AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CRACKING DOWN ON RANSOMWARE: STRATEGIES FOR DISRUPTING CRIMINAL HACKERS AND BUILDING RESILIENCE AGAINST CYBER THREATS

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 16, 2021

Serial No. 117–52

Printed for the use of the Committee on Oversight and Reform

Available on: *govinfo.gov*, *oversight.house.gov* or *docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

46–259 PDF WASHINGTON : 2021

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CORI BUSH, Missouri
DANNY K. DAVIS, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
PETER WELCH, Vermont
HENRY C. "HANK" JOHNSON, JR., Georgia
JOHN P. SARBANES, Maryland
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
MARK DESAULNIER, California
JIMMY GOMEZ, California
AYANNA PRESSLEY, Massachusetts
MIKE QUIGLEY, Illinois

JAMES COMER, Kentucky, *Ranking Minority Member*
JIM JORDAN, Ohio
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
PETE SESSIONS, Texas
FRED KELLER, Pennsylvania
ANDY BIGGS, Arizona
ANDREW CLYDE, Georgia
NANCY MACE, South Carolina
SCOTT FRANKLIN, Florida
JAKE LATURNER, Kansas
PAT FALLON, Texas
YVETTE HERRELL, New Mexico
BYRON DONALDS, Florida

RUSS ANELLO, *Staff Director*
PETER KENNY, *Team Lead*
ELISA LANIER, *Chief Clerk and Director of Operations*
CONTACT NUMBER: 202-225-5051

MARK MARIN, *Minority Staff Director*

C O N T E N T S

	Page
Hearing held on November 16, 2021	1

WITNESSES

The Honorable Chris Inglis, National Cyber Director, Executive Office of the President	
Oral Statement	7
Mr. Brandon Wales, Executive Director, Cybersecurity and Infrastructure Security Agency	
Oral Statement	9
Mr. Bryan Vorndran, Assistant Director, Cyber Division, Federal Bureau of Investigation	
Oral Statement	11

Opening statements and the prepared statements for the witnesses are available in the U.S. House of Representatives Repository at: docs.house.gov.

INDEX OF DOCUMENTS

The documents entered into the record for this hearing are listed below.

* "Biden tells Putin certain cyberattacks should be 'off-limits'," article, Reuters; submitted by Rep. Cloud.

* "Garland Refuses to Rescind Memo Asking FBI to Probe School Board Threats," article, U.S. News and World Report; submitted by Rep. Cloud.

The documents are available at: docs.house.gov.

CRACKING DOWN ON RANSOMWARE: STRATEGIES FOR DISRUPTING CRIMINAL HACKERS AND BUILDING RESILIENCE AGAINST CYBER THREATS

Tuesday, November 16, 2021

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND REFORM,
Washington, D.C.

The committee met, pursuant to notice, at 10:06 a.m., in room 2154, Rayburn House Office Building, and via Zoom. Hon. Carolyn B. Maloney [chairwoman of the committee] presiding.

Present: Representatives Maloney, Norton, Lynch, Connolly, Krishnamoorthi, Raskin, Khanna, Mfume, Ocasio-Cortez, Tlaib, Porter, Davis, Wasserman Schultz, Welch, Johnson, Speier, Kelly, DeSaulnier, Comer, Foxx, Hice, Grothman, Cloud, Norman, Sessions, Keller, Biggs, Clyde, Franklin, and Herrell.

Chairwoman MALONEY. Welcome, everyone. Welcome to today's hearing.

Pursuant to House rules, some members will appear in person, and others will appear remotely via Zoom. For members appearing remotely, I know you are all familiar with Zoom by now, but let me remind everyone of a few points.

First, the House rules require that we see you. So please have your cameras on at all times.

Second, members appearing remotely who are not recognized should remain muted to minimize background noise.

Third, I will recognize members verbally, but members retain the right to seek recognition verbally. In regular order, members will be recognized in seniority for questions.

Last, if you want to be recognized outside of regular order, you may identify that in several ways. You may use the chat function to send a request, you may send an email to the majority staff, or you may unmute your mic to seek recognition.

We will begin the hearing in just a few moments when they tell me they are ready to begin the livestream.

Let me say that this is a bipartisan issue. Everyone in the country is deeply concerned about cybersecurity, and I hope that we will be able to work with ways to strengthen protections for American business and government.

Are we ready to go? OK.

The meeting will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

I now recognize myself for an opening statement.

This has been an unprecedented year for cyber-attacks. The country is still reeling from last year's cyber-attack against the company SolarWinds that was linked to Russia and infected numerous Federal agencies. These attacks have been described as a wake-up call for America. It attacked all through the Federal Government and numerous private sectors also.

Just this weekend, it was reported that the FBI, our premier law enforcement agency for investigating cyber-crimes, was itself the victim of a hack that allowed emails to be sent from FBI email servers disguised as genuine FBI emails. In short, we are at a tipping point, as cyber-attacks have become more common and potentially more damaging.

Several recent attacks have used a type of malicious software known as ransomware, which encrypts a victim's system and demands a payment in exchange for restoring access or refraining from publishing stolen data. This is especially dangerous because it can shut down an entire system and can cause chaos in a community, an industry, or even an entire country.

And cybercriminals are now demanding, and receiving, more money than ever. In March, CNA Financial, an insurance company, reportedly paid the largest known ransom payment ever, a staggering $40 million.

In May, ransomware criminals from Eastern Europe attacked the company Colonial Pipeline, resulting in the shutdown of more than 5,500 miles of gasoline pipeline spanning from Texas to New Jersey and causing temporary gas shortages up and down the East Coast. The cost to unlock the system was $4.4 million.

Also, in May, JBS Foods, one of the largest meat suppliers in the United States, shut down its plants when it suffered a ransom attack. The cost to unlock their system was $11 million.

In June, this committee launched an investigation out of concern that these multimillion-dollar ransom payments would equip cyber criminals with even more financial resources and encourage future attacks. Today, the committee issued a staff memo with some of the committee's preliminary findings.

We found that these attacks often stemmed from minor security lapses, even at companies with seemingly robust cybersecurity. Our report also highlights the importance of clearly established Federal points of contact for companies to avoid wasting precious time when an attack is underway. Finally, we found that companies faced substantial pressure to pay these ransoms quickly, making it harder to stop these attacks.

And it is not just large companies that are targeted. Ransomware also harms small businesses, hospitals, schools, and local governments. Since taking office, the Biden administration has been countering ransom, and they are really focusing on ransomware as a top priority. This included bringing together 30 nations for a White House summit last month to discuss strategies to combat the threat. It also means taking a tougher line on countries, including Russia, that harbor cyber criminals.

The Biden administration has also dedicated significant law enforcement resources to take ransomware networks offline and bring criminals to justice. Just last week, the Department of Justice announced criminal charges against two foreign nationals connected to the prolific ransomware criminal group, REvil. DOJ also recovered more than $6 million in ransom money paid.

This is a good start, but we cannot afford to let up on our efforts. Congress must ensure coordination of anti-ransomware efforts across the entire Federal Government and between the public and private sectors. Last Congress, this committee held a hearing on the need to establish a position at the White House to lead the Federal Government's response to cyber threats. I was proud that President Biden nominated Chris Inglis to serve as the first National Cyber Director this year and that he is testifying before us today.

I also am pleased that the Infrastructure Investment and Jobs Act, which President Biden signed just yesterday, included $21 million in funding for the Office of the National Cyber Director. This law, which House Democrats passed over the objections of most House Republicans, will also provide $1 billion to help state and local governments shore up their cybersecurity so we can prevent ransomware attacks and $100 million to help critical infrastructure respond to significant cyber incidents. And the Build Back Better Act will provide new resources to CISA to help enhance cybersecurity in both the public and private sectors.

Ransomware attacks are a grave national security challenge. Today, we will hear from our witnesses about the "whole of government" effort needed to disrupt ransomware networks and how we can help businesses, state and local governments, and others to prevent, prepare for, and respond to attacks.

I now recognize the distinguished ranking member, Mr. Comer, for an opening statement.

Mr. COMER. Thank you, Madam Chair.

This year, we have seen an uptick in major ransomware attacks that have the ability to wreak havoc upon Americans' everyday lives. In March, CNA Financial, one of the largest commercial insurers in the U.S., was subject to a ransomware attack and paid $40 million to unlock its network. In May, Colonial Pipeline, one of the largest pipelines in the eastern U.S., paid $4.4 million in cryptocurrency to retrieve its data following a ransomware attack. In June, JBS USA, one of the country's largest meat packers, paid a ransom of $11 million to hackers.

These companies made these decisions to pay the ransoms because they did not want to disrupt their supply chain. The FBI's official policy is not to advise companies whether or not to pay these ransoms. During our many briefings with these companies, this is indeed the FBI's position they took during the negotiations with the ransomware attackers.

Even the FBI, the top law enforcement agency tasked with fighting cybercrime, is not immune from cyber-attacks. Over the weekend, hackers accessed the FBI's external email system and spammed potentially thousands of people and companies by issuing a fake warning of a cyber-attack. Hackers' ability to penetrate the FBI systems could create catastrophic consequences and chaos. We

need to hear from the FBI today on their efforts to disrupt and protect Americans from these cyber-attacks.

I am pleased that we have one witness here today who is Senate confirmed to discuss how we can disrupt cyber threats to better protect Americans from the devastating consequences of successful ransomware attacks. Unfortunately, this is only the second Senate-confirmed witness this committee has had this entire year. That is far below what is normal for this committee.

Unfortunately, the Oversight Committee, under Democrat leadership, refuses to call witnesses from the Biden administration and hold them accountable for waste, fraud, abuse, and mismanagement occurring on their watch. Today is the committee's first hearing since the citizens in Virginia sent a very loud message to the Biden administration, and that message to President Biden, "no more." The American people oppose the Biden administration's radical leftwing policies and are already seeking change.

President Biden and congressional Democrats' action to spend trillions of the taxpayers' hard-earned dollars on a socialist agenda has backfired. President Biden is now more unpopular with the American public than nearly any other President at this point in history.

Not only that, but over two-thirds of Americans think this country, under President Biden's leadership, is headed in the wrong direction. People are appropriately comparing President Biden to President Jimmy Carter.

President Biden's policies and decisions have created numerous crises that impact Americans' daily lives. Gas is now 61 percent higher than this time last year. Inflation is at a 30-year high, causing families to struggle with how to pay for meat, milk, eggs, and other basic necessities.

This year, Thanksgiving is set to be the most expensive Thanksgiving ever. The price of a 16-pound turkey is up 18 percent. There is chaos at our ports, with ships lining up, but nowhere to deliver the goods. And to add insult to injury, certain networks are criticizing truck drivers, the essential workers who have been shipping goods throughout the pandemic.

A record number of illegal immigrants were apprehended at our Southern border this year, and the surge continues because of this administration's pro illegal amnesty agenda. This, not to mention the drugs flowing across the border. The Biden administration has directed law enforcement to go after parents they deem domestic terrorists, but these parents are only concerned about radical curriculum being taught to our children.

At the same time, the Biden administration turned a blind eye to real terrorists in Afghanistan who seek to harm women, children, and U.S. troops. The Biden administration's disastrous withdrawal from Afghanistan has left a national security and humanitarian crisis in its wake. And sadly, this committee is ignoring it all.

Committee Republicans have written to the chairwoman over 20 times requesting hearings, investigations, and briefings on many of these topics and more. These issues are core to our committee's mission of rooting out waste, fraud, abuse, and mismanagement in

the Federal Government. But unfortunately, Chairwoman Maloney has ignored our requests.

We are the people's house. We must be responsive to the needs and demands of American citizens, but this committee, under Democrat leadership, refuses to do its job. It is no wonder this committee has received an F grade for how it has conducted oversight from a nonprofit organization.

It is past time for this committee to get back to its mission and conduct oversight on the many issues facing Americans today. The American people demand it, and they deserve nothing less.

Madam Chair, I yield back.

Chairwoman MALONEY. The gentleman yields back. But before I recognize Mr. Connolly for opening remarks, I would like to take a few moments to address some of his concerns.

The Biden administration has created over 5.9 million new jobs in the first nine months of President Biden's administration. This is a record for any new President. We created 531,000 new jobs just last month. And with the passage of the Infrastructure Investment and Jobs Act, which the President signed into law, a bipartisan bill, it is going to create even more jobs and help grow the economy.

Our unemployment is under 4.6 percent. And if the Republicans could see some of the very good things that the Biden administration is doing instead of just spending their time attacking them, we are working this week on the Build Back Better Act, which would further strengthen our economy by making historic investments in our infrastructure and people.

We did respond to your request for a classified briefing on Afghanistan. We have government officials before you today.

And with that, I yield to Mr. Connolly.

Mr. CONNOLLY. I thank the distinguished chair for holding this hearing, and let me join her in regretting the fact that the ranking member has chosen to use this hearing for propaganda rather than an in-depth examination of ransomware and its impacts on the U.S. economy and U.S. businesses and U.S. governments.

I find the word "chutzpah" is appropriate at this moment, given the fact that our Republican friends for four long years resisted any meaningful oversight of the Trump years, including, you know, serious legal issues from security clearances to the trampling of democratic norms——

Mr. COMER. Would the gentleman yield to a question?

Mr. CONNOLLY. If the chair will allow me extra time to do so?

Chairwoman MALONEY. Sure. Without objection.

Mr. CONNOLLY. I thank the chair. Yes, sir.

Mr. COMER. Would the gentleman, in his criticism of the—our criticism for not doing enough oversight, do you, Mr. Connolly, generally believe that this committee has provided any oversight?

Chairwoman MALONEY. Reclaiming, reclaiming my time. Let us get back to the purpose of the hearing. Let us not engage with their propaganda.

Let us get back. We have three important witnesses. Let us hear what they have to say. That is why we are here. I would like to hear what they have to say.

Mr. COMER. And again, Madam Chair, with all due respect, this is the Oversight Committee.

[Gavel sounding.]

Chairwoman MALONEY. The gentleman is not in order. Mr. Connolly has the time. He has worked hard on this issue, and he is absolutely right that we should focus on the purpose of this hearing.

Mr. CONNOLLY. I thank the chair.

The ramifications of ransomware permeate our economy, public health infrastructure, and national security. In recent years, ransomware has grown into a multibillion-dollar criminal industry. In 2020, more than 2,300 U.S.-based entities were affected by ransomware attacks, inflicting hundreds of billions of dollars in economic damage.

At least 113 of these ransomware attacks targeted government entities, costing an estimated $915 million. One of those attacks happened in my own congressional district. In September of last year, hackers launched into the Nation's 10th largest school district in Fairfax County, and the Fairfax County Public Schools computer system was attacked by ransomware after obtaining sensitive personal information about students and employees. That is just one example at the local level.

The coronavirus pandemic abruptly revealed how ill-prepared many of our state and local governments were in delivering vital public services securely and remotely. Criminals took advantage of overwhelmed public IT systems, generating a significant uptick in cybercrime.

In June of this year, our subcommittee held a hearing on the outdated IT infrastructure and rising cyber-attacks on state and local governments. The hearing examined the role of Congress and the Federal Government in accelerating IT modernization initiatives for states and localities so that eligible individuals and not cyber criminals could gain access to vital government services.

In response to the hearing, I introduced the House companion to the Senate's State and Local Digital Service Act. This important piece of legislation provides guidance and funding to state and local governments to form digital service teams focused on delivering fair, effective, and secure public services.

The bipartisan infrastructure bill, as the chair has noted, which President Biden signed into law yesterday, provides more than $1 billion of vital investments that will assist both private and public entities affected by major cyber events. These investments will save taxpayer dollars in the long term by reducing the vulnerability of state and localities to cybercrime, including ransomware attacks.

While these are important first steps in ensuring the Federal Government mitigates cyber-attacks, more must be done. I look forward to hearing from our witnesses today about the steps the Biden administration has taken to combat ransomware attacks and the ways Congress can ensure the United States implements a whole of government response to all cyber-attacks moving forward.

I thank the chair.

Chairwoman MALONEY. The gentleman yields back, and I would now like to introduce our witnesses.

Our first witness today is the Honorable Chris Inglis, who is the first National Cyber Director in the White House. I am proud of the role that this Congress and this committee played in creating the position along with Congressman Langevin. And we look very much forward to your testimony. Congratulations on your appointment.

Then we will hear from Brandon Wales, who is the Executive Director of the Cybersecurity and Infrastructure Security Agency. Originally, we had planned to hear from the Director of CISA, Jen Easterly. She was scheduled to testify. Unfortunately, she had a family medical emergency and was not able to be with us today. So, we are deeply grateful to Mr. Wales for appearing on extremely short notice to testify today. Thank you so much.

Finally, we will hear from Mr. Bryan Vorndran, who is the Assistant Director of the Cyber Division of the Federal Bureau of Investigation.

The witnesses will be unmuted so we can swear them in. Please raise your right hand.

Do you swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[Response.]

Chairwoman MALONEY. Let the record show that the witnesses answered in the affirmative.

Thank you. And without objection, your written statements will be made part of the record.

With that, Director Inglis, you are now recognized for your testimony.

STATEMENT OF CHRIS INGLIS, NATIONAL CYBER DIRECTOR, EXECUTIVE OFFICE OF THE PRESIDENT

Mr. INGLIS. Thank you.

Chairman Maloney, Ranking Member Comer, distinguished members of the committee, and dedicated staff, thank you for the honor to appear before you today alongside Deputy Director Wales from the Cybersecurity and Infrastructure Security Agency and Assistant Director Vorndran from the Federal Bureau of Investigation.

CISA's role as the operational coordinator for Federal cybersecurity and support to our Nation's critical infrastructure, combined with FBI's deep expertise and its essential role in victim assistance, investigation, attribution, and threat disruption, comprises a breadth of experience, authority, and resource that does make a critical difference for the American people. Cyber is a team sport, and I couldn't ask for better teammates.

I am eager to appear before you today and update you on the Biden-Harris administration's continuing actions to counter ransomware and to improve our national cybersecurity, including recent actions to prevent, deter, and mitigate ransomware attacks against public and private sector networks, as well as efforts to bring ransomware actors to justice.

Before turning to ransomware, allow me to say a few words about the office I have the privilege to lead. The role of the National Cyber Director was established by the Congress in January

of this year, instantiated by my nomination, confirmation, and entry on duty in July. I am grateful for the confidence that the President and Congress have placed in this role and for the essential investments in cybersecurity that you included in the recently enacted Infrastructure Investment and Jobs Act.

On October 28, I released the National Cyber Director's Strategic Intent Statement, which outlines the initial scope of work I expect the office to undertake. At the same time, I announced the designation of Chris DeRusha as Deputy National Cyber Director for Federal Cybersecurity, a dual-hatted title he will hold along with his current role as the Federal Chief Information Security Officer, to create unity of effort and purpose in our shared mission to ensure the security of Federal systems.

Both of these announcements lay the groundwork for a National Cyber Director team that continues to increase its contributions to the Nation's overall cybersecurity posture. Four key outcomes will serve as benchmarks to gauge the success of the Office of the National Cyber Director.

First, to drive coherence across the Federal enterprise, both in how it builds and operates its own digital infrastructure and in how it supports the defense of critical infrastructure owned and operated by the private sector.

Second, to continue to strengthen and improve private-public collaboration in cybersecurity.

Third, to work closely with the Office of Management and Budget to ensure that the U.S. Government aligns its cyber resources to its priorities to include advising departments, agencies, and the Congress on recommended changes.

And finally, to increase present and future resilience of technology, people, and doctrine within the Federal Government and across the American digital ecosystem.

As this committee well knows, ransomware attacks leverage systemic weakness in the cyber ecosystem. Cyberspace allows connectivity and efficiency of scale unrivaled in any other domain, meaning that by employing cyberspace, our geopolitical competitors can achieve global reach and strategic effect, while criminals and malicious actors can wield an unprecedented level of influence, impact, and coercion.

These attacks are costly and pernicious, and they undermine both critical functions and the confidence we must have in digital connectivity that underpins the modern economy. Accordingly, crafting a strategy to stop the scourge of ransomware has been a priority for this administration. That strategy begins with understanding what makes ransomware so effective.

Ransomware actors are able to purchase their tools on the black market and mount their attacks from leased and disposable cloud-based virtual infrastructure, which once exposed can be torn down and quickly rebuilt. The systems that these criminals target are far too often left vulnerable by failures to patch, to properly secure data, to create reliable backups, or to ensure that frontline employees of targeted organizations exercise basic cybersecurity practices.

Inconsistent application of anti-money laundering controls to virtual currencies permits criminals to leverage permissive jurisdictions to acquire and launder the proceeds of their crime. And fi-

nally, ransomware criminals are often able to operate with impunity in nation-states where they reside, facing no meaningful accountability for their actions.

The administration's counter-ransomware efforts therefore include action on four broad fronts. First, disruption of ransomware infrastructure and actors. Second, bolstering resilience to withstand ransomware attacks. Third, address the abuse of virtual currency to launder ransom payments. And finally, leveraging international collaboration to disrupt the ransomware ecosystem and address safe havens for ransomware criminals.

Consistent with and supportive of this strategy, the Biden administration supports legislative efforts to require cyber incident reporting to include ransomware payments to both the FBI and CISA that will help prioritize the use of precious resources to support victims, disrupt threat actors, and to guide future investments to improve resilience. These are daunting undertakings, and overcoming them will require a digital ecosystem that is resilient by design, a policy and commercial environment that aligns actions to consequences, and ensuring that public and private sectors are postured to proactively and decisively collaborate.

Thank you for the opportunity to testify before you today. I look forward to your questions.

Chairwoman MALONEY. Thank you for your testimony.

Mr. Wales, you are now recognized.

STATEMENT OF BRANDON WALES, EXECUTIVE DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Mr. WALES. Chairwoman Maloney, Ranking Member Comer, and members of the committee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency alongside National Cyber Director Inglis and Assistant Director Vorndran. I look forward to discussing CISA's efforts to elevate our Nation's response to the ransomware epidemic.

CISA is the national coordinator for critical infrastructure security and resilience, responsible for reducing risk to the digital and physical infrastructure Americans rely on every hour of every day. Within the administration's approach to countering ransomware, CISA's focus is on bolstering resilience. Unfortunately, strengthening resilience to withstand ransomware attacks is arguably the most difficult element of our collective efforts, as it ultimately relies on changing human behavior.

While certain steps, such as spotting phishing attempts, implementing multifactor authentication, or patching vulnerabilities, are easily implemented at the individual level, they are much more difficult to implement community, business, or organization wide. Building resilience requires a long-term investment in people, processes, and technology. Every organization that wants to avoid being a victim of ransomware must invest in the practices that will keep their customers, their systems, and their data protected, investments that make good security and business sense.

The question that we need to ask ourselves is what do we do now to truly have an impact? I'd point to three things.

First, we must give people the tools and guidance they need to increase their resilience and security. That is why CISA is working

to raise awareness and promote basic cyber hygiene across tens of thousands of businesses and organizations and governments throughout the country.

Earlier this summer, we led the interagency development and launch of StopRansomware.gov, the U.S. Government's official repository for resources from across the interagency to help public and private organizations tackle ransomware more effectively. To date, StopRansomware.gov has had more than 455,000 page views, and our Ransomware Readiness Assessment Tool has been downloaded nearly 15,000 times.

We just wrapped up Cybersecurity Awareness Month in October, which included over 300 events, trainings, and webinars, as well as CISA's fourth annual National Cyber Summit, which reached more than 73,000 individuals, helping them to understand the importance of being cyber smart.

Second, because vulnerabilities are widespread across technology environments, it is increasingly challenging for any organization to prioritize which vulnerabilities to fix. So last week, we released a binding operational directive, which established a dynamic system-managed catalogue of more than 300 known vulnerabilities that are exploited, requiring Federal agencies to remediate such vulnerabilities within a specific timeframe.

While aimed at the Federal Government, we strongly encourage every organization to adopt this directive and prioritize mitigation of these vulnerabilities, those listed in CISA's public catalogue, as we continually identify newly exploited vulnerabilities.

Third, we must drive impact at scale if we hope to achieve the level of resilience we seek. Critical to that effort will be our partnership with key players who could help us achieve broad-based effects.

In the coming weeks, we'll be announcing our Cybersecurity Advisory Committee, and the Cyber Safety Review Board, two groups of outstanding thought leaders and experts who will provide critical perspective, insight, and knowledge in dealing with our most difficult cyber challenges. These efforts build on the recently launched Joint Cyber Defense Collaborative, or JCDC, a partnership between key Federal agencies and private sector companies who see across networks and industries to help us identify emerging threats, provide actionable information, and take action at scale to reduce the risk of compromises of all types.

Finally, perhaps the most important role is to leverage our expanse of information-sharing authorities to ensure early warning of threats and attacks. But presently, we only receive information of a fraction of incidents. This hampers our ability to conduct critical analysis, spot adversary campaigns, release mitigation guidance, and provide timely response. This leaves critical infrastructure vulnerable, which is simply unacceptable.

Providing this information to CISA and our Federal partners quickly will allow us to enrich it and get it out broadly, protecting future victims and raising the baseline of national cybersecurity. Given the importance of visibility into the true size and scope of the cyber threats facing us, I urge Congress to move quickly on the urgent priority of adopting incident notification legislation.

I would be remiss if I didn't close with a thank you to Congress. Today marks our third anniversary as the Cybersecurity and Infrastructure Security Agency. You have entrusted us with a critical mission, and I am honored to work alongside an incredible group of men and women who execute that mission with professionalism, integrity, and excellence.

Thank you for your partnership and support. Our Nation is facing unprecedented risk from cyber-attacks undertaken by both nation-states and criminals. In collaboration with our government and critical infrastructure partners, international allies, and with the support of Congress, CISA will continue to lead our national call to action.

I want to thank you again for the opportunity to appear before the committee, and I look forward to your questions.

Thank you.

Chairwoman MALONEY. Thank you for your testimony and for responding on such short notice.

And our last witness today is Assistant Director Vorndran. You are now recognized for your testimony.

STATEMENT OF BRYAN VORNDRAN, ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. VORNDRAN. Good morning, Chairwoman Maloney, Ranking Member Comer, and members of this committee.

Thank you for the opportunity to be here to represent the FBI and our cyber program and to sit with Chris and Brandon as a unified front against a growing ransomware threat in this country. The three of us and our staffs are constantly in touch, and I appreciate the work both of them and their organizations are doing to keep this country safe.

I'd also like to thank, in no particular order, the Department of Justice, the Secret Service, U.S. Cyber Command, NSA, CIA, Treasury, and state—all who have a significant role. I hope everyone leaves the room today understanding that no one Federal agency can tackle cyber threats alone, but that we each have unique authorities and capabilities allowing us to create a whole greater than the sum of our individual parts.

Ransomware may just now be grabbing the headlines, but the cyber threats facing our Nation aren't new. In fact, the FBI's Cyber Division is turning 20 years old next year. Over that time, we've learned a lot. Most notably, how to work within the interagency, with foreign partners, and with private sector companies.

We also have recent reminders about the long arm of the law, with the arrest in Poland of Yaroslav Vasinskyi, the individual who conducted a ransomware attack against Kaseya.

Our current strategy for countering ransomware and other complex cyber-criminal schemes is focused not just on indictments or arrests, though we do think it's important to remove players from the field, but on pursuing and disrupting the actors, their infrastructure, and their money, all while providing help to victims and actionable intelligence to warn potential future victims.

Looking ahead, I have no doubt the playing field and the rules of the game will change over the coming months and years. In the face of this threat evolving, I believe our interagency team is im-

proving each day, and we're excited for the opportunity to continue to serve and protect our country from cyber threats.

As Chris mentioned, there are four critical outcomes for all of us—Federal coherence, improving public-private collaboration, aligning resources to aspirations, and increasing present and future resilience. The FBI, due to its unique authorities, will play an important role in achieving each of these outcomes, but the FBI won't be able to fully support these strategic outcomes if we don't receive timely information about cyber breaches.

As the cyber threat has evolved over the past 20 years, one thing has remained the same. The FBI has been at the center of acting on U.S.-based cyber threat intelligence. It's what we do best.

When I discuss the FBI's value proposition in cyber with people who want to see this country succeed, I describe it this way. The FBI is the only agency in this country who can get a well-trained agent working with local computer scientists, intelligence analysts, and others on any doorstep in this country within an hour. Cyber is a global, mostly foreign-based threat. And we can be on the doorstep of foreign law enforcement and intelligence services in a position to assist within a day in over 70 countries, too.

Our agents care. They want to make a difference. It's why I and almost everyone else joined the FBI.

Now I know there are several cyber incident reporting bills currently being considered, and I can't stress enough the importance of the FBI receiving full and immediate access to cyber incidents so we can act on them as soon as possible and in unison with our Federal partners at CISA. The faster we get this information, the faster we can deploy a local cyber threat expert to a victim's door; track, freeze, and seize funds taken; and ultimately hold cyber criminals accountable.

Twenty-four hours probably wouldn't seem like a big delay to most people, but the help we can offer within that time can be the difference between a business or a piece of critical infrastructure staying afloat or being crippled. Let me state the same as a sports metaphor. Why would a team bench one of its best players in the first quarter of the Super Bowl? It doesn't make a lot of sense to me. And we're all rightly focused on the incredible harm cyber actors are causing. To give those criminals a head start against the people protecting the public doesn't make sense.

As the U.S. Government continues to hone its approach to this problem to take full advantage of all instruments of power at its disposal, I believe we'll see two significant types of outcomes. First, we want to degrade the ecosystem where it's no longer worth our adversaries' time and effort to commit these crimes.

Second, we do want to remove players from the playing field. It's awfully hard to hack a computer from behind bars. Just ask Yaroslav Vasinskyi.

Chairwoman MALONEY. Thank you. Thank you very much.

I now recognize myself for five minutes.

The United States is a major target for ransomware attacks, and it is really a threat to our national security. It is my understanding there is legislation attached to the NDAA that will allow our government and require our government to start tracking data on

cyber-attacks, and I am hopeful that this will be signed into law. This is a good first step.

Many other experts tell me the next thing we have to do is get a stronger coordination between the private and public sector, which Mr. Vorndran spoke about in his testimony. It is hard for the government to respond and help if we don't even know about the attacks. There have been numerous bills before Congress for a long time. We have not been successful in passing them because there is resistance and, really, objection from the private sector.

I understand that England has been successful in setting up systems that have the private sector now working with their government to respond to cyber-attacks. I would like to start with Mr. Wales, but invite our other two panelists to answer, if they would, too. What can we do to pass this legislation, put in place this type of cooperation?

This is a threat to our national security, our economic security, and certainly to the public and private sector. So, if we could start with you, Mr. Wales?

Mr. WALES. Sure. So, I'll answer the question in kind of two parts. The first part is associated with the legislation you're discussing. I think as both—all three of us said during our opening statements, passing cyber incident notification legislation is a top priority. We need the information because that enables CISA and the FBI to both engage with that victim, offer our assistance, understand what's happening on their networks, and protect other victims, as well as all the threat response of going after the actor and following the money that the law enforcement community, including the FBI, begins to do from that point.

But even today, there is a lot that we are doing across the U.S. Government to improve our public-private partnership, to enable more effective cyber defensive activities in protecting the homeland. I mentioned during my opening statement the recently launched Joint Cyber Defense Collaborative, where we've brought together the critical government agencies, like the FBI and the NSA and Cyber Command, along with those companies in the private sector who have the best visibility into the cyber ecosystem.

We're talking about major cloud providers, major internet service providers, the cybersecurity firms in the private sector who provide response and support and protection to thousands, tens of thousands of companies across the country.

As we work together to identify and spot adversary activity, as we share indicators back and forth and enrich them on both sides, we're able to provide more protection than anyone can do independently. These are the companies that can take action on a massive scale to protect networks. And so even if companies are not part of that collaborative up front, they are often being protected by the activities that are happening within that structure.

It is something that is new. We rolled it out in August, and we've already seen fairly significant success in identifying recent campaigns and activities. And we really look forward to working on this more in the future and appreciate Congress' support, since this effort was enabled by authorities granted in last year's NDAA.

Chairwoman MALONEY. Thank you. And in the interest of time, I now want to move to Assistant Director Vorndran.

Last week, the Department of Justice announced charges against two foreign nationals for their role in the ransomware attack against the Florida-based software company Kaseya. One of the people indicted is a Russian national who is reportedly responsible for over 3,000 ransomware attacks.

I commend the Justice Department and our international partners for bringing to justice these attackers, but to hold cyber criminals accountable, Russia has to play by the rules. Can the charges against the Russian national be viewed as a test case for Russia's willingness to crack down on cyber criminals?

Earlier, Mr. Inglis has testified publicly, made public statements that because of the Biden administration's active engagement on combatting cyber that some of the activities in Russia seem to be more mild, but you said that you don't know if this is going to be sustained. But could you respond on this, and how should the U.S. respond if Russia fails to act?

Mr. VORNDRAN. Thanks for the question.

I would default the question or defer the question about the administration and test case to Mr. Inglis. But from an FBI perspective, we have not seen a decrease in ransomware attacks in the past couple of months originating from Russia.

Please understand we do have incomplete data. In a best-case scenario, we only see about 20 percent of the intrusions in the country, no different than our partners at CISA. But the FBI has remained focused on investigating the cyber criminals in and around Russia for well more than a decade at this point in time. So, the indictment of Yevgeniy Polyanin is just the latest indictment that we pursued based on criminal conduct here in the United States.

Chairwoman MALONEY. Would you like to comment, Mr. Inglis, on——

Mr. INGLIS. Yes, ma'am. I would simply add to that that it's very important that Russia play a part in this. It is far more effective to stop these threats at their source. In a permissive environment, if harbored, if given safe haven by the Russians would encourage more—more entry into the space.

That being said, we're not powerless, kind of using only the Russians as a tool to push back on this. The strategy that I articulated earlier and that others have reflected on actually says we can become a harder target. We can increase resilience and robustness. We can bring international coalitions to bear. We can find these transgressors not simply in Russia, but as they travel to other countries or as they kind of ship their illicit gains broadly across the internet.

So, all of those instruments should be brought to bear. We will continue to pressure the Russians very strongly to help them understand that they must do their part.

Chairwoman MALONEY. The gentleman yields back. My time has expired, and in answering the question, I went overtime. I give certainly as much time and more to my distinguished ranking member, Mr. Comer.

Mr. COMER. Thank you, Madam Chair.

In early July, a Florida software company became the victim of a ransomware attack, causing widespread outages for over 1,000

institutions ranging from hospitals to schools to grocery stores. It wasn't until July 23, three weeks later, that the company announced it had received a universal decryption key to help companies restore their files.

Now in September, the *Washington Post* reported the FBI had secretly obtained the digital key to unlock these files, yet sat on it for three weeks and never told the companies, costing untold millions of dollars in recovery cost. The FBI's rationale apparently was to carry out an operation to disrupt the hackers, a group known as REvil. Yet according to the Post, the group's platform went offline without U.S. Government intervention before the FBI even had a chance to execute its plan.

In September, the chairwoman and I wrote to Director Wray asking for a briefing on the FBI's decision. We never received that briefing. And Mr. Vorndran, I am going to address my first question to you, but with respect to the briefing, I understand that you are not at the top of the organizational chart at the FBI, but please relay to Director Wray that when the Oversight Committee requests a briefing, we expect a briefing.

I think—I don't think it is any secret in 11 months, we are probably going to be sitting over there, and we are going to have a lot of questions for the FBI. From the Steele dossier to the ransomware attacks, we have a lot of questions for the FBI. And at the very least, when we request a briefing, especially in a bipartisan manner, we expect a response.

So, Mr. Vorndran, I am asking you today, can you please explain the policy rationale behind the FBI's decision to withhold the digital encryptor key?

Mr. VORNDRAN. Sir, I think the question is how do we do what's in the best long-term interest of the public and balance that with protecting the public in the short term? Stated differently, if any one of us had a loved one with a disease, and we could take a longer-term approach to completely eradicate that disease, takes a little bit of time, perhaps a little discomfort for a loved one, we'd probably prefer that over a less-effective, shorter-term solution because, in the end, we'd know it would have a more long-lasting effect.

The decisions that you're referring to and asking about are very, very complicated, and they are ones we take seriously. And it's why decisions like those are not just made within the FBI, but they're taken into an interagency environment for final determination of what makes the most sense.

I think it's also really important to remember that those decryptor keys that you're referring to were developed and coded by safe harbored criminals. In this case, we took an extensive process to develop a safe and effective way to deploy that decryptor key to the victims at Kaseya. Obviously, simply grabbing malware that's been coded by criminals in Russia and deploying that onto U.S. infrastructure would not be a wise decision, and those things take time to get right.

We repeatedly tested that decryptor in different environments because an even worst-case scenario for us was providing criminal-generated decryptor keys to victims that introduced new vulnerabilities and backdoors into U.S. infrastructure.

So, I'll stop there for today, sir.

Mr. COMER. So, did the FBI conduct any estimates as to how much money was lost by the hundreds of institutions due to the Bureau's decision to withhold the digital encryptor key? Was that ever—did that play a——

Mr. VORNDRAN. Sir, I'm not—I'm not prepared to answer that question today.

Mr. COMER. We would—you know, that is—we get complaints from businesses, as their representatives and their Member of Congress, about decisions that government agencies make, and it is always frustrating when the government agencies or the bureaucracies, bureaucrats don't take into consideration how much this decision will actually cost. And that is a problem.

Director Inglis and Mr. Wales, did your agencies agree with the FBI's decision to withhold the digital encryptor key, and was the decision unanimous, or was there dissension?

Mr. INGLIS. Thank you for the question and the opportunity to comment.

My organization was not in place at the time that this operation took place. But my read of the record was that this was a well-discussed and a consensus position of the various agencies that had the opportunity to comment. I would simply observe, as Assistant Director Vorndran has said, there was never a question about the desire to, in a timely, broad way, disrupt this action and to save the downstream effects on potential further victims.

The question at the end of the day is how do you maximize the timeliness and the breadth? If you were to act in the very first instant, you might then expose your knowledge of what's happening, allow the criminals to escape, to take their accesses to various other customers that haven't yet been sprung and to spring them at some later time.

If you wait for a while—and that is, therefore, a very subjective choice, one that must be well considered—you might then be able to simply remove the entirety of this threat from the landscape. If you wait too long, then there are too many victims. And so, there's something between zero and infinity that you have to then come down on to align timeliness and breadth.

Mr. COMER. Mr. Wales?

Mr. WALES. I think Director Inglis' response was, you know, on the money. This was a—a challenging environment, and I think anytime you're in the middle of an incident response, balancing the various equities of what can be shared publicly, what needs to be held back so that you can achieve longer-term benefits, those are part of ongoing discussions during nearly every incident response that our agency, in cooperation with the FBI, is involved in.

And I think that care and open discussion was—was evident in this case as well. And, but I don't think there's anything else we can say about what happened in the interagency right now.

Mr. COMER. Well, I will close with this, Madam Chair. I would strongly encourage the FBI and whoever in the Biden administration is faced with this decision again to take into account the hundreds of millions of dollars that private companies are losing by a decision to withhold unlocking that. That is something that—that should be taken into account.

So, with that, Madam Chair, I yield back.

Chairwoman MALONEY. The gentleman yields back. The gentlewoman from the District of Columbia, Ms. Norton, is now recognized. Ms. Norton?

Ms. NORTON. Thank you, Madam Chair, for this important hearing. Very important.

The focus on ransomware in the news has been on big corporations. I was astonished to find that schools are more likely to be the target, and yet they have the fewest resources to deal with this matter. So, I looked for examples, and I found that in Broward County, Florida, a district there had a demand for $40 million in ransomware. And when the school district refused to pay, the hackers posted 26,000 stolen files on the Internet. So, harm can, in fact, be done.

Mr. Wales, it looks like schools face unique risks, and I wonder what can be done? They have few risks, yet we need to strengthen their cybersecurity in K through 12 schools. Could you briefly, Mr. Wales—and I thank you for agreeing to be here on short notice—briefly say what CISA is doing to address the problem of ransomware in schools?

Mr. WALES. Sure. Thank you, Congresswoman.

We are and have been working hard to expand our outreach to school districts as a result of the growing threat of ransomware that they have faced, in particular making them aware of the free resources that are available today that can help them improve their cybersecurity. Under a cooperative grant to the Multi-State ISAC, which helps support state and local communities throughout this country, there are a number of free services that the MS-ISAC offers to school districts and other state and local governments that can help them provide critical protections, including things that block malicious domains. They provide initial triage and support during incident response.

And there is more services that can be taken on. Unfortunately, school districts are among the least signed up for a number of those free services. So, we're doing a lot to kind of raise awareness.

In addition, thanks to some additional authorities provided by the Congress last year, we have been hiring state cybersecurity coordinators that are designed to live in each state and work directly with the state and local governments in their areas to make sure that they understand the services that are available. And we now have 36 of them onboard throughout the country, and part of their job is to help conduct this kind of outreach and awareness.

In addition, last month, the K through 12 Cybersecurity Act was passed and signed by the President. That required us over the next 120 days to better identify what more can be done to support state and local governments when it comes to protecting school districts and to begin to roll out those services, including new trainings. And we have a team across our agency working with relevant interagency colleagues like the Department of Education on our response to that legislation, and we look forward to briefing Congress on our plans in the coming months.

Ms. NORTON. Well, Mr. Wales, it does look like you are doing a great deal, but the Department of Education, in a report that has recently been issued by the GAO, noted that the—that various

services to help K through 12 with cyber threats appear to have an extremely low participation rate. You have a—you have something called Albert that schools can get for a modest fee. Yet less than 10 percent of districts across the United States have signed up for this service.

Mr. Wales, how can we encourage better participation in programs that CISA—that CISA funds and offers to school districts around the country? Is the fee too high? Is there lack of awareness about the program? What is the problem, and what can we do about it?

Mr. WALES. I think, like a lot of our cybersecurity challenges, this is a multifaceted problem. We do need to do more to raise awareness so that people in school districts, and there are a large number—you know, I think the number is around 13,000 school districts throughout the country—we need to raise more awareness so that those folks who are working on——

Ms. NORTON. There are 15,000.

Mr. WALES. Fifteen thousand. We need to do more to raise awareness so that those people understand what resources they can get, including a number of free resources for some things that there is going to require an investment.

Now we are very hopeful with the new state and local cybersecurity grant program that was established in the infrastructure bill that was recently signed by the President will give us more ability to provide resources down further into the state and local governments. Some of that money can be used to protect schools. That will be part of the ongoing conversation we have with the states about the implementation of that grant program over the next several years.

So, we do think help is on the way, but this is a—this is a collective problem, and I think anything that you can do from your perches to raise awareness in the districts that you represent about the services that are out there and reaching out to the government to see what else can be done to protect the Nation's schools, we'd strongly encourage you to do that. And we're willing to provide any support we can to help enable that kind of outreach and engagement.

Ms. NORTON. Thank you, Mr. Wales. My time has expired.

Chairwoman MALONEY. Thank you. The gentleman from South Carolina, Mr. Norman, is recognized.

Mr. NORMAN. Thank you, Madam Chairman.

Director Inglis, you have got a big job as head of cybersecurity of this country. The security of America, not just with cybersecurity, is being compromised by this administration allowing the millions coming in here from 152 countries that we have no idea what they—why they are coming. Do they have terror backgrounds? And the task that you have, along with the others, is just unbelievable now.

You mentioned Russia, and you mentioned pressure points. The only non-pressure point that this administration has done is allow them to build the Nord Stream pipeline, which aids and abets Russia, the very country that we are attributing the cyber-attacks to.

So, what specific pressure points do you think this administration, with their record, will actually do to bring them to comply? Is it just to ask them to be nice?

Mr. INGLIS. So, thank you very much for the question. It's an important question.

This administration, not unlike other administrations, has been very clear with the Russians about what we expect normal behavior looks like, not simply——

Mr. NORMAN. In words.

Mr. INGLIS. In words. Not simply kind of articulating what we believe they should not do, but what they should not harbor in the safe havens within their country or their near abroad. Now we've brought an international coalition to bear to make the same statement.

Mr. NORMAN. Give me specifics. What pressure points—with a rogue country like Russia, what specifics do you think, as head of the national cybersecurity team, would be implemented to use leverage to stop their actions?

Mr. INGLIS. The first opportunity we give them is to simply of their own accord to cooperatively respond to the request that we've made. We have provided——

Mr. NORMAN. OK. Just more words.

Mr. INGLIS. We have provided information to them. We are now assessing whether they provide that. We would withhold certain diplomatic status, certain economic benefits, certain historic rights——

Mr. NORMAN. What? Give me specifics. What would you do specifically that would at least slow them down as to the cyber-attacks? You give them I know words, but words with this administration mean nothing.

Mr. INGLIS. Attribution is important in this case. I think that we have clearly attributed these actions to persons who operate in the Russian or Russian near abroad. We've not attributed these actions to the Russian government.

We, therefore, have to give the Russian government an opportunity to understand what the nature of that problem is and then to address it. Our patience is not unlimited in that regard. We have conducted a number of what are called "expert group meetings" with the Russians to make it crystal clear who we think is accountable here and what we need them to do about that.

There is a limit to that patience, and when that is done——

Mr. NORMAN. OK.

Mr. INGLIS [continuing]. There are some diplomatic and financial remedies that are brought to bear on the leadership of those entities. We've also brought 30 nations to the city to have a discussion about what an international coalition might do in this regard, and I think that Russia clearly sees that the deck is stacked against them in that regard, and they must, therefore, act.

Mr. NORMAN. In all due respect, you gave words, but you didn't have any specifics. It is just asking. It is pleading with them. I feel for you in your job because, you know, the next major attack, if it is on our energy grid, as an example, our water supply, which is—I don't know whether it was one of the 17 items that this President

mentioned that were off limits, asking them not to attack that. I don't know if that is on the list.

At what point is this a declaration of war, a declaration that we cannot put up with? What is this administration going to do other than words?

Mr. INGLIS. It's an important question, and there are multiple pressure points. Russia is one of those pressure points, but we can also make it such that we're a harder target, and they simply cannot prevail. The criminals harbored or given safe haven by Russia cannot prevail because we correct the errors that we make in the construction and the defense of these systems.

We can ensure that we disrupt the architecture that is used against us, and we have done that. There are any number of examples from the last week of that. You can find——

Mr. NORMAN. What? Give me some examples on that.

Mr. INGLIS. Essentially taking the money back from the criminals. There are at least two occasions within the last month where we've done that, where we've arrested and extradited——

Mr. NORMAN. Were they in the country? Were they already here, or did you have to——

Mr. INGLIS. As you note, sir, cybersecurity is a borderless terrain, and therefore, as much as they can reach us, we can reach them.

Mr. NORMAN. It is borderless, but it has got people behind it. What I am asking is——

Mr. INGLIS. It does have people behind it. But therefore, if we bring allies to bear, we can use jurisdiction in places like Poland and Romania, the most recent two examples, to apprehend these criminals and to bring them to justice using the courts of law that exist in the West.

And so, all of those remedies, essentially giving Russia the ultimatum, we have to give them an opportunity to understand and address this. Two, addressing the actors and the infrastructure that is essentially holding us at risk at the moment, and making sure that we're sufficiently resilient and robust.

The sum of those will make a difference, and some of those can, in fact, push back on this threat. Deterrence isn't found by simply shooting your way out of it. That's an important part of the solution, but ultimately, you need to make it such that you're a hard target, and you're proactive, robust in your defense.

Mr. NORMAN. They are shooting their way into us. I yield back.

Chairwoman MALONEY. The gentleman yields back. The gentleman from Massachusetts, Mr. Lynch, is recognized for five minutes.

Mr. LYNCH. Thank you, Madam Chair. Thank you for holding this hearing.

And I especially want to thank our three witnesses for their great work, and I understand how difficult this challenge is.

I also serve as the chair on the FinTech Task Force over on the Financial Services Committee. So, I would like to change gears a little bit and talk about some of the ransomware attacks that have been happening with financial services firms.

I know that earlier this month, the FBI released a private industry notification, and basically, it reported that ransomware attackers are now leveraging specific significant financial events,

such as mergers and acquisitions, initial public offerings, as a focus point to launch ransomware attacks. And the idea is for the ransomware attackers is to impact the victim company's share price at that crucial time, you know, at the point of a merger or acquisition or an initial public offering.

Most recently, the ransomware group DarkSide, that is the same group that was responsible for the attack on the Colonial Pipeline in my part of the country and it shut down major fuel supplies in the East Coast, they recently said about these type of attacks—and I will quote them—"If the company refuses to pay, we are ready to provide information before the publication so that it would be possible to earn in the reduction price of shares." Basically, they are providing information to short the stock.

And Assistant Director Vorndran, a ransomware attack is usually not something that is on the top of a company's mind. You know, there is a lot to do with an IPO or with mergers and acquisition. I am just wondering is this a particularly vulnerable moment for these companies, and how much damage can a ransomware attack inflict especially during this process?

Mr. VORNDRAN. Thank you, sir, for the question.

You know, I think as the threat has continued to evolve, we have seen our cyber adversaries continue to change direction where they have the most leverage. So, the private industry notification that you're referring to highlights vulnerability for companies in your discussion in the financial space that have a lot to lose during the M&A process.

And I think if I were a company, the primary recommendation I would have would be to evaluate all the vectors of risk through that M&A process, and how are you going to manage that situation if something does go wrong?

But to Director Inglis' point, a lot of this comes back to our net defense posture and our resiliency posture. So, the same question has to go to those companies. Have they taken all the proper precautions to build a defense posture that they deem appropriate for their risk profile as they go through an M&A process?

So I'll stop there. Certainly happy to take followup questions.

Mr. LYNCH. Sure. Are we doing anything—the FBI or Mr. Inglis or Mr. Wales, are we doing anything with some of these companies at this moment? You know—you know, looking at IPO—maybe working with NASDAQ or the exchanges so that we can identify that point of vulnerability and have them, you know, plus-up their—their own security so that at least they are aware and taking proactive steps to defend themselves during that period of vulnerability?

Mr. WALES. Sir, I'll take a first stab at that. I think we have a fairly aggressive posture when it comes to working with the financial sector. It's one of those sectors that has focused heavily on organizing itself to make sure that they are sharing information amongst the various companies in the financial sector and that they want to work very proactively with the government to share information and to take action when possible. So that partnership is good.

There are a number of organizations that have been set up to enable that type of strong public-private partnership in the financial

industry. There is certainly more that can be done. I think things like the incident notification that FBI mentioned earlier are designed to feed into that process, raise awareness inside that community so that it can be more of a focus.

But I would say, sir, you're looking at one side of the challenge. But this is—this is—this is industry wide. It shouldn't matter whether you're going through an IPO or not. Every board should care about the cybersecurity of their company. It should be part of the questions on due diligence when they're going through M&A in every case.

Mr. LYNCH. Thank you.

Mr. WALES. And so we are trying to give them more of that kind of——

Mr. LYNCH. Thank you.

Mr. WALES [continuing]. Make sure that they're asking the right questions and taking the right actions quickly.

Mr. LYNCH. Yes, OK. I was trying to get another question in, but my time has expired. OK, thank you.

I yield back.

Chairwoman MALONEY. Thank you. The gentleman from Pennsylvania, Mr. Keller, is recognized for five minutes. Mr. Keller?

Mr. KELLER. Thank you, Madam Chair, and thank you to the witnesses for being here today.

The increase in both frequency and severity of ransomware attacks shows the urgent need for action. So, I appreciate the topic of today's hearing. Malicious attacks represent a very real threat to Americans' privacy, financial well-being, and the integrity of our national infrastructure. We cannot afford to let these continue to happen.

So, I just would like to ask Assistant Director Wales, we all know that fuel prices are already skyrocketing. Gasoline is already $1 more per gallon than it was last time this year, and Americans are projected to pay up to 30 percent more to heat their homes this winter.

Cyber incidents such as the Colonial Pipeline attack just six months ago underscore how vulnerable we are to various cyber threats. Can you explain to us how another ransomware attack on a pipeline or other critical energy infrastructure might affect the already-high price of fuel?

Mr. WALES. Sir, your point is exact right—is exactly right. During times like this, the infrastructure becomes even more critical because disruptions could have even more significant consequences, and it's why we continue to encourage critical infrastructure owners and operators of all types and across all sectors to think carefully about the risk profile that they have, the potential consequences that could stem from a disruption of their operations, and what more they can do to enhance their security and their resilience. That even if they have a disruption, they can get back up and running quickly without the full consequences happening.

In the case of pipelines, we have worked since the Colonial Pipeline with the Transportation Security Administration, which is the sector risk management agency for the pipeline subsector and who regulates the security of pipelines. They've put in place a number of security directives designed to improve the cybersecurity posture

of the pipeline industry, requiring them to conduct certain assessments on their cybersecurity, provide those assessments to the government, and provide information on cyber incidents in those sectors.

There has been a lot more engagement and outreach with the pipeline industry in response to what we saw from Colonial and from other information available to the U.S. Government. Certainly, more can be done, and we have an ongoing work program underneath the White House focused on improving natural gas pipeline cybersecurity. At the end of September, CISA released new industrial control system performance goals across industry, across all of our critical infrastructure, setting for the first time what we believe should be the baseline cybersecurity posture for any company operating industrial control systems in the United States.

So, we think we're really pushing hard on this to protect our critical infrastructure. We've got a ways to go, but we really support—really, we're encouraged by what we're seeing and really appreciate the support we're getting from Congress for some of these important initiatives.

Mr. KELLER. Thank you for that. And you mentioned everything that the companies could be doing for this, and I know they are going to do that because they need to. Other than—and the importance of it.

And it is the job of the Federal Government to make sure that Americans and that would be companies that Americans own and rely on can produce this. So other than—other than giving Putin a list of things that they shouldn't hack, you know, other than the President giving a list, which the list should be very short. Nothing that affects an American or any of our allies should have been the list. I mean, it would have been a really short list if I had put it out there.

So, in addition to giving Putin a list of things they can't hack, what else has the administration done to make sure that our adversaries know that we are not going to tolerate them any kind of ransomware, any kind of cyber-attacks on our infrastructure or, quite frankly, anything that is an American interest around the globe?

Mr. INGLIS. Congressman, I'll be happy to complement the answer thus far, which I support.

I would say the administration, again, has been clear with the Russians about what the consequences of failing to assist in cleaning up this safe haven in their near abroad would be. They are diplomatic, economic. They indicate also law enforcement.

But again, we are not powerless if the Russians were to fail to take their appropriate action. We brought a coalition to bear such that that coalition will bring further pressure on the Russians. We've done our own research necessary to understand who these criminals are, and when and where possible, we have caused them to be arrested in the various countries they may travel to and extradited to the United States.

We have followed the money flows and apprehended that money when and wherever possible. We have used our intelligence resources to assist the private sector in understanding what the

threats to them are and at the same time give them best practices so that might up their game and become a harder target.

The sum of all of those will make a determinative difference. The Russians can help make that a better program, but it's not a—it's not a completely weak program without the Russian cooperation.

Mr. KELLER. I understand the Russian cooperation and what you are talking about. But if you followed this around and they have been arrested and there has been some money recovered, I think that ought to be money that goes back to the American people and the people that were impacted by this.

I would just like to know what we have done—and maybe this is—can't cover it in five minutes. But I would like to know what we have done to make sure that we are certain that Putin is going to make sure that these things don't happen, and he is going to do everything he can to stop it. I don't know that we have that confidence yet. And handing him a list of things, quite frankly, the list should say nothing. You can't hack anything, or we are going to hold you accountable.

Thank you, and I yield back.

Chairwoman MALONEY. The gentleman yields back. The gentleman from Virginia, Mr. Connolly, is now recognized.

Mr. CONNOLLY. I thank the Chairwoman.

And I agree with my colleague, by the way, that the danger of handing a list of proscribed cyber-attack items is that the inference could be drawn everything else is fair game, and that is a real risk.

Mr. Inglis, last month, the Department of Justice launched the National Cryptocurrency Enforcement Team and the Civil Cyber Fraud Initiative to marshal the Department's resources on complex cyber and cryptocurrency investigations. Earlier this year, the Department also created a Ransomware and Digital Extortion Task Force.

In July, the National Security Council established a Ransomware Task Force. We, of course, have a Cyber Division at the FBI, and we have Mr. Wales as the Executive Director of CISA. When you were before the Senate for your confirmation hearing, you said that one of the primary purposes of your position was to create coherence among Federal agencies with respect to cybersecurity. Given the proliferation of various entities in the Federal Government on cyber-related issues, how—how big of a challenge is that coherence?

I worry about the traditional compartmentalization that characterizes how the Federal Government responds to everything.

Mr. INGLIS. Sir, it's an excellent question and a question that I think is on the minds of many when they look at the complicated organizational arrangements that pertain in cyberspace, no less complicated than the United States Department of Defense, which has an Air Force, an Army, a Navy, a Coast Guard, now a Space Force. It can be coherent if we use those strengths, those diverse strengths in a way that they're applied in a joint, combined fashion.

That's actually the task before us is to use each of those deep and sharp strengths such that they actually collaboratively, collectively, concurrently make the difference that they should. That's our job. That's what we're actually pursuing.

If you were to ask any one of those task forces whether they understand what the other task forces are doing and how they complement one another, I think you'd get a solid answer. I would be happy to come back and talk at length about the details underneath of all of those.

If I might address your earlier observation, which the President, kind of having given Vladimir Putin a list. If you were to ask any cyber expert within the United States, frankly, and various other places, but within the United States how do we describe critical functions, that person would likely say we describe it in 16 ways. There are 16 critical infrastructures.

And therefore, if you were to say don't attack critical infrastructure, turns out that there are 16 definitions. It's the energy sector. It's the transportation sector, and so on and so forth. That's simply a way broadly to say don't attack anything critical.

Mr. CONNOLLY. Yes, let me just say to—Mr. Inglis, I will stipulate that last point. But with respect to your observation about my question, let me just say the experience is at best spotty within the Federal Government. You look at terrorism as a challenge, and the coordination among Federal agencies, say, prior to 9/11 not something to be proud of.

In fact, information was withheld. Information wasn't shared. Intelligence wasn't shared. Cooperation was not a characteristic of the culture not only within the Federal Government, but between the FBI and other agencies of the Federal Government and our local law enforcement.

Mr. INGLIS. Sir, I do acknowledge the historical accuracy of your observation. You are quite correct. We have had moments when we failed to connect the dots or, worse, where we've failed to combine our efforts to even form the dots. I think what you're hearing from this panel today is that we understand that we must integrate and collaborate such that we discover and do things together that no one of us can do alone. That's the challenge.

Mr. CONNOLLY. Well, I will—I will observe that we had the CEO of SolarWinds, Mr. Ramakrishna, before this committee talking about the attack his company experienced that affected a lot of Federal agencies. And his observation was having a single entity to which all of us can refer will serve the fundamental purpose of building speed and agility in this process. Too much time is wasted in communicating across agencies where information is very fragmented.

Mr. INGLIS. Sir, we agree.

Mr. CONNOLLY. OK.

Mr. INGLIS. And to quote my good friend Jen Easterly, who's not able to be with us today, we shouldn't need a Ph.D. in government to get responsive, coherent service from the government.

Mr. CONNOLLY. Well said. Final observation, maybe to you, Mr. Vorndran. Should companies or Federal agencies or state and local governments pay a ransom? What is the guidance we give? And if a ransom is ever to be paid, should it not be a last resort, rather than the first response to the threat? Your observation. And what policy guidance does FBI give, and then I would yield back.

Mr. VORNDRAN. Sure. I appreciate the opportunity to get this on the record. The FBI's official position is that we do not recommend

any company paying a ransom. However, we understand that a company's decision to pay a ransom should be based on their own business priorities. And if they choose to pay the ransom, we would ask that they simply let us or CISA, or the appropriate Federal law enforcement agency they're working with at the time, know.

Because the quicker we're able to see the money, the better the chance we have to trace it. So, our bottom line position is we do not recommend paying ransom because it fuels a huge criminal enterprise, but we do understand it's a business decision, and we understand that that's a company's decision.

Mr. CONNOLLY. Thank you, and I yield back.

Chairwoman MALONEY. The gentleman yields back. The gentleman from Arizona, Mr. Biggs, is now recognized.

Mr. BIGGS. I thank the chairwoman, and I thank the witnesses for being here today.

So, some cybersecurity experts have said that diplomatic pressure, economic sanctions, and criminal prosecutions are insufficient to deter adversaries and that the administration should use offensive cyber operations to degrade an adversary's capabilities and create credible deterrents. I am wondering, and I guess this is for each of you, is what offensive cyber operations might be effective in deterring cyber-attacks on our businesses and our government entities?

Director?

Mr. INGLIS. Thank you for the question, sir.

I think taking a broader interpretation of what offense looks like in cyberspace, it might not be what if you—one would imagine in kinetic space, using all instruments of power, trying to impose cost to perhaps stop, thwart, or apprehend, right, the threat of the moment. We can use diplomatic power to use other nations' authorities to arrest, extradite people. Combine that with legal authority, we prosecute those people in our own court. That, to the individual miscreant, is an offensive maneuver.

We can essentially use our capabilities to find and arrest money flows. We can use our capabilities to take down illicit infrastructure. We can collaborate with the private sector to thwart these attacks in situ as they come across the boundaries that those various operators have.

As the law of conflict would say, and I avoid the term "armed conflict." This is not an armed conflict. But as the law of conflict or contention would say, the remedy must be proportional to the need. And in this case, we have many instruments of power at our disposal such that we can understand what's happening to us, engage it at the earliest possible moment, and bring these threats to heel.

Mr. BIGGS. So, Director—I am sorry, I was going to give you all a chance. I will try to get back to you. I just want to ask, you mentioned a number of things that you thought would be categorized as offensive in the cyber world.

How successful—how much have you engaged in that? How successful have you been? And then—and then I will turn the first question and those over to Mr. Vorndran and then Mr. Wales.

Mr. INGLIS. I think that we have applied all of those instruments to have the powers of early discernment through diplomacy,

through legal means, through financial means, and understanding in cyberspace what's transpiring and at those moments when we understand a threat is being arrayed against us, to interdict that at the earliest possible moment.

I would say that anecdotally over the last few weeks or months, you have seen some evidence that those are beginning to succeed against the nature of the threat, which is long in the making. It's not unlike climate change, which is decades in the making and, therefore, can't be turned around in a fortnight. It's too soon to tell whether we will sustain that in a concurrent, applied fashion to have the changes—to make the changes necessary.

That being said, as important as that offensive component is that you address and that I've attempted to explain, defense is equally, if not more, important. Stopping these threats by simply making them such that they may not succeed is as important as any other because there's no nation in the world that is more dependent upon infrastructure, digital infrastructure, than we are. And therefore, we have to be concerned that if we were to——

Mr. BIGGS. Director, I thank you.

As you are answering the questions, Mr. Vorndran, I would like you to elaborate on arrest, indictment, and also interdiction and interception of flows of money that are being—that you are undertaking, if you can.

Mr. VORNDRAN. Of course. I just want to go back to the first question you asked, sir. One item to build on what Director Inglis said is we heard a reference here to pre-9/11 and post 9/11. The ecosystem in cyber moves at a pace that far outpaces what we saw post 9/11 and terrorism.

The reason I highlight that is because the public-private collaboration and what private sector sees on their infrastructure is infinitely high. And without that flow of intelligence from private sector, it inhibits our ability to be more proactive and be more offensive.

To your second question about, you know, the term "following the money," we have virtual currency efforts in the FBI. Secret Service has them. IRS has them. We are all looking at those money flows. Treasury is heavily engaged in sanctioning individuals and entities so that U.S. persons and U.S. businesses can't partake in that.

So virtual currency remains a very, very key focus area for us in terms of putting pressure on the threat.

Mr. BIGGS. Thank you.

And this is for you, Mr. Vorndran. Earlier this year, the Washington Post reported that the FBI refrained for almost three weeks from helping to unlock computers of hundreds of businesses and institutions hobbled by a major ransomware attack, even though the Bureau had secretly obtained the digital key needed to do so.

And I guess the question is do you believe there are steps the FBI could have taken in that case to provide relief to the victims of the ransomware attack without also compromising the Bureau's efforts to disrupt the Russian-backed hackers there, knowing that it was estimated that literally millions of dollars were lost by the victims?

Mr. VORNDRAN. Sir, my answer to that question is already on the record. I'm happy to go through it again if you desire.

Mr. BIGGS. Yes, I would.

Mr. VORNDRAN. So, and Director Inglis provided some commentary as well. I think from our perspective, the question is how do we do what's in the best long-term interest of the public while also protecting the public in the short term. And I compare it to if I had a loved one with a terminal disease. If I could take a more long-term effort to sustain their life for longer, right, knowing I have a more impactful outcome, then I would probably play that hand versus a band-aid solution.

So, in our efforts, right, we thought with our interagency partners—and this decision was taken to a complete interagency team where there was consensus—that it was best to play the long game. I think it's really, really important to understand that those decryptor keys that you're referring to were built by criminals, right? They weren't built by us.

And so, taking a decryptor key built by a criminal and simply deploying it to, in this example, Kaseya or their downstream victims is not a good decision either and requires multitudes of testing environments and time tied to those testing environments to make sure that we're not inadvertently introducing back doors or other malicious code onto U.S. infrastructure.

Chairwoman MALONEY. The gentleman yields back. Mr. Raskin, you are now recognized.

Mr. RASKIN. Madam Chair, thank you very much.

In July, Justice Department official Richard Downing testified before the U.S. Senate that DOJ believes only one-quarter of ransomware intrusions are reported. At this rate, the government is missing crucial information that it could use to help ransomware victims and deter future attacks.

But for victims who do want to report a ransomware attack, the guidance on who to report to is not exactly clear or efficiently organized. For example, if I am the victim and I visit the FBI's website to report it, I am encouraged to take one of three steps. I can report the ransomware attack to my local FBI field office, submit a tip through the FBI's tip portal, or report it to the FBI's Internet Crime Complaint Center, or IC3.

Assistant Director Vorndran, how many FBI field offices are there?

Mr. VORNDRAN. Sir, there's 56.

Mr. RASKIN. Fifty-six. So, if I am the victim of a ransomware attack, there are potentially 58 different points of entry to the FBI to report the attack, counting the online portals. Now if I visit the website StopRansomware.gov, which is supposed to be the one-stop ransomware resource, I am advised that I can report not only to these 58 points within the FBI, but also to CISA or the Secret Service, which has its own network of field offices, too.

Director Inglis, let me ask you. I appreciate the possibility that I might have multiple points of access, but doesn't this sound potentially confusing and byzantine to a ransomware victim to try to figure out where actually to go?

Mr. INGLIS. Congressman Raskin, thank you for the question.

I admit that if those were independent entities, it would be confusing. There would be too many opportunities, and you wouldn't know that it got to the right place at the right time.

Our job on the Government side is to ensure that if you've told one of them, you've told all of them. CISA, FBI, the Secret Service routinely coordinate the information that they receive, and we've established something called the Joint Cyber Defense Collaborative where that information is synthesized and pushed out to a much broader population.

Mr. RASKIN. All right, good. Well, I want to pursue that point.

When CISA receives a ransomware report from a victim, does it automatically share that information with the FBI or the Secret Service, Mr. Wales?

Mr. WALES. Yes. So, I would say that in almost all cases, we're always going to work in partnership largely with the FBI and also with the Secret Service. In almost every case where we have conducted direct engagement with or notified a victim, that is always coordinated ahead of time with the FBI. We almost in all cases do that jointly to ensure that CISA's role in terms of providing support and responding to the—helping to understand what happened and share information, the FBI's threat response role, that we can both support that company through that engagement.

Mr. RASKIN. In what cases would you not?

Mr. WALES. You know, I don't think there's any case where we say we're not going to do it. I just want to leave myself a little bit of flexibility that if something came in in a weird way and one of our field personnel did not report it up properly that it may not have happened. But that is not the standard operating procedure that we operate under.

Mr. RASKIN. OK. Assistant Director Vorndran, when the FBI gets a ransomware report from a victim, does it automatically share that information with CISA or the Secret Service?

Mr. VORNDRAN. Sir, I will double down on Mr. Wales' statements. We have central coordinating entities between FBI Headquarters Cyber Division and what is referred to as CISA central to share all of that information. All of our threat reporting and notifications flow from our field offices back into that portal.

So certainly, our intention and we believe our practice almost 100 percent of the time is cross-leveling the coordination with CISA. And, but certainly, none of us are failure proof. So, I'm sure there is one or two examples out there we haven't gotten it exactly correct.

Mr. RASKIN. Director Inglis, if a victim reports a ransomware attack through any of the channels listed on the StopRansomware website, does that guarantee that every agency that needs to know about the attack is notified, or is it more ad hoc? Does the collaboration, as just set forth by these other two gentlemen, does that collaboration work systematically and uniformly?

Mr. INGLIS. As my colleagues have said, the design and the intended operation is that having told one of them, that all of them will then know and be able to respond with their unique authorities.

Mr. RASKIN. Right. I just am finding it curious that no one wants to state categorically that it happens. So——

Mr. INGLIS. Sir, I would say that the caveat here is that, you know, we're kind of allowing for the fact that the system is not per-

fect and, therefore, may be a situation or two where it doesn't work. We will work to correct that and identify those.

Mr. RASKIN. I see. So, if it doesn't happen, that would be an accidental thing. That would not be——

Mr. INGLIS. That's correct.

Mr. RASKIN [continuing]. As the product of a deliberate policy?

Mr. INGLIS. That's correct. There are no policies that would fail to share, but the implementation is what we're then cautioning might not be perfect.

Mr. RASKIN. OK. So, if a ransomware victim thinks that he or she has been the victim of a crime, they don't need to file an independent report with the FBI, it is enough to report it to CISA, for example. Is that right?

Mr. INGLIS. That's correct, sir.

Mr. RASKIN. OK. All right. Finally, Mr. Wales, is there any specific reporting advice you can provide to a small business owner suffering from a ransomware attack? What should they do?

Mr. WALES. Sir, we actually worked with the Multi-State ISAC to release a ransomware guide last year. It was designed for state and local governments, but it's very applicable to small and medium-sized businesses. And it actually goes through kind of a checklist what to do ahead of time, how do you better protect yourself and prepare for ransomware incidents.

And then it goes through like my last memory is we added maybe like 19 steps that you should undertake if you have a ransomware incident, including kind of understanding what happens, isolate your network to the extent you can, when you should turn off devices, who you should call. Kind of works through the steps as someone who has been a victim, what they should do and how they should potentially engage with an outside firm who can potentially help them, reach out to the Government who could potentially offer some support.

That information is out there. It's on StopRansomware.gov. We think it is well designed for the small and medium-sized business.

Mr. RASKIN. Thank you very much. I yield back, Madam Chair.

Chairwoman MALONEY. The gentleman from Florida, Mr. Franklin, is recognized.

Mr. FRANKLIN. Thank you, Madam Chairwoman.

Mr. Vorndran, what is your estimate of the percentage of cyberattacks that are criminally motivated versus foreign intelligence cyber operations?

Mr. VORNDRAN. Sir, I don't have a good answer to that question today. I would be happy to take that back and get you a more refined answer. All I can say is that between nation-state actors and criminal attacks on U.S. infrastructure, both are extremely prolific.

Mr. FRANKLIN. Do you ever see or do you believe, in your opinion, do you think there are nation-state actors that are posing as criminals at times to probe our networks under the guise of just seeking ransomware but actually have a more nefarious intent?

Mr. VORNDRAN. Sir, we can—this is more of a classified discussion. But what I can say here is we would refer to that as a blended threat. And so, there are some intelligence gaps about whether intel service individuals are moonlighting as criminals or state actors are hiring criminals to conduct certain activity.

So those are some gaps. Certainly, happy to have a more classified discussion with you if that's an interest to you.

Mr. FRANKLIN. OK, thank you.

Do you think with the spike that we are seeing in ransomware, is it more that people are more willing to report it, or are there more attacks because crooks are seeing that it is more profitable, it is more lucrative? Why the recent spike, do you think?

Mr. VORNDRAN. So, our data—and again, I think it's important to highlight that we only see—our estimates are about 20 to 25 percent of the total intrusions, and I'm quite sure Brandon would share approximately the same figure with you. So, it's very hard to say increase/decrease.

What we can say, though, is in the last six months we have not seen a decrease in the amount or frequency of reporting on ransomware attacks. We attribute it to the simple fact that it's incredibly lucrative for the criminals. That's partially due to the valuation of virtual currency, but it's partially due to the vulnerability of our systems and our infrastructure here that makes it profitable in both ways.

Mr. FRANKLIN. Thank you.

Director Inglis, the Colonial Pipeline attack caused major disruption at the gas pumps. There was talk about—concern about shutting down the energy grid. If something like that were to happen, obviously there would be mass chaos. It is not hard to think of other examples of attacking healthcare systems, where we could see a significant loss of life.

I know this isn't completely within your purview, but you also have a military background as well. In your view, when would such an attack rise to an act of war?

Mr. INGLIS. Typically, classically, the attack rises to an act of war when it achieves the same degree of damage that a kinetic weapon would achieve, the loss of health, safety, kind of national security of a significant nature. That being said, these are serious at any level and, therefore, requires that we respond fully with the remedies that are proportionate to that need.

We need to double down on resilience and robustness. We need to proactively defend these spaces, and we need to find and bring to justice the miscreants, the transgressors who conduct these actions.

Mr. FRANKLIN. And we talked earlier about the 16 critical infrastructure areas, and it is one thing to reach out to a foreign country like Russia and tell them "pretty please," you know, "please don't do these things," but should we be engaging in treaties or some sort of formal documents with other nations to establish those tripwires? You know, like a Geneva Conventions or something of that nature?

Mr. INGLIS. There was a global group of experts kind of sponsored by the United Nations in the 2015 timeframe that described norms that constitute reasonable expected behavior in this space. The United States signed onto those.

Just a week and a half ago, the Vice President in Paris announced that we would support the Paris Accords, which are a similar articulation of what is reasonable and responsible behavior in this space. They do not have the force, the effect of treaties, but

they clearly are recognized by like-minded nations as the way one should behave in this space and what the responsibilities of nations are in this space.

Mr. FRANKLIN. So, something like that would provide us cover and justification if violated. Then when we responded in kind, then we would have kind of an international support?

Mr. INGLIS. It has, for practical purposes, established what we would describe then as reasonable and appropriate behavior, and therefore, we are able to describe what is not.

Mr. FRANKLIN. Mr. Wales spoke earlier in his testimony of improving our incident reporting system. Should the definition of "major incident" change so that Congress is better informed when cyber-attacks occur against Federal agencies?

Mr. INGLIS. I think that we need to have a standard definition of what "major incident" constitutes such that we can uniformly, regardless of where an event might take place, inform the Congress, so those things that are truly major or, in some cases, significant. To your point, if those decisions are all made locally, then there's going to be a certain degree of inherent unevenness.

If we're going to operate with unity of effort, unity of purpose, we need to make sure that we have a common standard, a common definition, and that when and where appropriate—and there are various situations where that is entirely appropriate—inform the Congress.

Mr. FRANKLIN. Thank you, and I yield back.

Chairwoman MALONEY. The gentleman yields back. The gentlelady from Illinois, Ms. Kelly, is recognized.

Ms. KELLY. Thank you, Madam Chair.

As ransomware threats continue to spike, our response has been plagued by the challenge of hiring cybersecurity workers into the Government. As of August, there was a shortage of about 36,000 public sector cyber jobs across all levels of Government and about 1,700 of these were vacancies at the Department of Homeland Security.

Needless to say, it is essential for our Nation's cybersecurity that we fill these positions and ensure our cyber defense systems are operating at full capacity. The Department of Homeland Security recently made a dent in these cyber vacancies with a successful hiring initiative, which led to the onboarding of 300 new cybersecurity professionals and the extension of 500 additional offers.

Mr. Wales, what made the Department's cyber hiring initiative so very successful?

Mr. WALES. Thank you, Congresswoman.

This is a high priority for both CISA and the broader Department, and we've made hiring a really high priority for everyone. So just in terms of the past year, in Fiscal Year 2021, we hired more than double the number of new employees into the agency than we did in both Fiscal Year and Fiscal Year combined. So, we are making—making real progress.

In addition, just yesterday we announced the launch of the new Cyber Talent Management System, which used authorities that Congress had granted us a number of years ago to create a new system designed to hire cyber talent and give us additional tools to bring in to recruit and retain the best and brightest into the gov-

ernment when it comes to this space. We're really looking forward to using that over the next year to dramatically increase our ability to fill our ranks.

In addition, we are working hard to kind of broaden that pipe, work with—work with different groups, Girls Who Code, the Girl Scouts, just getting more people interested into this space, aware of the opportunities and to highlight the importance that this kind of work plays to our overall security. And we're working hard to look at bringing new groups to bear, whether that's working with community colleges and historically black colleges and universities.

There's a lot of efforts underway to grow that pipe and make sure that we can bring in the right diverse work force that is expected to solve the hardest cyber challenges. But I know Director Inglis has been working hard in the education and training space as well and may have additional points.

Mr. INGLIS. Congresswoman, I would simply add to that that, as you've indicated, leadership matters in this regard. This is not something that can be put on autopilot.

We need to revisit the definitions for these jobs to make sure that we've properly described what those skills are. I think we'll find that we opened some of these jobs to a much broader population. We need to appeal to the broadest possible population, use all methods, and then work as hard on retaining these people as we do at getting them onboard in the first place.

Ms. KELLY. So, the other thing that I always think about, the difference between public and private, of course, is compensation. It is extremely hard for the Federal Government to compete with outside private corporations. So, one proposal I put forward with Rep. Gonzales in the NDAA was creating a Cyber Digital Reserve Corps to bring in private sector talent to complete rotations at Federal agencies.

Director Inglis, how can the Federal Government overcome this compensation discrepancy so we can compete with others and get top talent?

Mr. INGLIS. Congresswoman, I quite agree that money is an important determinant when people select or kind of stay in jobs, but so is job satisfaction. So, in that case, I think we need to be competitive, but we're not going to pay the largest salary. The Congress has given many tools to the Federal Government that I think we can and should employ, and we need to work as hard at applying those tools uniformly across the government as we do at giving job satisfaction feedback to the people who take these jobs such that they stay on the merits of the sum of those factors.

Mr. WALES. Let me just add the new Cyber Talent Management System that we rolled out yesterday does include the ability to pay more competitive salaries, but as Director Inglis notes, we're never going to be as competitive as the private sector.

But the opportunity to work in the government, the opportunity to, one, serve your country and to do things in the cybersecurity field that you cannot do anyplace else, public or private, I think is an attractive opportunity for a lot of professionals in this space, and it's incumbent upon us to demonstrate that opportunity when we're engaging with audience and prospective candidates for jobs here.

Ms. KELLY. My other question was going back about attracting diversity, but you talked about that already. I don't know if you have anything else that you want to add.

And Mr. Wales, I hope the people that you send out to recruit have your—the passion that you just displayed about it. So, hopefully, we can—if they are like you, we will be able to get good people that want to work for the government, but I didn't know if there was anything else you wanted to add around the diversity piece?

Mr. WALES. The only thing I'll add is that increasing the diversity of our work force is one of the highest priorities for Director Easterly, and we are seeing the results of that in the new employees, particularly at the junior employees. We are growing that pipe of cyber professionals, and it's going to represent this country well.

Thank you.

Ms. KELLY. Thank you, and I yield back.

Chairwoman MALONEY. The gentleman from New Mexico—the gentlelady from New Mexico, Ms. Herrell, is recognized.

Ms. HERRELL. Thank you, Madam Chair, and I believe it is a very important hearing. I mean vital that we confront the threat of cyber-attacks on our government and critical infrastructure like the food industry and, of course, energy.

Director Inglis, as you know, earlier this year JBS faced ransomware attacks that halted production on the country's second-largest processor of beef, pork, and poultry. JBS supplies about 25 percent of the beef, about 20 percent of pork and poultry to the United States.

Concentrated control heightens the potential for severe disruption to our food supply, and it is vital that we mitigate against future risks. I actually think it is dangerous, in and of itself, to have 4 companies control 80 percent of the beef processing industry, but what I want to ask you is, Director Inglis, do you agree that such concentration of our food supply creates an additional risk to our Nation from cyber-attacks?

Mr. INGLIS. The concentration, of course, gives a concentrated target to those who would hold that at risk. That's not an unfair concentration if we make it sufficiently resilient and robust that it's either impervious or it's resilient, right, to those attacks.

And so, I think our first endeavor should be to take the systems that we have to make them more resilient and robust. That's a hardware problem, a software problem, a people issue, a doctrinal issue. Does an adversary have to beat all of us to beat one of us?

Make sure that we're then proactively defending those supply chains and that we're responding with all the instruments, to include government instruments, to any given incident so that we can quickly restore those systems to their proper function.

Ms. HERRELL. Great. And I thank you for that because I think—and you just actually answered my next question, which briefly would have been, you know, what is the administration doing to put protections in place so that we don't have a future threat to especially our food supply chains.

The administration is also considering shutting down Line 5, an oil and natural gas liquids pipeline that carries and transports fuels from Wisconsin to Michigan to Ontario. I think this would be

reckless and endanger Americans in the heart of winter, causing a surge in prices for heating and oil. This is an unnecessary danger to the American people, especially if we consider what is at risk when we have the cyber-attacks.

Rather than thinking about shutting down a vital pipeline, is the administration studying how to prevent future pipeline shutdowns like the Colonial Pipeline, the ransomware attack that occurred earlier this year?

Mr. INGLIS. I'll start, and I'll be happy then to defer to Deputy Director Wales, who I think there are some very specific programs at DHS. And the answer is yes.

Looking at the various critical infrastructure sector components to include pipelines, the government has stepped forward to determine what are the nondiscretionary features in hardware or software that are required to create defensible architecture. More recently, we've articulated what those should be for pipelines broadly, and I'll defer to Deputy Director Wales.

Mr. WALES. Thank you.

As I mentioned earlier, there's a number of activities underway specifically designed to address the cybersecurity risks in the pipeline area. Some of that is in response to the Colonial Pipeline incident. In its wake, the Transportation Security Administration released two security directives designed to improve the cybersecurity of critical pipelines throughout this country. So that required them conducting more detailed vulnerability assessments, so that required incident reporting to the Federal Government so we can more quickly take action in response.

In addition, on the natural gas pipeline side, there's a number of activities underneath a White House ICS initiative focused on industrial control systems. Those are the systems that operate the pipeline between cyber and physical, and CISA is a critical part of that.

There is certainly more work to do, and we recognize how critical pipelines are to the economic security and national security of this country, and it's why we're working in such close partnership with both industry and our government partners to provide more information, more expertise, conduct our own assessments, and make sure that our pipelines are as protected as possible.

Ms. HERRELL. Great. And I really do appreciate that, and I think Americans, you know, after seeing this happen earlier this year, the importance of protecting our assets, whether it is oil and gas or our food supplies—and you already kind of touched on this, but I was going to ask what are we doing to counter these attacks and how are we responding to protect our Nation's energy sector? But you just basically answered that.

So, I do appreciate your responses, and I appreciate you all being here. And Madam Chair, I will yield back.

Chairwoman MALONEY. The gentlelady from Florida, Ms. Wasserman Schultz, is recognized.

Ms. WASSERMAN SCHULTZ. Thank you, Madam Chair.

Ransomware attacks on critical infrastructure threaten essential services that Americans count on every day, whether it is timely access to medical care, safe drinking water, or affordable energy prices. In testimony two weeks ago, CISA Director Easterly said

that cyber-attacks on our critical infrastructure pose a serious risk to—and I quote—"the American way of life." And Florida is squarely in those crosshairs.

Attacks were launched in hospitals in Central Florida, leaving nurses and doctors with lost patient files. A hacker tried to dangerously spike the levels of sodium hydroxide. Thankfully, a savvy water treatment worker blocked it in time from causing sickness and death.

In one prolific recent U.S. attack, hackers targeted hundreds of schools, businesses, and government customers served by Kaseya, which was a Miami-based company. And that creates more than just a little economic stress. When Colonial Pipeline systems were breached in May, gasoline prices skyrocketed, and gas stations across the Southeast experienced fuel shortages.

So, it appears that various actors target critical infrastructure, including not only cyber criminals, but also nation-states and their proxies. Director Inglis, these attacks focus on high-stakes targets and large organizations that have robust security systems, but our committee's investigation found that even large organizations lacked initial points of contact with the Federal Government.

Right now, we seem to have a patchwork of Federal agencies that are focused on cyber threats. In your position, what are you doing to clarify roles and make sure that state and local governments and large nongovernmental organizations know who to contact and how they should respond to a cyber threat?

Mr. INGLIS. Yes, Congresswoman. Thanks for the question.

Appreciated the report that was issued by this committee today and the recommendations, the findings and recommendations in it, one of which was that it is essential that the Federal Government be joined up and coherent as individual citizens or organizations attempt to report or to seek service from that government. My office, as I indicated, has four broad outcomes that we should be held accountable for.

The first of those is Federal coherence. Not simply in how we manage our own digital infrastructure, but how we support and respond to support the defense of critical infrastructure. Despite the fact the Federal Government is quite diverse, that can be brought to bear as a strength if we're joined up, and you report that incident to one of us such that all of us then understand it and can bring all of our various authorities and resources to bear. That's the goal, and that's what we should be held accountable for.

Ms. WASSERMAN SCHULTZ. But that doesn't really answer what you are doing to clarify the roles and make sure that state and local governments and large NGO's know who to contact and how they should respond to a cyber-attack.

Mr. INGLIS. So, let me give you some specifics then on that. Since the office was created—and funded yesterday. But since the office was created, I've worked very closely with the Cybersecurity and Infrastructure Security Agency, CISA, to ensure that they had the necessary inputs from the various sector risk management agencies. Those are classically the Federal entities that deal directly with the critical infrastructure—Department of Energy, Department of Defense, so on and so forth—such that if you reported at

the interface of one of those critical sectors to some part of government, CISA would receive that.

In the same way, I have worked with CISA to ensure that as they synthesized and got that big picture that that was then disseminated out broadly, right, to all of the respective organizations so that if the government knows something in any particular place, the government knows it in every place. And more importantly, that we push that proactively to the beneficiaries.

That work is not complete, right? It is a very diverse and it grew up as of various—as they said, of various and separate stovepipes. But that's the work before us. That's what we've been doing. I spend arguably half of my time on that issue alone.

Ms. WASSERMAN SCHULTZ. Thank you. I appreciate that specificity.

I also want to followup on a response to Chairman Connolly's question about the Federal Government's position on ransom payments.

Assistant Director Vorndran, as you know, cyber insurance policy will typically cover the costs associated with a ransomware attack, like hiring incident response consultants, bringing data system back online, and covering interruption losses. But some policies can even cover ransom payments.

Given your stated position on ransom payments, what would you recommend to local and state governments when they are making a decision about whether to purchase cyber insurance policies to cover losses related to an attack?

Mr. VORNDRAN. Thank you for the question. That's a challenging space for me to venture into in my job and within the organization I represent.

But what I would say is simply that those same local governments need to understand their risk calculus and where they are in their maturity of net defense and resilience and how much time they would be able to take to legitimately bring all their systems back online to have a functioning state or local government. And based on the totality of that analysis, that should drive whether they do or don't want to buy cyber insurance.

Ms. WASSERMAN SCHULTZ. Thank you very much. Madam Chair, I yield back the balance of my time.

Chairwoman MALONEY. The gentleman from Texas, Mr. Cloud, is now recognized.

Mr. CLOUD. Thank you, Chair.

A lot of our discussion today, and rightfully so, has focused on a number of the cyber-attacks against national, big national interests, Colonial Pipelines, some of our insurance companies, meat packing plants, and the like. I wanted to focus a little bit on some of the rural counties.

A lot of the district I serve is rural. We have had at least two communities affected by attacks against them, Ingleside and Jackson County. And Jackson County, for example, has a population of about 14,000. There is three incorporated cities. May 28 of 2009, they experienced a cyber-attack by hackers using the Ryuk ransomware. Servers were disconnected. Data backups were compromised. The system shut down, and the hackers demanded

$362,000 in bitcoin, which for a rural community like that is a lot of money.

They were able to—the state of Texas responded, and the Texas military department cyber incident response team, along with the Texas Department of Information Resources and It contractors, were able to accomplish about what they say is six months of work in about 15 days and clean and reimaged 85 old machines, brought 31 back onboard. Anyway, they were able to recover, but it was at a bit of a cost.

What tools or programs are currently available to these municipalities to assess their current systems and develop and implement plans to address vulnerabilities before they are attacked?

Mr. WALES. Sure. So, I'll start. I mentioned earlier there's a number of services and resources that are available for our state and local communities, including rural counties. A number of those are offered at no cost, either from CISA directly or through the Multi-State ISAC that was designed and set up under a cooperative grant from CISA to support the state and local governments.

Some of that includes assessments. Some of that includes actual technology that will detect and block activity on those networks. And some incident response support, should they need it.

I think Congress has also spoken, and with the recently passed infrastructure bill, there will be additional resources available. The state and local cybersecurity grant program that was established by Congress in the infrastructure bill has a specific amount of money that's designed to go to rural communities. And so, it's designed to kind of get to some of those challenging areas that you've identified and provide additional capabilities that could help them protect themselves.

In addition, the infrastructure bill established a Cyber Response and Recovery Fund. It's starting small. This would be the first time that we're going to be utilizing it, and it is a way to help in the face of significant cyber incidents, a way for the Federal Government to surge resources to respond and recover from those—from those incidents.

And so, we are looking now about the standup of both of those programs and identifying how exactly we will work with our state and local colleagues to get those off the ground, what will be the policy and parameters around getting that funding available. But in the case of the grant program, it's going to ride on FEMA's existing processes, and so they are good about getting that money out to local communities, and we're working in close partnership with them in its standup.

Mr. CLOUD. OK, thank you.

Director Inglis, it has been mentioned already, but I would like to submit for the record this article, "Biden Tells Putin Certain Cyber Attacks Should Be Off Limits." And just the logic behind this and us listing 16 areas that are off limits really does open up the door from a messaging standpoint that everything else is on limits. Notably, these rural counties, you know?

And I would just suggest, if you can take the message back to the White House, that we should be having the message that all cyber-attacks are off limits and that we need to be standing strong on that, it would be certainly greatly appreciated.

Mr. Vorndran, I wanted to ask you about our talent pipeline because it seems to us that, you know, we are in competition globally with other nation-states, and it is extremely important that we have this talent pipeline and that we manage the resources within our cyber entities and the FBI. Could you speak to how we can develop the pipeline? And Mr. Wales, you may need to speak to this as well.

But also, if I could just say this, I would submit this for the record, too. "AG Garland Refuses to Rescind Memo Asking FBI to Probe School Board Threats."

Now as we sit here and talk about real nation-state threats and then we see news like this, and then we are asked to give more resources, you all are coming here because you would like more resources, which there is bipartisan support for, no doubt. We need to firm up our cyber. It is a critical defense mechanism for our Nation.

But when we see resources in our intelligence agency being dedicated to probe—to investigate parents at school board meetings, it really makes it hard to, you know, just blatantly just give more money to these sort of resources. So, could you speak to the talent pool and then using the resources of our intelligence agency and cybersecurity apparatus?

Thank you.

Mr. VORNDRAN. Sure. I think I'm going to stay really squarely focused on one topic. Within the Department of Justice and with the FBI, we are different from DHS and CISA and different from DOD and NSA, that we don't have a special pay scale for our cyber talent. So, what DOD through NSA and what DHS through CISA can pay someone who's 22 years old coming out of college with a computer science degree far, far outpaces our scale by approximately 50 percent. And that is a very, very significant concern of ours moving forward.

Mr. CLOUD. In the private industry, too.

Mr. VORNDRAN. Yep. We do believe that once we have people in the door that we can retain them well, and our numbers indicate that. Our retention rate is well over 99 percent, and it has been well over 99 percent. But the key is how do we attract that talent, especially the technical talent, and right now, our biggest gap is the pay gap when we compare directly to our counterparts in Federal Government.

Mr. CLOUD. And to the question of resources being used to investigate parents instead of going to other actual national security threats?

Mr. VORNDRAN. Sir, you know that I can't comment on that. That's a memo that was issued by the Attorney General, and I'm here to represent the FBI Cyber Division.

Mr. CLOUD. So, is the FBI taking it seriously, the memo from the AG or not?

Mr. VORNDRAN. Sir, I'm not in a position to answer that question. I'm sorry. What I can tell you is that our Cyber Division uses our resources very, very squarely on cyber threats.

Chairwoman MALONEY. The gentleman's time has expired. The gentleman from Illinois, Mr. Davis, is recognized for five minutes. You need to unmute, Mr. Davis.

Mr. Davis, we can't hear you. You need to unmute.

Mr. DAVIS. Thank you, Madam.

Chairwoman MALONEY. OK.

Mr. DAVIS. Thank you, Madam Chairman.

This hearing is focused on the need for the Federal Government to marshal all of its resources to strengthen the Nation's cyber defenses against ransomware attacks, led by National Cyber Director Chris Inglis and CISA Director Jen Easterly. But the success of our entire ransomware policy won't be completely determined by decisionmakers in government buildings. It will also be determined by decisions made in company boardrooms, by businesses, or even our local school boards.

Director Inglis, you have previously stated, and I quote, "We need to increase awareness so that every citizen, every person who experiences cyberspace has what is necessary to cross the digital cyber street in the same way that we teach children to cross actual streets."

Of course, large corporations have entire departments dedicated to IT, whereas small businesses and individuals typically use off-the-shelf IT products and have minimal expertise in cyber defense. Director Inglis, how important is broad-based education and outreach to improving our Nation's cyber defenses, and how can we effectively communicate this need to individuals and organizations of all sizes?

Mr. INGLIS. Congressman, thank you very much for the question.

I stand by those previous remarks. I would say that it's very important to get the people piece of this right. A definition that I like of what cyberspace is, what "cyberspace" the noun is, of course it's technology. But it is also people, not simply kind of people being served by cyberspace, people are in cyberspace. The decisions they make determine the operation of cyberspace. And then, finally, doctrine. How do we get the roles and responsibilities right?

Two of those pieces, people and doctrine, depend fundamentally upon people understanding how cyberspace works, what their roles are in cyberspace, and who's doing what in cyberspace, who's accountable to defend what under what circumstances. That's not simply something that people who have the word "cyber" or "IT" in their job title need to get their head around, everyone. Everyone could be that strongest link or that weakest link on the front lines of cyber.

How do we do that? Broadly, I think there needs to be some sense of accountability of what individuals are accountable for, organizations accountable for, the private sector, the public sector. There's an increasing awareness of that. A reduction in complacency of this is somebody else's problem, that somebody else will handle what mistakes I make. We need to each feel some degree of accountability, and training and awareness at the earliest possible level.

I've suggested in that quote that you gave that we do that in kindergarten, right? At the earliest possible moment that someone is brought into contact with cyberspace, we need to teach them the ins and outs of that inasmuch as we teach them how to navigate a hot stove or a busy street.

Mr. DAVIS. Thank you very much.

The National Institute of Standards and Technology Cybersecurity Framework provides five key functions that form the backbone of good cybersecurity—identifying risk and assets, protection of data and systems, detection of attacks, response, and recovery. CISA Director Easterly previously testified that 90 percent of successful cyber-attacks start with a phishing email and that multifactor authentication would reduce chances of successful attacks by 99 percent.

Mr. Wales, do you see organizations not investing enough attention or money to guard against ransomware attacks, and if so, please explain.

Mr. WALES. So, I think, as you would expect, the implementation of sound cybersecurity practices will vary significantly across industry. There are small businesses that are going to be well protected, and there are large businesses that are going to have—that are going to have significant holes. We feel like it is our responsibility to help raise that baseline of cybersecurity by highlighting the key things that need to be done by everyone, get us to that right baseline of cyber hygiene where things like multifactor authentication is widely used, where privileged accounts, those that can actually affect the operations of a network, are well protected and limited in use, that people are keeping up with their patching, identifying vulnerabilities.

We've continued to hit and promote these. As I mentioned in my opening statement, we recently finished Cybersecurity Awareness Month in October, and we were extremely focused on trying to raise the awareness of the importance of multifactor identification on all accounts, but in particular those accounts with higher privileged access.

You know, it's not going to be enough. There are still going to be companies who are not focused on this problem or who will not focus on it until it's too late, until after they're hit. And I think we need to do everything we can across the U.S. Government and in partnership with the private sector to raise the awareness, highlight the best practices that should be used, highlight the bad practices that should be avoided, and make sure, as Director Inglis notes, that the right individuals and organizations are held accountable.

Mr. DAVIS. Let us say that I am a small business owner without a dedicated IT staff. Where should I focus most of my attention and resources to protect against ransomware attacks? Is it prevention, or what should I do?

Chairwoman MALONEY. Your mic, please. We can't hear you.

Mr. WALES. Congressman, we actually released on our StopRansomware.gov website a list of what we call "cyber essentials." What are the first things you should do when putting in place more effective cybersecurity?

I think, as you've highlighted, implementing multifactor authentication at scale is among the first steps you should take, but we've actually walked through a series of steps that small and medium-sized businesses can and should do to make sure that their level of cybersecurity is appropriate for the risk that they're facing.

Mr. DAVIS. Thank you very much. Thank you, Madam Chairman.

Chairwoman MALONEY. All right. Thank you so much. The gentleman from Georgia, Mr. Hice, is recognized.

Mr. HICE. Thank you, Madam Chair.

Mr. Inglis, last year, when Congress was debating whether or not to create your position, the National Cyber Director, there were some concerns that we were just going to be creating yet another layer of bureaucracy. So, if you can, help me understand within the context of what we are talking about today, ransomware, what role does your office play?

Mr. INGLIS. Sir, thank you for the question. If I might put that in the context of describing three roles, my role being the one you asked about.

In the context of ransomware, my job would be to ensure that the various instruments that the Federal Government can bring to bear are deployed in a way that they are concurrent, that they're useful, that they're complementary. Therefore, to be proactive and concurrent foremost in mind.

We have talked at some length in this hearing about the roles of sector risk management agencies like the Department of Energy, the Department of Defense, about the roles of the FBI, about the roles of CISA. My job is to ensure that those are applied and they are applied in a way that's concurrent. And looking back at the government, you don't need a Ph.D. in government to essentially deal with the government.

The second broad role that I would then describe is the role of the National Security Council, which outside of cyberspace is accountable to use all the instruments of power that this Nation can bring to bear—diplomacy, intelligence, military resources, financial resources, sanctions that might be applied—to bring about the proper conditions in all domains, not least of which is cyberspace. And so that role is also important.

And then the third role is those discrete, individual roles of CISA, the FBI, sector risk management agencies, all of whom need to within their lanes do what they do, again, in a way that's complementary, concurrent, coherent such that the sum of those parts is much greater than its arithmetic sum.

Mr. HICE. So, it sounds like the buck stops with you insofar as ransomware is concerned for every agency of the Federal Government. Would you or do you set Federal policy?

Mr. INGLIS. The buck does stop with me in terms of the performance of the Federal Government. I'm not entirely kind of capable of setting the Federal policy, often which is dictated by law or existing statute. But to the extent that we need to adjust the various roles and responsibilities and relationships, I'm the accountable person.

Mr. HICE. OK. So, as it would relate to whether or not, just as an example, we are going to withhold encryption keys from victims, as it appears the FBI has done, what role or policy would you have in that decision?

Mr. INGLIS. I should be involved in that decision. I wasn't, of course, on scene at the moment that that particular decision that we refer to in this hearing was made.

But I should be—I should be at the table for that decision. There are other factors that come into play in terms of making a deter-

mination about a decision of that sort, but I should have a huge influence on that.

Mr. HICE. OK, let us talk about those other factors. What other variables go into a decision of that nature?

Mr. INGLIS. So, let us take that incident again. I wasn't there. So, I will just kind of observe from the distance that I enjoyed.

Mr. HICE. Well, the buck now stops with you. So, what kind of variables would go into making that kind of decision with you at the helm?

Mr. INGLIS. Two. There are two variables. The one that is not variable or at issue is a desire by the Federal Government to achieve the greatest, broadest possible disruption, right, of the threat that's being held against the United States or its citizens.

The variables in that are how timely and how broad, right, can you be in the application of that disruption? If you're timely in the extreme, meaning that you disclose the moment you understand some insight into what the actors are doing, then you might give them the opportunity to escape kind of with their ill-gotten gains and to recover and to repeat that experience on another day. You might not know enough about the nature of what they've done such that you can disrupt it more broadly.

If you wait too long, such that you take it down in a strategic way, you've allowed too many victims to fall kind of victim to that. So, the alignment has to be made between timeliness and breadth, but there's no question that disruption is the goal.

Mr. HICE. OK. That doesn't really answer the question in terms of variables when it comes to making a decision about withholding encryption keys. You are talking in broad principles. If you would, I appreciate if you could give me a more detailed answer in writing.

Mr. Vorndran, I want to go to you now. The FBI certainly has had some credibility issues in the past years, recent years, but overall, I believe Americans look at the FBI as a source of confidence as it relates to the cyber area. And yet this past weekend, at least as reported and appears to be accurate, that thousands of spam emails masquerading as FBI were sent to state and local officials warning them of a phony cyber-attack.

So, can you explain to me now how this event does not raise somehow more questions regarding the veracity, the veracity, the accuracy of FBI alerts in the future?

Mr. VORNDRAN. Sir, I'm not sure I understand your question, but let me do my best to answer. Certainly, this weekend, you know, what has been——

Mr. HICE. Let me clarify the question because I don't want you beating around the bush. I want to hear a direct answer as much as possible.

The question has to do with the phony emails that went out from the FBI warning of a phony cyber-attack to state and local officials. That being done, how can the accuracy of future emails from the FBI be depended upon from state and local? How are they going to know what is real and what is not real if your own cyber has been hacked?

I just want to make sure we are protecting state and local officials, how they know what is coming from the FBI is accuracy if what we saw last week, this past weekend happens again?

Chairwoman MALONEY. The gentleman's time has expired, but the gentleman may answer the question.

Mr. VORNDRAN. Sure, no problem. Sir, that is an isolated incident that you're referring to that happened this weekend. We know specifically how it occurred. We also know that no FBI data, no personally identifiable information was compromised.

That software application and hardware, associated hardware was taken immediately offline. So, we consider the incident contained, and we don't think it'll impact any future communications coming out of that email server.

Mr. HICE. I yield, Madam Chair, but that did not answer the question as to how people can rely upon the FBI's information in the future, totally evading our question, and I would like an answer.

Thank you.

Chairwoman MALONEY. The gentleman's time has expired. The gentlelady from New York, Ms. Ocasio-Cortez, is recognized.

Ms. OCASIO-CORTEZ. Thank you so much, Madam Chairwoman.

Director Easterly, your team looked some of the excess death data during the ransomware attack on University of Vermont's health network. I was frankly quite surprised by the conclusion of that case study that ransomware attacks on hospitals are correlated significantly with loss of patient life.

Now, briefly, how is it that these ransomware attacks have that kind of impact?

Mr. WALES. Congresswoman, that study looked broadly at excess deaths during COVID, during the COVID pandemic, largely looking at what happens when hospitals are overwhelmed with ICU patients suffering from COVID. What were the number of excess deaths from other—from other types of needed hospitalizations or ICU admittances? So, there were excess deaths from things like heart attacks and cancer, et cetera.

We were highlighting during the course of that study that ransomware incidents have the potential to exacerbate the strain on hospitals and result in additional excess deaths, and that is why it is incumbent upon hospital administrators to make sure that they have the right level of cybersecurity in place and they are aware of the potential for significant—they're prepared for what might happen should their hospitals be overwhelmed by cyber or other disruptions.

And it is why we are working so hard to kind of highlight the results from that work and, additionally, what we can do to offer additional assistance to hospitals across the country as we've been doing over the course of the COVID–19 pandemic.

Ms. OCASIO-CORTEZ. Thank you.

And you know, as I understand it, the victims of ransomware attacks, including institutions like hospitals, are often reluctant to admit that they were targeted, and sometimes they just pay this ransom and try to essentially not report it. But just to confirm, and again, very briefly, Director Vorndran, paying ransoms to cyber criminals instead of reporting it out and working with the government does not necessarily guarantee that that data will be decrypted or that their systems will be secure. Correct?

Mr. VORNDRAN. That's correct. There are no guarantees that if any corporation, organization, or entity pays ransom that it will necessarily be decrypted. We have use cases between us and CISA where the decryption keys provided by the actors have not worked.

Ms. OCASIO-CORTEZ. Mm-hmm. And Director Easterly, currently the House is seeking to pass the Build Back Better Act. Now, among other things, this bill includes more than $400 million for your agency, the Cybersecurity and Infrastructure Security Agency. Now in concrete terms, can you help communicate to us and to the public what that $400 million would allow your agency to do, and what kind of capacity and what sort of implementation does that buy, per se?

Mr. WALES. Sure. So, Congresswoman, there's a number of provisions in there that deal with cybersecurity beyond CISA, but I'll focus on the provisions that deal with our agency and the additional funding that it would potentially provide. And I think there's a number of initiatives there that go to a series of concerns that have been raised by members during the course of this hearing, particularly related to the security of our critical infrastructure and the industrial control systems that enable our infrastructure to operate.

There is money in there that will help us expand our ability to monitor and detect activities that are actually happening on critical infrastructure networks and take quicker action in response. There is money in there for research and development focused on the critical infrastructure domain and the industrial control systems to identify new and emerging ways in which we can detect and protect those critical assets.

There is funding in there for expanded training and education that go to a number of the topics related to work force that we've hit on. So, I think that there is a series of provisions that will certainly help bolster our ability to provide support to the cybersecurity of this country.

Ms. OCASIO-CORTEZ. Thank you very much, and I yield back.

Chairwoman MALONEY. The gentleman from North Carolina—gentlelady from North Carolina, Ms. Foxx, is recognized.

Ms. FOXX. Thank you very much, Madam Chairman.

I thank our witnesses for being here today, and I have a question for Executive Director Wales and Director Ingles—Inglis. Pardon me, Inglis.

We know that ransomware attacks can be devastating. To further complicate the effects of an attack, healthcare entities face additional requirements because their data can include protected health information that is covered by HIPAA.

Entities covered by HIPAA are required to report a breach of protected health information within 60 days of the discovery of the breach. However, it can sometimes take several weeks of forensic investigation after a ransomware attack to discover if protected health information was compromised.

There is pending legislation that may require the reporting of a network breach to the Department of Homeland Security. Since healthcare entities often need time to discover the protected health information was compromised, are there plans to address the interagency communication so that the Health and Human Services Of-

fice of Civil Rights 60-day countdown does not begin when the ransomware payment is reported to the Department of Homeland Security, but rather once the healthcare entity has determined that a breach of protected health information has occurred?

Mr. WALES. Ma'am, obviously, there's a number of different versions of the cyber incident reporting legislation that are moving around. They will have somewhat different responsibilities for the degree of regulatory harmonization that may be required because, obviously, there's a number of other regulators that require incident reporting from our critical infrastructure and the financial sector and the energy sector and others.

Part of that legislation that we've seen would require CISA to work with those agencies if we are implementing our regulation. Part of it would require once information is reported in to them, it be further reported to us within 24 hours once they get that information. But it's a little too hard to say in terms of what will be the final passage of the bill.

We're still working closely with relevant congressional committees on that legislation, but I can assure you that our goal, working with Director Inglis and others, will be to ensure the maximum harmonization of those various regulatory requirements. But that will take some time to work through.

Ms. FOXX. Thank you.

Mr. Inglis, do you want to add anything?

Mr. INGLIS. I would simply add, additive to the comments made, is that I think most of these bills have a rulemaking period such that the bill is not implemented immediately upon passage, but after some months, in some cases as much as two years afterwards, after there is a kind of full consideration of the concern that you raised and others.

Ms. FOXX. Thanks.

Mr. Wales, attracting qualified workers is a challenge facing every sector in America. With regard to cybersecurity, are there enough qualified workers for you to hire at CISA?

Mr. WALES. You know, that question is kind of hard. We're not hiring them in a vacuum. We're hiring them in an environment where there is intense competition for top cybersecurity talent, and we are doing a lot to try to recruit and retain the cyber work force that we want.

And I touched upon some of those issues earlier, but I do think it is essential for the Nation that we grow the pipeline of people who are focused in this area. It is not going to be enough to just look at the people who are available today. We need to think about what the needs are going to be in the future, and to do that, we are going to need more people who are interested and focused on this area, willing to devote themselves to the cybersecurity field and get involved.

And whether that's at the Federal Government level, a state and local government, or in the private sector, in academia, in the research and development community, in security research community, we need people in all of those areas. And so, we really need to grow that pipeline. We've got initiatives to do it, but it's going to take really a whole of nation effort to make sure that we have the talent required.

Ms. FOXX. Well, Chairman Scott and I are trying to work on the Workforce Innovation and Opportunity Act, and if you have specific suggestions, I am sure we would be happy to have them.

Director Inglis, cybersecurity is not an issue that people often think about until there is a problem. Does society need to treat cybersecurity with more urgency, or should strengthening cybersecurity be the role of the private sector and the government rather than citizens?

Mr. INGLIS. Thank you for the question. It's a wonderful question.

I don't think that cybersecurity, at the end of the day, can be completely shopped out to kind of a group of experts who build, operate, and defend the infrastructure independent of the people who actually are served by the infrastructure. As I'd indicated earlier, people are not simply served by cyberspace, they're a part of cyberspace.

Individual choices that are made by ordinary users who depend upon it to conduct their livelihoods or their personal affairs or businesses, those choices are actually reflected in the weaknesses or the strengths of cyberspace. Therefore, everyone must be involved, and we need broadly a campaign for awareness and some degree of awareness and training that then equips people so that they can fulfill the roles that they need to as individuals, organizations, or sectors.

Ms. FOXX. Well, again, I would invite you, if you have some suggestions on how we can enhance our national cybersecurity that you don't have a chance to talk about today, I hope you will share those things with us.

Mr. INGLIS. I would welcome the opportunity to engage you and your staff.

Ms. FOXX. Thank you very much. I yield back, Madam Chair.

Chairwoman MALONEY. The gentlewoman from Michigan, Ms. Tlaib, is recognized.

Ms. TLAIB. Thank you, Chairwoman.

Thank you all so much for being with us.

If you work at an organization that is successfully hit with ransomware attack, this is an example of the kind of ransom note you might find on your computer system. This is a ransom note left, I believe, by a cyber-criminal group called REvil that is behind some of the most prominent ransomware attacks of the past few years, including those on software provider Kaseya and the meat marketing process, JBS Foods.

This note reportedly was part of Kaseya's attack and was deployed against some of their customers. There is a lot of information, as you all can see on here, on this page. But I want to focus on the line that says you have two days. Right under that deadline, it says you pay, you know, $5 million ransom, and it says, quote, "If you do not pay on time, the price will be double."

So, Mr. Wales, you know, this is fairly a common ransom tactic used by attackers, put pressure on its victims to pay quickly. Correct?

Mr. WALES. I think my colleague from the FBI can probably describe this in a little bit more detail, but that is generally, yes. I

mean, this is what cyber criminals are going to do to try to extort money out of victims.

Ms. TLAIB. And so, does the FBI—would you like to comment in regards to that? Because I think the timeline and like the counting down——

Mr. VORNDRAN. Sure. I appreciate the question and appreciate the opportunity.

Certainly, to Brandon's point, we would agree with that. You know, the bottom line is, it is an extortion tactic that is heavily leveraged based on time. We have unique data in our holdings based on the number of these that we worked that show how long we can potentially negotiate and what type of reductions, and that's information that we're happy to share with victims should they get hit by a certain ransomware variant.

Ms. TLAIB. You know, Assistant Director and Mr. Wales, I mean, part of that threatening is not just a deadline and doubling, but they also threaten to like leak the stolen data, make news of the attack public, or destroy the key to pressure—make victims pay, right? So, you know, Assistant Director, in your view, I mean, should companies pay the ransom immediately?

Mr. VORNDRAN. Let me split that question into two, right? Ransomware groups are moving to a double extortion model where they exfil data, and then they hold it, and then they encrypt. The exfil data is used as additional leverage for a double extortion option for them, to hold additional leverage over the company or the affected organization.

So, our position on paying ransoms has remained the same, which is this. We do not recommend paying the ransom because it fuels the criminal enterprise, but we do understand that it's a business decision for any corporation or entity about whether to move forward with paying that ransom. The only thing that we would collectively ask, as the Federal Government, is that we be notified as soon as possible when that ransom is paid so we can do our best to track the money.

Ms. TLAIB. Director Inglis, one of the things that I find here in Congress in the three years I have been here is there seems to be always emphasis on new laws and criminalizing, right, when we already, I believe, have some strong legislation now on these types of attacks and criminal activity. Do you think that it is really about resources and more funding and investment in enforcement, or do we really do need new legislation to try to attack this?

Mr. INGLIS. Thank you for the question.

I think that your question goes to the heart of the matter, which is that we need a comprehensive approach. We need to double down on investing in resilience and robustness across technology, people, making sure they have the right skills, and doctrine, making sure we've got the right roles and responsibilities.

Do we, in fact, make it such that a transgressor needs to get past all of us to get at one of us? We need to make sure that we double down on the proactive defense of these systems to detect an anomaly at the earliest possible moment, which then if we fail in those first two pieces, which should have a determinative effect, we're left with responding to an incident and perhaps chasing, finding the criminal, bringing them to justice.

But if we only did that third bit, right, we would find ourselves in an impossible tail chase. So, we have to do all three of those.

Ms. TLAIB. And you know, Director Inglis, I mean, one of the things that I know happens even in the kind of local government in trying to enforce that, is there—is there a way to measure, you know, OK, we invested this much in your department or division, and the result became—you know, are we able to really track that? That the result of investing, you know, in Build Back Better, what we have is millions of dollars investment in combatting this issue. How are we going to be able to measure like it is actually working so that colleagues can see that we need to do more in this way instead of just continuing——

Mr. INGLIS. Yes, that's a great—that's a great question, too.

During my time in the private sector, I was often asked the question of how much money do you need to properly defend this organization, cyber defend this organization, which is typically not the best first question. The best first question is do I understand what the role that digital infrastructure plays in my business? Is that an appropriate role? Am I taking risks that I don't want to actually spend time and money to secure because it's not a risk that I think is worthwhile?

Have I balanced, right, my risks such that I've done the necessary preparation? It's resilient and robust. Am I actually following what the system is actually doing such that only that last bit of then can I detect an anomaly, some transgressor inside the system?

You have to first then think about what the purpose of the system is, have you balanced your investments across that? If you've done both of those things, then you can ask do I need further dollars to buy down risk attendant to something that I have determined is an essential risk, and I've determined I haven't been able to secure through resilience, proactive defense, or pursuit.

Ms. TLAIB. Well, thank you so much. Very insightful.

I yield.

Chairwoman MALONEY. Thank you. The gentleman from Wisconsin, Mr. Grothman, is recognized for five minutes.

Mr. GROTHMAN. Thank you.

First question, this is for Mr. Inglis. As I understand it, there was recently a cyber incident in an important part of government, and it took your agency quite a while to become aware of it. It wasn't reported to your agency for quite a while. Is there any reason why agencies are apparently afraid or hesitant to share information with you, or without—could you give me a general, your general opinion of that incident?

Mr. INGLIS. Yes. So, if I recall the incident that you refer to happened in late July. I think that we came forward to the Congress, the Federal Government came forward to the Congress in mid-August to describe the nature of that incident, what we were doing about that. Is that the one, sir?

Mr. GROTHMAN. I believe so, and I believe your agency was not made aware right away either.

Mr. INGLIS. We were not. But my agency didn't come into being until I showed up on the 12th of July. So almost coincident with

the incident that ultimately was revealed as being, we believed, significant. And I think there's a couple of challenges here.

One is that there are hundreds of things that happen in a system every day that might be constituted as anomalous. It's not something you would have expected. It's something that may, in the end, simply be a simple anomaly, a bit flipped the wrong way. They're not all cyber events that rise to the level of significant or major.

And therefore, it's almost impossible instantaneously to determine what's major, what's not. Those often take time. A transgressor doesn't always reveal, right, their methods on that first day. So long story made short, it might legitimately take two or three weeks.

The challenge, though, in that particular incident was that you had an agency that determined that something had happened. It had understood that this was in the context of a lot of other events taking place and determined on its own merits that this didn't meet the kind of level of major or something that should be reported.

Quantitatively, right, the statistics that they cited were appropriate, and therefore, it was a reasonable decision locally. But looking more broadly across the Federal enterprise, what we determined when we became aware of that in the middle of August was that this was an incident that could have happened in other places. We need to take that signature and check those other places, which we did, and it was something that in the longer term, the longer scheme, required an investment to make sure that we prevented this from happening again.

My long story made short is that the context matters greatly. And the fact that it took 2, 2 1/2 weeks to get to me is not something I find terribly surprising. We need to be quicker on the draw. We need to reduce noise to kind of information that matters. We need to even—we make it even and perhaps level set across various agencies and departments that we come to the same repeatable, defensible answer day after day after day. That's the scheme that we're implementing at this moment.

Mr. GROTHMAN. I was just a little bit concerned that they didn't report to you quicker.

Next question. You know you can tell by the discussion here today that people talk about China or Russia or North Korea, Iran. I guess without identifying those countries, because I can imagine why you wouldn't want to, do you feel that is a comprehensive list of countries you have to worry about here, or are there other countries that you believe should be of concern as well?

Mr. INGLIS. I think we have a pretty clear understanding of which nations hold us at risk in and through cyberspace, if that's the question, sir.

Mr. GROTHMAN. OK. And do you feel that is a comprehensive list?

Mr. INGLIS. I think that we know what that list is, and the names that you mentioned are on that list.

Mr. GROTHMAN. OK. And presumably, other countries as well? I guess that is the question.

Mr. INGLIS. The good news is there are few. The bad news is there are more than one.

Mr. GROTHMAN. OK. Should we be concerned that al-Qaeda or ISIS would be planning an attack like that? Do you feel they have the means to do it?

Mr. INGLIS. I would say that there are any number of entities or organizations or nation-states in the world that have the ability to hold cyberspace, cyber infrastructure at risk. We've been discussing this morning a variety of individuals who operate in the safe havens near Russia that have held us at risk. And so, I would say that al-Qaeda, ISIS, anyone who places time and attention on the development of cyber methods could hold us at risk. We don't at the moment discern that that is at this time a risk from them.

Mr. GROTHMAN. OK. And that would include countries adjacent to or I guess Afghanistan is right now kind of a little bit of a hodge-podge. But would you say that, say, the successor governments or groups operating in Afghanistan would perhaps be a problem?

Mr. INGLIS. I'm worried about any collection of individuals that would have a low cost of entry and some ability to develop talent that could hold us at risk. Again, we have been describing this morning a number of individuals who have formed themselves into a syndicate who held this Nation and other nations at risk using the scourge of ransomware. We are not powerless to prevent that if we increase the resilience and the robustness of our systems and we proactively and collaboratively defend those systems.

Mr. GROTHMAN. Thank you.

Chairwoman MALONEY. Thank you. And the gentleman from California, Mr. DeSaulnier, is recognized.

Mr. DESAULNIER. Thank you, Madam Chair. Thank you for having this hearing.

Thanks for the witnesses for your testimony.

I wanted to talk a little bit about healthcare organizations and specifically hospitals. A recent report surveyed 600 healthcare organizations and found that as many as 40 percent of them were targets of these types of attacks. And at least in one instance, there was a loss of life, an infant lost their life. Extended stays in hospitals are a normal response to surveys because of these attacks and an undetermined as yet cost to our healthcare system.

Mr. Wales, maybe you could talk to us a little bit about why healthcare systems, and hospitals specifically, are so vulnerable?

Mr. WALES. Sure, Congressman. You know, we've had one of our senior health analysts described hospitals and a number of other sectors as target rich and resource poor. And ones that are the focus of adversaries because they believe that they have a soft underbelly and that in the case of ransomware that they would be willing to pay to get that hospital back up and running very quickly.

On the other hand, they don't necessarily have the resources and capabilities to devote to enhancing the cybersecurity matching the degree of risk that they are facing. That is why I think that we've been trying over the course of the COVID–19 pandemic to try to make sure that as hospitals became increasingly fragile, being overwhelmed with COVID patients, that we were able to kind of

surge cybersecurity support to those entities, get them loaded into some of the free services we offer.

But frankly, that's only scratching the surface. There is a lot more that we need to do to make sure that hospitals are as protected as they need, given the potential for disruptions there to have really significant consequences on both the communities as well as the patients within those hospitals. You know, this is an area where there's a lot more work that's needed. I'm not here to pretend that what we've done is nearly enough. This is going to be a constant focus for our agency in the years ahead to match the level of risk that's out there.

Mr. DESAULNIER. Well, I would love to work with you more, and I am sure there are many people in the Congress who would like to work with you more. Having had a healthcare experience and having been in an ICU for a long time, this infrastructure is obviously really important, and there should be a sense of urgency, as you say, coming out of COVID, both for the clients, the patients, but also for the staff.

Assistant Director Vorndran, could you tell us about specific organizations that are targeting our healthcare industry and hospitals that you are aware of?

Mr. VORNDRAN. Sir, if I understand your question correctly, you mean which ransomware variant groups are targeting healthcare? Is that accurate?

Mr. DESAULNIER. Yes, that is the question.

Mr. VORNDRAN. Sir, it's a little bit of a difficult question to ask because these criminal groups really go after targets of opportunity where they can find vulnerabilities. So, to Mr. Wales's commentary, certainly there may be common vulnerabilities in the healthcare network that any number of the 101 ransomware groups that we track could target.

But I think it's important to recognize that it's really the calculus of where can the criminals find the best vulnerability and the best access, and certainly that is prevalent in the healthcare industry, but it's also prevalent in many, many other critical infrastructure industries as well.

Mr. DESAULNIER. Specific to this industry, though, are there—we have got laws, HIPAA, protecting both patients and doctors, both Federal level and the state level providers. Are there things unique to this industry that we could help, be helpful with so that hospitals and healthcare organizations can provide you with the information but not feel as if they are becoming susceptible to some other privacy issue, sir, or litigation? Director Inglis or Director Vorndran?

Mr. VORNDRAN. I'll start, sir. This is Bryan Vorndran.

So, within the FBI, we have a concerted effort to engage the healthcare industry, and really, the focus of that engagement is sharing tactics, techniques, and procedures of these ransomware criminal groups, but also specific indicators of compromise that they can build into their net defense posture. We work very, very closely on those lines of effort with CISA on a very routine basis to make sure that we get to the hospital communities at large.

Regarding your questions about HIPAA, where HIPAA and other PII really come into play is during an incident response framework,

and there is concern, certainly HIPAA, PII across multiple industries, of willingness of those affected entities to share inadvertently PII. And one of the biggest recommendations we could pass along is to have those organizations, in this case, the hospital or healthcare industry, work through in a moment of crisis how would they be able to inform CISA or the FBI or the other relevant Federal Government entities as quickly as possible by lowering the barriers on PII and HIPAA.

Mr. DESAULNIER. I really appreciate that. I look forward to working with any of you and with the committee to make sure that we can protect this important part of our culture of the healthcare system.

Thank you, Madam Chair. I yield back.

Chairwoman MALONEY. Thank you. The gentleman from Texas, Mr. Sessions, is recognized.

Mr. SESSIONS. Madam Chairman, thank you very much, and thank you to this hearing. I think it is well worth our time, and important questions are being asked.

I want to ask the entire panel, but General, I will probably focus on perhaps you first. I would like to move down the pathway that Mr. DeSaulnier was moving, and that is what I would call lessons learned.

Can you tell me how many prosecutions, Federal prosecutions have occurred in the last five years on these issues of cybersecurity?

Mr. INGLIS. Sir, I don't have that information at my disposal at the moment. I'd be happy to take that question for the record or defer to Assistant Director Vorndran.

Mr. SESSIONS. Director?

Mr. VORNDRAN. Sir, I can't answer that question with great fidelity. I can certainly take it back and get you a very precise answer. But it's a threat that we've worked on continuously for five years and would have accurate data to support it.

Mr. SESSIONS. Yes. Well, the reason why I asked the question is, just like Mr. DeSaulnier said, we are interested in what are lessons that are learned from the investigations that you do, and we are interested in knowing how best—there was a question that was asked earlier about new laws, but I think we ought to know the effectiveness of what we are doing. We are spending a lot of time, a lot of resources. It is a national priority that we are engaged in.

Which one of you should I look for getting that answer from?

Mr. INGLIS. I'd be happy to take the lead on that, sir.

Mr. SESSIONS. Thank you, sir. We will write you a letter to help you. Being up here is a whole lot of fun, but we will followup and write you a letter requesting that information. We will include the chairwoman in that request.

So, for any one of you, you could probably dissect the marketplace problems into about 15 different areas. I put it—I am going to put it simply today in one or two ways, and that is malware, which is, you know, this malicious use of the computers. The other might be computer-induced or someone broke in necessarily maybe from an employee or found out about something.

But as it relates to an employer and related to how the employer has protected their own data and their employees, are you finding

or what would the discussion be of company, what I would call a company-induced breach? In other words, not related to something else. Somebody was not doing the right thing. Someone had a breach of their employee who did this. How would you respond to that to let us know about the size or scope of that threat?

Mr. VORNDRAN. So preliminary estimates or the best data we have that drives our estimates are that 90 percent of cyber breaches on user, end-user equipment or infrastructure for a company are induced by human error. But I think where we see an intersection is between what we would call an insider threat and the information the insider has access to that's trying to sell to a nation-state or somebody trying to get economic gain, and the overlap between that set of information, intellectual property, whatever have you, and what hackers are also going after.

And we see a core intersection between insider threat, hacker breaches, going after the same thing. We've seen it in COVID research, advanced defibrillators, aerospace engineering designs by subject for human penetrations, corruption is surfacing across a gamut. So, we do see a very, very keen intersection right there.

Mr. SESSIONS. So, in other words, your investigators, once they were able to effectively get their handle around the problem and look at how things happened, you are finding that employees and systems within companies many times has a large breach. So, one of the questions I would like to ask, General, is then and then if you have this information about how many people then were prosecuted what I would call on an internal basis by their company, one of the questions why we ask this—and one of my colleagues previously asked—is, are there new laws?

Years ago, we were really concerned with making sure that someone could report their information without being held liable necessarily. In other words, to share information about the things that were happening, which would help everybody. But in this case, if a major part of or, as you allude to, some part of the failure is with an employee, for us to know more about those employees.

Did they come from a certain pool, perhaps a school, MBA program where they had been involved? Perhaps an area of the country. Perhaps on something, whatever your investigation might be. If you could give us any clue about at least——

Mr. INGLIS. I would be happy to take that question and provide a fulsome response. I would say that the 90 percent figure that Assistant Director Vorndran cited is one that I cite as well, but the vast majority of those people don't intend to make those mistakes. They simply make them, right? They're not well equipped to make an appropriate choice at the moment. They might click on a link thinking it's one thing. It's provided by someone who's phishing them, and so on and so forth.

Mr. SESSIONS. Yes.

Mr. INGLIS. And so, we can give you very great clarity about the percentage of things attributable to a human being and those that were malicious in their intent.

Mr. SESSIONS. Yes, and I think that is important. I am not an athlete. I am a football player, and I threw interceptions that I didn't mean to. But I had to correct my behavior in some circumstances to understand what happened when I threw the pass.

And I think if business understands more clearly the huge part that their employees play, and I know we talk about it in the private sector a lot and in the government a lot. But I think that focus off that activity would help me.

And I appreciate you being here, each of you. This is a serious attempt. I will tell you—it is just a byline—but in 1985, when I was in New Jersey at what might be in old Bell Labs, I was on the original Bell Labs team that invented what might be ISP and our broadband, what became broadband.

And we began gathering data and information that would be in a switch, which would then gather data and information about how this data stream would be included in the Bureau. My father was the director at the time, and the Bureau was very concerned about what was being built in as information that could be gleaned on both sides of that not only from a perpetrator, but also from a company to gather information about that.

And I might ask—not now—but I might ask at some point for you, Assistant Director, about your viewpoint of gathering data and information, whether that has stayed up with time that would aid and help not just law enforcement, but the managing companies in their effort.

Mr. VORNDRAN. Sir, I'd be happy to have that conversation with you at any time.

Mr. SESSIONS. Great. Thank you very much.

Madam Chairman, thank you.

Chairwoman MALONEY. The gentleman's time has expired, and we are moving on. The gentleman from Georgia, Mr. Johnson?

Mr. JOHNSON. Thank you, Madam Chair, for holding this very important committee meeting today and hearing on this very important subject.

I introduced the Cybersecurity Opportunity Act with Senator Ossoff to fund a cybersecurity grant education program at historically black colleges and universities and minority-serving institutions. This legislation would promote cybersecurity education and research through grants to HBCUs and MSIs and help build a more diverse workplace.

Mr. Inglis, Mr. Wales, and Mr. Vorndran, how valuable is it to bring diversity into the cybersecurity work force?

Mr. INGLIS. I think diversity is essential in the cybersecurity work force. A diverse work force brings every perspective, cognitive diversity, as well as experiential diversity to the table in a way that that team is much harder to beat than any other team. And so, I think it's very important for us to make investments of that sort.

Mr. JOHNSON. Thank you. Mr. Wales?

Mr. WALES. Yes, to echo Director Inglis, I think cybersecurity is often thought of as largely a technical problem. What we have often said is that it's really a problem-solving challenge, and we need people who are effective at solving problems. And the more people and the more diversity we have looking at those problems, the better we're going to be at solving them and bringing to bear the right solutions to the significant risks and challenges that we face in this area.

And so, we are working hard. As I mentioned, this is one of the top priorities for Director Easterly at CISA is to expand our diversity, our work with HBCUs and minority-serving institutions. And bringing in, reaching out to communities that have never been priorities for engagement in the cybersecurity sphere is among our highest priorities, and really happy to work with you on the legislation that you discussed.

Mr. JOHNSON. Thank you, sir. Mr. Vorndran?

Mr. VORNDRAN. Sir, thanks for the question.

I'm going to broaden your question just a bit and just say for the FBI and for Director Wray, diversity across the entirety of the organization is a number-one priority for all of us. Certainly, that cuts into cyber and the need to diversify. But to echo what Director Inglis and Mr. Wales said, diversity, gender, ethnicity, it just makes us better because it accounts for every different viewpoint that's represented in our society.

Mr. JOHNSON. Thank you.

Mr. Inglis, according to an article published by the Association of American Medical Colleges, about a third of healthcare organizations globally reported being hit by ransomware in 2020. While the inconveniences of cyber-attacks such as the one on the Colonial Pipeline were felt in many homes, our family members' and friends' lives are at risk when hospitals go offline.

With so much reliance on the internet in general, are hospitals generally prepared to meet the challenges to patient care that arise from ransomware attacks?

Mr. INGLIS. Thank you very much for the question, Congressman. I don't have the data at hand to indicate how many of those were successful. Again, we know about 25 percent broadly of attacks that take place. We don't know about the other 75 percent.

That being said, I think that every critical sector of the hospitals being kind of in the center of one very important critical sector I think can do a better job of improving resilience and robustness, kind of mounting a proactive defense, and ultimately ensuring that they access all resources to include governmental resources, right, to help in that defense or in the response.

As I think was indicated earlier, it often is a target rich environment, a resource poor environment. So, we need to make sure that the hospitals have the necessary resources to make those investments and to properly defend those assets.

Mr. JOHNSON. Thank you.

Mr. Inglis, in that same article, it was disclosed that rural hospitals are more vulnerable to cyber-attacks than those located in urban or suburban areas. How are—How is your office addressing the need for cybersecurity resources such as training and software in smaller rural hospitals?

Mr. INGLIS. Sir, if I might kind of defer that question to Deputy Director Brandon Wales, who addressed this earlier, and I think quite thoughtfully so.

Mr. JOHNSON. Thank you.

Mr. WALES. It is the real challenge to make sure that we get out to the organizations that are most urgent need of our support, and I think we're trying to do this at a number of different levels. A lot of it starts at working at the state level with the state authori-

ties that we can help bring down supports they may have into the local communities, identify those places that most need support, and be a conduit back.

There are some states that have things called cyber navigators that are cybersecurity experts provided by the state to support local communities as they're building their cybersecurity posture. We've deployed cybersecurity state coordinators from CISA to be a linkage back to the Federal Government, back to CISA, and make sure that our products and services are being used in communities at the state and local level throughout the country.

In addition, the most recent infrastructure bill included a cybersecurity grant program that could help many public hospitals throughout the country particularly because it has certain provisions that require certain support to go out to rural communities as part of that grant program. So, we think that it could be an important steppingstone to begin to provide some of those resources that those communities need to begin to put in place the baseline cybersecurity that we would want for such a critical infrastructure to have.

Chairwoman MALONEY. The gentleman's time has——

Mr. JOHNSON. Thank you, Madam Chair. I yield back.

Chairwoman MALONEY. Thank you. The gentleman from Georgia, Mr. Clyde, is recognized.

Mr. CLYDE. Thank you, Madam Chair.

Director Inglis, it is a pleasure to see you again, and Assistant Director Vorndran and Executive Director Wales, thank you for being here today to share your insights on the threats of ransomware that it poses to our security. I would also like to wish CISA a happy third birthday.

Director Ingels—or Director Inglis rather, I would offer you this question, and then I would like a followup from Mr. Vorndran. I believe that a country's defense is best summed up in its offense, in its offensive capabilities. So, without a strong offense, I think our Nation will lack the ability to deter and respond to attacks conducted by both state and non-state actors.

Can you briefly highlight what capabilities are at the government's disposal to properly respond and eliminate those threats, and if you believe that you cannot discuss those capabilities to the extent you would like to in this hearing, would you be willing to come back and hold a classified hearing to help my colleagues and I better understand those capabilities?

Mr. INGLIS. I would certainly be pleased to come back in a classified hearing and describe these things more fulsomely. But I would say that in cyberspace, as much as cyberspace can impact any instrument of power, we should, in return, be able to use any instrument of power to affect cyberspace.

So, our offense, as it were, is not simply our ability to do things in and through cyberspace, but to apply legal remedies, financial remedies, diplomatic remedies, private sector remedies that have authorities on their own infrastructure, to bring all that to bear in a concurrent fulsome way such that we impose cost on adversaries, that would be, I think, a proper and fulsome offense. Again, offense must be an extension of the defense. Defense needs to be kind of equally important to us.

Mr. CLYDE. Thank you. Mr. Vorndran, could you comment on that, too, please?

Mr. VORNDRAN. Of course, sir. I'm going to take your question a little bit of a different direction, but still get to the point. When we talk offense, I understand what you're saying, but I think a lot of times in this discussion we miss sometimes how big of a role investigation plays in helping provide that defense, making sure that our victim entities in this country are in good shape.

You know, for every one victim, there is usually a dozen or 100 more being affected by the same malware strain. In a recent critical infrastructure compromise, we were able to get agents out to the scene immediately and identify a zero-day vulnerability. We immediately pivoted, using our investigative tools. We found other zero-days in critical infrastructure, worked with CISA, and were able to patch all of those when the patch became available. Those other critical infrastructure companies never would have known they were potentially vulnerable victims.

We had a situation with a hospital recently where we were able to get to a hospital within hours and share indicators of compromise that allowed them to eradicate an adversary from their network in real time.

So, we—I appreciate the question about offense. I would want to be part of that classified briefing with Director Inglis, but I think it's really important. There's a hybrid space in here between true defense and true offense that our field-deployed force is filling extremely well on a day in and day out basis.

Mr. CLYDE. Well, thank you. I think that cyber-attacks are one of the most dangerous ones where outside entities can pierce our defenses and affect our civilians that don't have the defensive capabilities.

Also, Assistant Director Vorndran, in your testimony here, you say that DOJ also has extensive experience in navigating complex privacy and civil liberty issues that will inevitably rise from new requirements and would prove to be invaluable in helping to set the standards that strike the right balance to ensure that incident report information is collected, stored, and shared appropriately.

What is not mentioned is ensuring that civil liberties are protected. Would you speak to the importance of protecting these civil liberties and the commitment of the FBI and the DOJ to do just that, please?

Thank you.

Mr. VORNDRAN. Sure. Any new incident reporting legislation, the FBI and Department of Justice's position has always been the same. We want full and immediate access to any data that's reported to the U.S. Government because we are a decentralized organization, and we can get people onsite almost immediately.

We're also very, very attentive and understanding to civil liberties, personally identifiable information, and everything that's derivative of that, and we would be willing to work within confines of a bipartisan bill to make sure that those elements are clearly protected, to make sure everybody is in a good space.

Mr. CLYDE. OK. Thank you. I appreciate that commitment.

And I have got just a few seconds left for Director Wales. Director Easterly recently had the opportunity to discuss how the Fed-

eral Government's hiring process has hindered CISA's ability to recruit the work force it needs to safeguard our Nation's important entities. She highlighted how the Federal Government has 20 steps to hiring someone, and the process takes about 200 days. In comparison, the private sector's hiring process typically takes about 60 days.

Can you provide the committee with some recommendations on how we can streamline the hiring process so that CISA can be better staffed so it can more effectively carry out its mission?

Mr. WALES. Sure, sir. That's a great question.

This is an area that is of intense focus for our entire agency right now. We have worked over the past year to reduce the time by about 15 percent. I think it went from about 240 down to 200 days on average to hire a person, but that's still obviously too long.

We are looking at an end-to-end review to understand what do we have the ability internally to change, how can we streamline it without any requirements for new legislation, but we're happy to come back to you and talk about what we've identified and if there are additional tools that we need in order to streamline it further than we can do internally.

Mr. CLYDE. Thank you very much, and I yield back, Madam Chair.

Chairwoman MALONEY. Thank you, and I join you in your request for a classified briefing. Democrats have also expressed concern in wanting to investigate this further.

But before I close, I want to offer Mr. Grothman an opportunity to offer a closing statement.

Mr. GROTHMAN. I would like to thank you for having the hearing.

Chairwoman MALONEY. Thank you.

Mr. GROTHMAN. I thought it was a good bipartisan hearing without the partisan rancor that you sometimes have.

I would like to thank our guests for being here. This is a very important topic, and failure is really not an option. I mean, there are some agencies out there they can probably fool around and our country will continue on, but you guys cannot fail.

And I hope that you make dealing with cybersecurity pressed threats your number-one priority. There were some indications from some of your comments that that might not be your number-one goal, but it has got to be your number-one goal.

I share in the request for a private meeting sometime, and again, I thank the chairman for keeping such a cordial hearing going one more time.

Thank you.

Chairwoman MALONEY. Thank you. The gentleman yields back.

I would like to thank, first and foremost, all of our witnesses for appearing today, including Mr. Wales, who appeared on very short notice. Thank you.

Today's hearing advanced several important goals. The hearing highlighted key findings the committee released today from our investigation into major ransom payments made by U.S. companies to cyber criminals. The FBI confirmed today that these payments only fuel more criminal attacks.

Today's witnesses also agreed with the committee's findings that we need to do more to enhance coordination among Federal agen-

cies in responding to these attacks. Mr. Inglis, whose role as National Cyber Director was championed by this committee, will be crucial to that effort. His office finally received permanent funding yesterday when President Biden signed the bipartisan infrastructure bill, and I am looking forward to his continued leadership.

Today's hearing also demonstrated the significant strides that the Biden-Harris administration has already taken to tackle ransomware head on, including by helping the private sector to prevent attacks, prosecuting attackers, and working with our allies to fight back against this global challenge.

Finally, today's witnesses made clear that the time for Congress to act is now. We need to disrupt ransomware incentives, and we need to require incident reporting so that the Federal Government has full visibility into every attack. I urge all my colleagues to support this critical bipartisan legislation.

To all of the witnesses, I thank you for your service, and I look forward to working with you to strengthen our Nation's cyber defense.

With that, I would like to just end by saying and in closing that I want to commend all of my colleagues and the panelists for participating today in this important conversation.

With that, and without objection, all members have five legislative days within which to submit extraneous materials and to submit additional written questions for the witnesses to the chair, which will be forwarded to the witnesses for their response. I ask our witnesses to please respond as promptly as you are able.

This hearing is now adjourned. Thank you.

[Whereupon, at 1:08 p.m., the committee was adjourned.]