Not within 100 miles on an energy project. At the border. When was the last time?

Secretary MAYORKAS. Congressman—

Mr. HARRIS. It was June 2021. I know you are delaying. It was June 2021. She has only been there one time 2 million crossings ago. Now, let me tell you something. If you have a problem somewhere and you are running an organization, you actually keep on visiting the border to figure out if you are solving the problem. Our

border czar should also resign, because she isn't doing her job either.

Finally, TSA has asked for billions of dollars in new money functionally by budget gimmicks that transfer money. You mentioned that airports are actually an economic tool in some States. What is the State's share of TSA protection at airports? How much do States contribute to those TSA lines at airports, percent?

Secretary MAYORKAS. Congressman, is this a question that you actually will allow me to answer?

Mr. HARRIS. I yield the rest of my time to Mr. Guest.

Mr. JOYCE. The chair recognizes Mr. Guest.

#### BORDER SECURITY: STATISTICS

Mr. GUEST. Thank you, Mr. Chairman.

Mr. Secretary, Chief Ortiz posted on Twitter on March 17, said the week in review: Seven agents assaulted; 34,800 apprehensions; 16,900 approximate got-aways; \$307,421 seized; 1,117 pounds of cocaine seized; 658 pounds of marijuana; 77 pounds of fentanyl; 69 pounds of meth; 21 firearms; 8 sex offenders; one gang member; one warrant; one assault with a deadly weapon.

The Chief then posted the stats from last week. This post was posted 4 days ago. This week in review: 8 agents assaulted; 33,000 apprehensions; 15,292 approximate got-aways; 239 pounds of meth; 50 pounds of cocaine; 106 pounds of fentanyl; 8 sex offenders; 14 firearms seized; \$129,318 seized; and 17 gang members apprehended.

The Chief then posted just 2 days ago, we are talking about what has happened just over the weekend: 1 agent assaulted; 14,200 apprehensions; 399 pounds of cocaine; 185 pounds of meth; 135 pounds of fentanyl; 55 pounds of marijuana; \$64,000 seized; one firearm; one stolen vehicle; one gang member; and two sex offenders.

Again, Mr. Secretary, it baffles me and others, when presented with evidence such as this from the Chief of the Border Patrol and the numbers that we have seen over the last 2 years, that this administration continues to maintain that the border is secure.

And I know that you and I will never agree on that. We will just have to agree to disagree. But I hope you understand the frustration that we, as Republicans, see when those statements are made to Congress that when we see what is happening on a weekly basis, those stats are startling.

And for this administration to come in before Congress and testify that the border is secure because we are doing a better job of detecting, I think that that is just an inaccurate, if not a false, misleading statement.

One of the things that Chief Ortiz said 2 weeks ago is he said that CBP, he said that under this administration has become the processing enterprise. To kind of expand out, he basically said that securing and apprehending the border came second and took a backseat to the fact that we are processing, and that we are processing and allowing illegals into the country in an expedited manner.

I see in your recent budget request, beginning on page 3 and continuing onto page 4, you state that: Fiscal year 2024 budget in-

cludes a Southwest Border Contingency Fund of up to \$4.7 billion, an emergency funding source to respond to immigrant surges along the border.

I have been to the soft-sided facilities. I was at the soft-sided facility in El Paso, a facility that is just basically a gigantic tent that is out in the middle of nowhere. And that facility, I was told that the cost of that facility on an annual basis is \$200 million, just for that facility. And again, that includes the staff that mans that, and I know that there is medical personnel and processing personnel and food personnel, all the things that go along with that.

But you equate that across the southern border. And I know that there are multiple processing centers. If there are just five soft-sided facilities, that is \$1 billion a year that we are spending just on processing alone.

I know that when these processing sectors become full, that we will often then fly immigrants to other sectors to have them processed. And I was told that that costs roughly \$90,000 per flight.

And so, I believe that Chief Ortiz is correct when he says that what has happened, or this administration is, instead of trying to secure and stop the flow of illegal immigrants coming across the border, we have just gotten better at processing those immigrants.

And that to me is extremely disturbing, disturbing that we are not doing any better job of preventing people—and we can talk about the conditions that exist in South America and some of these other countries and those push factors, but we also have to address the pull factors, which is that immigrants believe that once they step foot on the soil of the United States that they are going to be able to claim asylum—and that in most cases that is correct—and that, as we know and we talked about the broken immigration court, that they are going to be allowed to remain in the country for 7-plus years before their case is ultimately adjudicated. And so, those things are very disturbing to me.

#### BORDER SECURITY: TITLE 42

I do want to ask you a question, particularly as it relates to title 42. We know title 42 ends May 11. When title 42 was originally set to expire late last year, there were numbers by DHS that talked about that there was believed that there would be a surge of immigrants somewhere roughly 9- to 14,000. I have seen estimates as high as potentially 18,000, but let's just take 14,000. 14,000 immigrants a day over 30 days, that is 420,000 immigrants, a number that would dwarf our previous high of 300,000 that we saw in December.

Do you still anticipate—when Title 42 ends, are you still anticipating a surge? Are you preparing for the surge, and that once these immigrants come across the country that we are able to handle the volume that we will be seeing, assuming that these estimates that DHS prepared are accurate?

Secretary MAYORKAS. Congressman Guest, let me answer your question. Then I want to say, if I may, a few things in response to what you expressed before the question was posed.

Yes, we continue, of course, to prepare for the end of Title 42 on May 11. We began preparing in September of 2021. We published a six-pillar plan. We refreshed that six-pillar plan in April of 2022.

Let me assure you that we indeed are indeed, trying to prevent unlawful entries at our southern border. What we implemented on January 5 is a powerful example of how we are trying to prevent that, and doing so effectively while staying true to our asylum laws, the asylum laws that Congress has passed. That January 5 program, as I have testified previously, has proven extraordinarily successful, number one.

Number two, with respect to what you articulated. I do not understate the gravity of the challenge at the southern border. I want to assure you of that. Some of the data that you shared speaks of the gravity of the challenge accurately, correctly. It also speaks to the heroic work of our U.S. Border Patrol agents.

With respect to processing, case processing—and Chief Ortiz certainly will communicate this—we have been very, very focused on deploying personnel to do that processing, contract personnel, case processing personnel, to make sure that our Border Patrol agents are out in the field doing the law enforcement work that they are equipped to do.

We, in addition, fundamentally need to fix, as you and I agree, our broken immigration system.

#### BORDER SECURITY: DRUG TRAFFICKING

Mr. GUEST. Mr. Secretary, one last question.

And I know I am bleeding over into my time, Mr. Chairman. And then I will yield back and will not ask for any additional time.

Mr. JOYCE. We will just let it roll right into yours.

Mr. GUEST. Thank you.

Last question, as it relates to drug trafficking, what we are seeing across the border as a whole: Do you believe that one of the primary missions, if not the primary mission of DHS, should be to prevent the flow of illegal drugs—cocaine, methamphetamine, particularly fentanyl, heroin—from coming across the southern border?

Secretary MAYORKAS. Yes.

Mr. GUEST. So you do believe that, correct?

Secretary MAYORKAS. Yes, along with our federal partners and State and local partners. It is an all-in effort.

Mr. GUEST. And I know that—and you and I may disagree on those that come through ports of entry versus not. I believe that many of the estimates that I have seen from DHS believe that 90 percent of the illegal drugs flow into the country across ports of entry. Is that correct as well?

Secretary MAYORKAS. That is correct. When I cite that statistic, I am speaking specifically about fentanyl.

Mr. GUEST. Yes, sir. And so, then let me ask you: As I understand from looking at your budget request, there is, is it \$305 million for new technology?

Secretary MAYORKAS. Yes.

Mr. GUEST. And that would be including scanners and things along the border, maybe canine officers, things to be able to better detect, better screen traffic that is coming across the United States?

Secretary MAYORKAS. That is in addition to, for example, canine officers. That is with respect to our technologies such as nonintrusive inspection technology, which is so effective.

Mr. GUEST. And so I guess my concern, if that should be—and I believe that it should be one of the primary missions, if not the primary mission, of DHS to prevent the flow of illegal drugs coming into the border, your budget has requested \$4.7 billion for emergency funding to respond to the immigrant surge, but only \$305 million to upgrade the necessary technology to control our ports of entry. Because ports of entry, they also fall under DHS. Every vehicle, every individual that comes across there, we have the potential to screen those individuals, but it would seem to me that our priorities are misaligned.

If we are spending \$4.7 billion for processing and we are only spending \$300 million for new technology, technology that could keep drugs out of our community, technology that could keep young people from ingesting fentanyl and help stop this drug crisis, I will just tell you that, as a prosecutor, that I believe those priorities are misaligned.

And so do you believe that we should be spending more than the \$305 million that is in the budget? And I understand that as the budget that came from your Department, but do you believe that that is an adequate amount, particularly comparing that to the \$4.7 billion that you have requested to respond to the surge?

And I will allow him to answer and then I yield back. Thank you, Mr. Chairman.

Secretary MAYORKAS. Congressman, I would welcome the opportunity to share with you all of the money that we are spending to interdict and to prevent drugs from entering our country through the because the \$305 million is with respect to technology. That is not our only investment. We also are investing in personnel. We also are investing through the infrastructure legislation that passed, a monumental achievement. We also are investing in modernizing our POEs so that we can maximize the impact of the devotion of personnel, of the implementation of new technologies.

So I would welcome the opportunity to speak with you, because the \$305 million is, by no means, the only investment in the effort that you and I agree needs to be a high priority.

Mr. JOYCE. Thank you, Mr. Guest.

For the get-back questions that were asked today members of the subcommittee had, I would ask you to respond within 15 business days. And any of the members who have additional questions that they want to put in writing, I would ask you to also respond to those within 15 business days of your receipt.

I would like to thank you again for being here, Mr. Secretary.

And, with that, the subcommittee stands adjourned.

[Answers to submitted questions follow:]

**QUESTIONS FOR THE RECORD**  
SUBCOMMITTEE HOMELAND SECURITY  
U.S. HOUSE COMMITTEE ON APPROPRIATIONS

---

**Budget Hearing – Department of Homeland Security**  
**Wednesday, March 29, 2023**

---

**Representative Hinson**

**1. Procurement of Technology**

To: Secretary Mayorkas

For the last two years, this Committee has provided, with strong bipartisan support, significant additional resources for force multiplying border technology for use between the ports of entry. We've also heard directly from the Border Patrol Sector Chiefs and agents about the value of these technologies, like Tactical Awareness Kits for every USBP agent and the Autonomous Surveillance Tower Program of Record. However, your FY 24 budget fails to provide approximately \$95M to sustain critical border security technology operations, including Tactical Awareness Kits (TAK), Border Towers, and counter UAS platforms.

**Question 1:** How do you envision border operations will be affected in FY24 because the Department's budget request does not support the technology investments this Committee provided CBP? Please provide an update on how each of the USBP border security technology programs will be impacted by the proposed FY24 funding levels. In your response, please include funding and operations impact data for each border security technology program by sector.

**Response:** The change in the FY 2024 President's Budget does not reflect a change in U.S. Customs and Border Protection's (CBP) focus on leveraging new and emerging technology. CBP will continue to field new systems, working to obtain operational advantage and expand persistent surveillance capabilities. Procurement processes continue utilizing previously appropriated funds and the agency will continue to leverage its authorities and available funds to increase the use of technology in our border security mission.

CBP made strategic decisions to include any reductions across the budget. CBP has identified high priority areas and will prioritize resources to the most critical areas. Please



see enclosure for current and planned technology program by sector. This enclosure is Law Enforcement Sensitive, and will therefore be transmitted separate from the public record.

Question 2: How has feedback from the sectors about the value of autonomy shaped future procurements of between the ports technology, both with the resources Congress has provided as well as future technology procurements?

**Response:** CBP envisions that all future domain awareness technology will incorporate an autonomous backbone. Current surveillance systems will be enhanced to incorporate autonomy and all future deployments will require autonomy as a key functional requirement. Autonomous systems are capable of consistently executing redundant tasks such as persistent surveillance, which allows for the agent operator to be reallocated to the field. These autonomous features increase situational awareness and achieve greater consistency in meeting our key performance parameters across systems and operational domains.

To achieve increasing levels of autonomy throughout all surveillance and intelligence systems, USBP will leverage current and future advances in Artificial Intelligence (AI), machine learning, and commercial sensors designed for an ever-evolving, autonomous world. USBP has deployed 216 Autonomous Surveillance Towers (AST) as of the end of the second quarter of Fiscal Year (FY) 2023. A total of 333 AST's will be deployed with the funding received to date. In addition, USBP is conducting a pilot for the USBP Common Operational Picture (COP) which will inform the development of functional requirements for the COP acquisition program. Funding received in FY 2023 will be used to develop and deploy COP to Douglas Arizona, establishing Initial Operational Capability (IOC). This will include creating a common user interface using WebTAK, creating a unified targeting queue that integrates detections from Integrated Fixed Towers (IFT), Remote Video Surveillance Systems (RVSS), ASTs, imaging sensors, and Linear Ground Detection Systems (LGDS), as well as building out cloud infrastructure and applications, and continuing to work with USBP Agents and human factors experts to design and build workflows.

Regarding feedback from the sectors about the value of autonomy shaping future procurements, USBP utilizes their Capability Gap Analysis Process (CGAP) to capture, develop and analyze operational gaps for current and future procurements. The process has resulted in the identification of autonomous requirements that mitigate USBP gaps derived from analysis conducted, examples of such procurements are AST towers, USBP COP, and the Mobile Video Surveillance Systems – Radar (MVSS-R).

Additionally, all southern border sectors and stations have completed technology laydown exercises to support their respective plans for achieving operational advantage of the border. The effort was facilitated by USBP Operational Requirements Management Division (ORMD) and included the participation of Sector and Station leadership, key planners and USBP Program Management Office Directorate (PMOD) technology Program Managers. This effort provides a mechanism for developing notional solution and laydowns that are informed by both operational and programmatic expertise.

The notional exercise informs resource allocation planning (i.e., funding) and provides a starting point for more comprehensive pre-deployment planning by PMOD. During the exercise, field commanders identify those capabilities required to gain operational advantage within their respective AORs. As a result of the notional operations laydown exercise, key takeaways regarding the requirement for autonomous technology include the following:

- Field commanders identified autonomous surveillance solutions as a preference to traditional alternatives based on their improved force multiplying value.
  - Autonomy allows agents to be more effective at maintaining awareness of border activity while conducting multiple mission essential tasks.
  - Autonomous surveillance technology enable sectors that have limited command and control infrastructure the ability to effectively deploy and use persistent surveillance assets
- Every USBP sector along the southern, northern and coastal border environments identified ASTs as a solution to meeting persistent surveillance requirements.
- Collected solutions sets are notional in that they are not currently funded and remain subject to refinement by PMOD pre-deployment planning teams.
- Laydowns were built around current or currently expected operational conditions and are subject to change as needed.
- Solution sets were built out to reflect holistic technology requirements and associated laydowns.
- Proposed solutions and laydowns emphasize the containment of illicit activity and compression of operations toward the immediate border to the extent possible.

USBP and the CBP Innovation Team strive to identify, adapt, and deliver industry advances with autonomous functionality, and will continue to be a priority based on frontline personnel input upon utilizing these operational capabilities. Feedback on these early autonomous systems indicates enhanced situational awareness, accuracy of detections, and overall improvement in operational efficiencies and coverage.

## **2. DHS Enforcement of CFATS**

To: Secretary Mayorkas

I have concerns about DHS' enforcement of the Chemical Facilities Anti-Terrorism Standards (CFATS) program, as it relates to reportable chemicals contained in gasoline mixtures. Although the due date for submitting the Top Screen under CFATS for facilities with COI present in gasoline mixtures is indefinitely extended, DHS never issued a final regulation amending the CFR and thereby formally removing this reporting and compliance liability from liquid terminal companies who store and transport gasoline. This reporting obligation rests solely at the whimsical discretion of DHS that would potentially impact hundreds of liquid terminal sites across the country. Many of these liquid terminal companies are small businesses with fewer than 250 employees and must account for the expense of this regulatory reporting requirement.

Question: Do you support issuing a final regulation to give full effect to the July 20, 2016, Federal Register publication to clarify and remove the regulatory burden on liquid terminals storing COIs in gasoline mixtures?

**Response:** The Department is aware of the view that gasoline mixtures should not be regulated under the Chemical Facility Anti-Terrorism Standards (CFATS) and received extensive comments on this issue in 2015 when we last asked for public comment on Appendix A, our list of chemicals of interest, in 80 FR 82504.

The July 20, 2016 publication in the Federal Register, in relevant part, reiterated the Department's practice of indefinitely extending the due dates for submission of Top-Screens, and as applicable SVAs and SSPs, for chemical facilities of interest whose only reportable COI is present in a gasoline mixture. It was not a rulemaking action that could result in a Final Rule under the laws and statutes that govern agency rulemaking.

Modifications to the CFATS regulations and Appendix A as proposed in your comment are made by the Department through rulemaking. In the Fall 2022 Unified Agenda, DHS published its intent to issue a Notice of Proposed Rulemaking (NPRM) covering these issues. In the fifteen years since the Department issued the CFATS regulations and Appendix A, DHS has gained extensive experience in analyzing chemical holdings and determining which facilities should be classified as high-risk and subject to future regulation. Given its experience, the Cybersecurity and Infrastructure Security Agency (CISA), which administers CFATS, has determined that it should adjust its list of regulated chemicals, threshold quantities, and counting methods to better reflect the security issues implicated by these chemicals.

**QUESTIONS FOR THE RECORD**  
SUBCOMMITTEE HOMELAND SECURITY  
U.S. HOUSE COMMITTEE ON APPROPRIATIONS

---

**Budget Hearing – Department of Homeland Security**  
**Wednesday, March 29, 2023**

---

**Representative (Case)**

**1. STOP ACT Implementation**

To: Secretary Mayorkas

The Safeguard Tribal Objects of Patrimony (or STOP) Act of 2021 (P.L. 117-258) was signed into law in December. It is designed to prevent the international trafficking of Indigenous people's sacred items. It requires the Departments of the Interior, Justice, State and Homeland Security to undertake important and immediate implementation actions. The Department of Homeland Security is specifically required to provide training to U.S. Customs and Border Protection personnel, participate in the STOP Act's interagency working group and detain items prohibited from being exported or that lack an export certification.

To help Congress better understand any challenges the Department of Homeland Security may be encountering while implementing this law, will you please answer the following questions:

Question:

1. How is the Department of Homeland Security implementing the STOP Act?

**RESPONSE:** CBP Office of Field Operations (OFO) is committed to ensuring the STOP Act is enforced and that those who would try to evade the law are identified. OFO utilizes its layered enforcement approach to prevent the international trafficking of Indigenous people's sacred items. CBP's layered enforcement strategy includes working with carriers and government partners overseas, implementing security measures across the global supply chain and leveraging risk-based targeting and intelligence driven strategies on imports.

2. Does the Department of Homeland Security have a process for verifying the provenance of cultural items detailed in export certifications? If so, what is that process?

**RESPONSE:** CBP Office of Field Operations (OFO) does have a process for verifying the origin of cultural items. CBP officers will initially detain the artifacts and objects until a subject matter expert (SME) is identified and makes further determinations as to the authenticity, age, characteristics, and possible protection of the artifacts or objects. OFO works with U.S. Immigration and Customs Enforcement (ICE)/Homeland Security Investigations (HSI) Special Agents (SAs) in all cases where an artifact or object has been detained for further HSI investigation. If the goods are genuine and export is not legitimate, OFO may seize the goods and work with our partner government agencies towards repatriation of the cultural item.

3. What budgetary resources do you anticipate are needed to carry out the Department of Homeland Security's responsibilities under the STOP Act?

**RESPONSE:** CBP Office of Field Operations (OFO) anticipates the need for additional infrastructure, staffing, and equipment to expand outbound mail exams and processing. The addition of non-intrusive scanning equipment would assist in detection of cultural and other outbound restricted items. Staffing at ports for outbound teams is limited, which inhibits their ability to increase operations into other areas.

The FY 2024 President's Budget Request to Congress includes \$305.4 million to identify, procure, and deploy enhanced inspection capabilities in the land and mail environments.

The \$305.4 million will provide enough funding to hit targets for deploying and increasing scanning, assuming all funds planned for civil works are executed towards commercial cargo trucks and passenger occupied vehicles.



## WITNESSES

---

	Page
Easterly, Hon. Jen, Director, Cybersecurity and Infrastructure Agency .....	1
Prepared statement .....	4
Answers to submitted questions .....	42
Mayorkas, Hon. Alejandro, Secretary, Department of Homeland Security .....	95
Prepared statement .....	97
Answers to submitted questions .....	146
Pekoske, Hon. David, Administrator, Transportation Security Administration .....	49
Prepared statement .....	51