CYBERSECURITY FOR THE NEW FRONTIER: REFORMING THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JANUARY 11, 2022

Serial No. 117–59

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
46–680 PDF WASHINGTON : 2022

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
SHONTEL M. BROWN, Ohio
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

JAMES COMER, Kentucky, *Ranking Minority Member*
JIM JORDAN, Ohio
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
VACANCY

RUSS ANELLO, *Staff Director*
EMILY BURNS, *Team Lead*
ELISA LANIER, *Chief Clerk*

CONTACT NUMBER: 202-225-5051

MARK MARIN, *Minority Staff Director*

CONTENTS

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 listed below are available at: docs.house.gov.

* Scorecard; submitted by Chairwoman Maloney.

* Statement for the Record; submitted by Rep. Brown.

CYBERSECURITY FOR THE NEW FRONTIER: REFORMING THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Tuesday, January 11, 2022

House of Representatives,
Committee on Oversight and Reform,
Washington, D.C.

The committee met, pursuant to notice, at 10:02 a.m., in room 2154, Rayburn House Office Building, and on Zoom; Hon. Carolyn B. Maloney [chairwoman of the committee] presiding.

Present: Representatives Maloney, Norton, Lynch, Cooper, Connolly, Krishnamoorthi, Raskin, Mfume, Tlaib, Porter, Brown, Davis, Wasserman Schultz, Welch, Speier, Kelly, DeSaulnier, Comer, Foxx, Hice, Grothman, Cloud, Gibbs, Sessions, Keller, Mace, Franklin, LaTurner, Fallon, and Donalds.

Chairwoman Maloney. I want to start this hearing with an announcement we just received.

CISA, the FBI, and the National Security Agency are, as we speak, releasing a new joint cybersecurity advisory on mitigating Russian state-sponsored cyber threats to U.S. critical infrastructure. It provides information on 17 vulnerabilities to help organizations reduce the risks presented by the Russian state-sponsored cyber actors.

I applaud this action and convene today's hearing to discuss how to reduce these kinds of state-sponsored cybersecurity risks for the Federal Government, which is so important to our national security.

[Gavel sounds.]

Chairwoman Maloney. The committee 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.

Today, we are discussing the urgent need to improve the Federal Government's defenses against cyber attacks. Over the past year, we have seen devastating cyber attacks against Federal agencies, state and local governments, and businesses. These attacks have caused real-world damage like stolen intellectual property, hundreds of millions of dollars paid in ransoms, and even shutdowns of critical infrastructure like oil pipelines.

Many of these attacks were carried out by America's geopolitical adversaries. Last January, a group of Chinese hackers unleashed a massive cyber attack that ripped through computer networks around the globe through Microsoft, a software. The attack spread to as many as 60,000 U.S. organizations, including businesses, hospitals, schools, and city governments, and posed a grave risk to Federal agencies.

According to FBI Director Christopher Wray, economic espionage from China is “the greatest long-term threat to our Nation’s information and intellectual property and to our economic vitality.” Director Wray has explained that this information theft amounts to “one of the largest transfers of wealth in human history.”

Federal agencies are also still reeling from the SolarWinds breach in which Russian actors infiltrated and roamed the networks of at least 9 agencies and 100 private companies for months. And today, we are dealing with the fallout from the Log4j software vulnerability, which the Director of CISA, Jen Easterly, described as the most serious vulnerability she has seen in her decades-long career.

The mounting attacks by China, Russia, and other bad actors are constantly changing. They are as dynamic as they are diabolical. Today, we will be discussing how the Federal Government can protect itself against these threats.

The Federal Information Security Management Act, commonly known as FISMA, establishes a cybersecurity framework for the Federal Government. It is the best defense our Federal information networks and supply chains have against cyber attacks, but the reality is that it is simply not enough to protect us in its current form.

Threats have transformed dramatically since FISMA was last updated in 2014 and in ways that were unimaginable when the law was first written 20 years ago. Now it is no longer enough to guard our networks at their perimeters, as was the focus in the past. Today, we must also guard within the perimeter, continuously monitoring for the smallest trace of abnormal activity that might signal an intruder.

Modernization cannot wait because our adversaries certainly won’t, and we are already woefully behind. Congress must reform FISMA and create a cutting-edge, whole of government approach to meet the challenge of the constantly evolving cyber frontier. That is why today Ranking Member Comer and I are releasing a discussion draft to modernize FISMA called the Federal Information Security Modernization Act of 2022.

The bill would improve the cybersecurity of Federal networks through a risk-based approach that uses the most advanced tools, techniques, and best practices. It would also clarify and streamline the responsibilities of Federal entities so that they could respond quickly and decisively to breaches and major cyber incidents.

By modernizing the law and focusing it on the most important security outcomes, we can ensure that Federal agencies are better equipped to combat the evolving threats they face. Our bill contains key similarities to the companion legislation in the Senate, which was introduced by our counterparts, Chairman Gary Peters and Ranking Member Rob Portman. I applaud their bipartisan leadership on this critical issue.

Our committee has a strong bipartisan track record of shining the light on the country’s cybersecurity challenges and fighting to improve Federal information technologies. Last year alone, we held hearings on ransomware attacks, the SolarWinds breach, and the hundreds of open recommendations by the Government Accountability Office to improve cybersecurity in the Federal Government. Our committee was also instrumental in creating the role of the National Cyber Director, who serves as the President's top adviser on cybersecurity and has a crucial role to play in the FISMA framework.

I also want to recognize our Government Operations Subcommittee chairman, Mr. Connolly, for his crucial work to improve Federal IT, including through his seven years of biannual FITARA hearings. In addition, he has led the charge on H.R. 21, the FedRAMP Authorization Act, which will enhance security and modernize cloud computing Government wide. That bill passed the House on suspension last year, and Chairman Connolly has my full support in encouraging the Senate to pass it so it can reach the President's desk as soon as possible.

I want to extent my thanks to the witnesses for being here today and to Ranking Member Comer for his partnership and diligence in working on the discussion draft we are releasing today. We are committed to perfecting the bill together, and I am confident that today's hearing will help our bipartisan, bicameral coalition get this priority across the finish line this year.

I now recognize Mr. Connolly for an opening statement.

Mr. CONNOLLY. Madam Chair, were you recognizing me or the ranking member?

Chairwoman MALONEY. You, first.

Mr. CONNOLLY. Ah, OK. Thank you so much, Madam Chairwoman, and thank you for elevating this issue to the full committee level. It is that important. And frankly, as we learned during the pandemic, information technology platforms undergird everything we do, and they have to help the Government deliver services, be efficient, effective, but also be cybersecure.

Over the past several years, we have witnessed the consequences of vulnerable cybersecurity infrastructure across the Federal Government. Poor cyber hygiene leaves sensitive IT systems and data susceptible to cyber attacks by criminals, prompting significant disruption and high cost. This hearing will examine the urgent need to reform FISMA and evolve the Federal Government's approach to cybersecurity.

Seven years ago, the Office of Personnel Management suffered a massive data breach that completely disrupted the operations of OPM and affected more than 20 million Americans, including contractors, family members, others who had undergone background checks for Federal employment, as well as Members of Congress. Since then, cyber incidents have continued to grow in frequency and sophistication. Fiscal year 2020 alone, Federal agencies reported more than 30,000 cybersecurity incidents.

The SolarWinds, as you mentioned, Madam Chairwoman, and the Microsoft Exchange hacks demonstrated the unique patience, sophistication, and aggressiveness of our adversaries. More recently, on December 9, a vulnerability was discovered in freely available and widely used open-source software provided by the Apache Foundation called Log4j, which has been used to build a vast array of Web services for over a decade.

Ensuring the cybersecurity of our Nation is critical, protecting taxpayer data and dollars. In its 2021 High Risk List, the GAO says that the Federal agencies and other entities need to take urgent action to implement a comprehensive cybersecurity strategy, perform effective oversight, secure Federal systems, and protect critical infrastructure, privacy, and sensitive data.

The foundation of the Federal Government's cybersecurity posture relies on modernized, nimble technology systems that bake in security from the outset. A fundamental component of this security is FISMA, which was first signed into law, as you indicated, Madam Chairwoman, back in December 2002 and was last updated in 2014. The law requires each Federal civilian agency to establish an agency-wide program to ensure the security of the agency's information systems.

Despite FISMA's positive contributions to improving Federal cybersecurity, Government officials have cited FISMA requirements as sometimes onerous and overly focused on compliance rather than on mitigating potential cyber threats. Further, when FISMA first passed, many of today's key cyber stakeholders had not yet been established, like the Cybersecurity and Infrastructure Security Agency and the National Cyber Director. We must take more proactive cyber measures that ensure the Government runs on modern, well-designed IT.

For example, I have long advocated for the codification of FedRAMP, the Federal Risk and Authorization Management Program, which you very generously mentioned and very much we welcome your support in our endeavor to get that into law. For the past five years, we have worked to improve and make permanent the FedRAMP program.

And by the way, it has passed the House four different times, four different times in two Congresses. It has never passed the Senate. And it has finally come out of the Senate committee, but we believe, frankly, that the House has clear providence, and we want to make sure it gets passed.

The future of Government IT is paramount to effectively serving the public. That future should involve an agile Federal work force that can respond quickly, relying on technology and supply chains to deliver results.

I was thrilled to see that President Biden made Federal cybersecurity a priority early in his administration. His executive order on improving the Nation's cybersecurity ensures agencies are adapting and adopting best practices of secure cloud services, zero trust architecture, and multifactor authentication and encryption.

But today's hearing reminds us more must be done, and Congress has a critical role in ensuring that laws evolve to accommodate and anticipate new realities. I look forward to working with you and the ranking member on the draft legislation, Madam Chairwoman, and I thank you for your leadership in holding today's very critical hearing.

I yield back.

Chairwoman MALONEY. I thank you for your statement, and I now recognize the distinguished ranking member, Mr. Comer, for his opening statement.

Mr. COMER. Thank you, Chairwoman Maloney, for holding this hearing to examine a central law governing Federal cybersecurity, the Federal Information Security Modernization Act.

Prior Congresses have not encountered the same array or frequency of cybersecurity threats that we face today. Last year's breach against SolarWinds exposed weaknesses throughout multiple Federal agencies and throughout the private sector. Just last month, we learned of a new vulnerability infecting an Internet tool called Log4j. Some estimate that this is used in nearly a third of all websites, impacting Government agencies and businesses large and small.

These incidents highlight why FISMA, a law which assigns cybersecurity roles and responsibilities for the protection of Federal information systems, is a critical component in our cyber defense arsenal. Public and private sector entities continue to play whack-a-mole while hackers take advantage of every possible weakness in information systems. A modern uptake to FISMA will ensure Federal agencies, in coordination with the private sector and Government contractors, can better protect, disrupt, and deter damaging digital intrusions.

The Federal Government maintains extensive public records, which contain sensitive information on all Americans and the private sector businesses and institutions that drive our economy and civil society. Congress and the executive branch must be smart and diligent stewards of this sensitive and valuable information.

In examining FISMA, we need to clearly understand the full scope and evolving nature of cybersecurity challenges our Government faces before enacting systematic changes. Recently, the Senate and the administration addressed FISMA reform through legislation and executive guidance. These are important steps, ones that the chairwoman and I hope to buildupon to ensure reforms not unnecessarily impose restrictive burdens, duplication, or complications.

FISMA reform must provide agencies with the authority to effectively address threats with speed and precision while also freeing time to continuously monitor new and emerging threats as they arise. To get this right, we must understand a core principle of cybersecurity—that it is impossible to have a completely secure system.

As technology continuously evolves, our systems and networks will become more interconnected, allowing bad actors to continue to discover or engineer new methods of attack. Any reform must enable Federal agencies to respond to an incident in real time to mitigate damage, fix the problem, and effectively share critical information about the attack so it does not happen again.

Burdensome red tape requirements for coordination and outdated compliance checklists cannot remain significant hurdles when responding to major cyber incidents. Nor should Congress be subjected to delayed and disjointed agency briefings following major incidents.

That said, we also recognize the cyber expertise and knowledge housed within the executive branch, along with Government contractors performing valuable cybersecurity services. We have listened to these experts. We have accounted for their advice and guidance in drafting House companion legislation. We greatly appreciate OMB's technical assistance and have honored an overarching request to avoid imposition of overly burdensome bureaucratic reporting and compliance controls, which hamper agencies from addressing daily cybersecurity challenges.

I also want to thank the chairwoman and her staff for working diligently to incorporate this feedback. I encourage our members to support a streamlined legislative product the chairwoman and I are crafting, which adheres to a risk-based cybersecurity model. We are confident our approach gives more flexibility to our Federal agencies and private sector partners to address a quickly evolving threat landscape.

We are also focused on offering statutory authority enabling agencies to take proactive steps to harden our Nation's cyber defenses. I am confident that cybersecurity modernization is largely achievable through carefully balanced FISMA reform.

I look forward to hearing from our witnesses, each of whom have a unique perspective in working in the cyber arena. Together, I hope our collective efforts in reform will place the Federal Government on a solid security footing for years to come, improve coordination, and present a united front in deterring and defeating cybersecurity threats.

Now I would like to yield to the distinguished ranking member Mr. Hice, who is no doubt an expert in this area.

Mr. HICE. I thank the ranking member. Appreciate that very much.

And if I could, just as a point of personal privilege, just give a great shout-out and congratulations to the Georgia Bulldogs for a great win last night. It is my honor to represent Athens and the University of Georgia, and we are thrilled with the win that they brought home last night.

But with that, listen, I appreciate a hearing to examine the potential updates to FISMA. The Federal cybersecurity issue, of course, is an extremely important issue, but I must admit that I am confused, and I am sure some of my other colleagues also share in some of my confusion, as to specifically why the majority has failed to invite the administration witnesses to testify concerning their experience operating on the cyber front lines.

No doubt we have an esteemed group of witnesses who are with us here today, and they have a lot of Federal years of experience. But nonetheless, the agency operators currently battling threats from our adversaries are inexplicably absent, and I am sure it is because, quite frankly, they were not even invited to be a part of today's hearing. But if Congress is to examine the modern cyber threat environment fruitfully, we must hear from the very administration officials who understand why we are falling short in cybersecurity preparedness.

It is no secret that our Federal cyber apparatus is a massive bureaucracy, and it has grown exponentially since the last revamp of FISMA in 2014. And yet it is no question, a reality—and a legitimate question to ask does anyone—does anyone believe that our Nation's cybersecurity has improved at the same pace as the bureaucracy? The answer, of course, is no.

Our adversaries, particularly China and Russia, continue to exploit our weaknesses, weaknesses that are born from bureaucratic layers, from misaligned roles and responsibilities, and the failure to exhibit strength. When our Government fails to address cybersecurity weaknesses, what is at stake? What is at risk? Literally reams of sensitive information that the administrative state has amassed on American citizens.

Malicious actors and America's enemies know our cyber gaps, and they target them. They do so accordingly. Just this past year, they targeted infrastructure like meat production, our oil pipelines, and ubiquitous software supply chains. And the list goes on and on and on. We are vulnerable.

Cyber attacks are no longer merely a product of war games. They are genuine threats to our American livelihoods. They are a threat to our daily digital interactions and the numerous Government and private sector services.

The Government Operations Subcommittee, understanding this threat, we have worked hard to improve the adoption of modern secure technology in Federal agencies through initiatives like FedRAMP and IT Modernization Centers of Excellence. And I believe our efforts to adopt modern cloud technology solutions will similarly help deliver efficient, effective, and secure Government services.

My hope, my hope sincerely is that FISMA reform will spur further migration to the cloud, to transition spoken of optimistically in the aftermath of SolarWinds for improving the Federal Government's cybersecurity posture. I am hopeful that eventually we will actually have discussions with administrative witnesses that will allow us the opportunity to explore ways to further the Government's effective utilization of its IT assets by moving away from legacy insecure technologies, consolidating and optimizing the use of existing data centers, improving agency inventories of their IT systems, and focused defense of critical data assets are always that FISMA reform in our upcoming hearing regarding FITARA can contribute to better Federal cybersecurity.

And I hope we will go down these paths with genuineness in the days, weeks, and months to come. And with that, I yield back.

Chairwoman MALONEY. The gentleman yields back, and I thank him very much for his comments and particularly the ranking member and his staff for working in such a positive way to confront what is a national security threat to our country.

Earlier, we had several months back in October a hearing with the Government cybersecurity experts. We had the Director of Cybersecurity, newly appointed, a representative from CISA, the FBI. We also consulted with representatives of the Biden administration and the Government, Government professionals on the drafting of this bill. They were deeply involved in all of it. We can have another hearing on it.

This hearing focuses on the private sector, which is an important part of our country. We need to hear what their challenges are and what they are doing. We have already heard from Government. We can have them in and hear again, or we can have just a panel and a committee discussion.

But we have already consulted them, and they were consulted deeply and effectively and many times. We were partners in drafting this legislation along with the Senators that were involved.

I would now like to introduce our witnesses.

Our first witness today is Ms. Jennifer Franks, who is the Director of Information Technology and Cybersecurity at the Government Accountability Office.

Then we will hear from Mr. Grant Schneider, who is a Senior Director of Cybersecurity Services at Venable. He previously served as the Federal Chief Information Security Officer at OMB and as the Senior Director for Cybersecurity Policy at the National Security Council.

Next, we will hear from Mr. Ross Nodurft, who is the executive director of the Alliance for Digital Innovation.

Next, we will hear from Ms. Renee Wynn, who is the CEO of RP Wynn Consulting. Previously, she served as the Chief Information Officer at NASA, which always is a target of cyber theft.

Finally, we will hear from Mr. Gordon Bitko, who is a Senior Vice President of Policy at the Information Technology Industry Council and was previously the Chief Information Officer at the FBI.

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

Do you swear or affirm that the testimony that 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. Without objection, your written statements will be part of the record.

With that, Ms. Franks, you are now recognized for your testimony.

STATEMENT OF JENNIFER R. FRANKS, DIRECTOR OF INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. FRANKS. Chairwoman Maloney, Ranking Member Comer, and members of the committee, thank you for inviting GAO to contribute to this important discussion about FISMA reform.

As you know, IT systems supporting Federal agencies are inherently at risk. The protection of these systems is vital to public confidence, safety, and national security. Without proper safeguards, computer systems are increasingly vulnerable to attack. As such, GAO has designated cybersecurity as a governmentwide high-risk area for the last 25 years.

As the cyber threat landscape has significantly evolved, it is important for Federal agencies to ensure that their information security programs under FISMA can mitigate the risk and impact of threats to their data, systems, and networks. Today, I will focus on the key preliminary results from our ongoing reviews of agencies' FISMA implementation.

Our ongoing review highlights the reported effectiveness of Federal agencies' implementation of cybersecurity policies and practices and the extent to which relevant officials at Federal agencies consider FISMA to be effective at improving the security of agency information systems. Our preliminary results indicate varied levels of effectiveness of Federal agencies' implementation of FISMA requirements.

For example, IGs identified uneven implementation of cybersecurity policies and practices across the Federal Government. For Fiscal Year 2020, IGs concluded that only 7 of the 23 civilian CFO agencies had effective agency-wide information security programs.

Specifically, most agencies continued to struggle in the security core functions to identify, protect, detect, and recover. On a positive note, more agencies were, indeed, meeting the cybersecurity goal of taking appropriate actions needed to respond to a cybersecurity incident.

In responding to our questionnaire and interviews regarding the effectiveness and usefulness of FISMA, cybersecurity officials at the 24 CFO agencies highlighted the benefits of FISMA, identified impediments to implementing FISMA requirements, and made suggestions to improve FISMA and the annual reporting process.

Regarding the benefits of how FISMA helped improve their agencies' security posture, agency officials identify standardized security program requirements, justifiable cybersecurity requests to management, establish agency metrics to track performance of the security program, and establish responsibilities and authorities related to the cybersecurity program, among others.

In terms of the impediments, agency officials identified a number of barriers to their agencies' implementation of FISMA. The most cited were a lack of resources, that annual reviews focused more on compliance with the law than on the effectiveness of cybersecurity programs, and that there was insufficient time to implement new requirements and/or remediate findings identified in the annual FISMA reviews before the next review season begins.

With respect to the suggestions, most agencies did not identify legislative changes to FISMA nor the need for additional authorities. Specifically, seven agencies made suggestions on reducing the frequency of the FISMA IG reviews. Other suggestions were related to the consistency of IG evaluations, IG reviews focusing more on risk as opposed to compliance, and the advancing of data automation.

In summary, the risks to IT systems supporting the Federal Government are increasing, and the tactics and techniques of cyber criminals are constantly evolving around the globe. Further, high-profile events, such as the SolarWinds and Microsoft Exchange Server incidents, demonstrate the need for further attention and improvements to agency cybersecurity capabilities. This means that Federal agencies need to continue to build stronger cybersecurity programs through more effective FISMA implementation, which could better protect against increasing cyber threats.

This concludes my remarks, and I look forward to answering any questions you may have.

Thank you.

Chairwoman MALONEY. Thank you.

Mr. Schneider, you are now recognized for your testimony.

STATEMENT OF GRANT SCHNEIDER, SENIOR DIRECTOR OF CYBERSECURITY SERVICES, VENABLE, FORMER FEDERAL CHIEF INFORMATION SECURITY OFFICER, OFFICE OF MANAGEMENT AND BUDGET

Mr. SCHNEIDER. Thank you very much.

Chairwoman Maloney, Ranking Member Comer, members of the committee and your staff, thank you for the privilege to appear before you today.

I've spent my entire 30-year career focused on our Nation's security. This includes over 20 years at the Defense Intelligence Agency, seven of which as the Chief Information Officer. I then spent six years within the Executive Office of the President, involved with all aspects of Federal and critical infrastructure cybersecurity.

As mentioned, I served as a Senior Director for Cybersecurity Policy on the National Security Council staff and most recently as the Federal Chief Information Security Officer working with agencies to secure Federal systems.

For the past 16 months, I have been a Senior Director for Cybersecurity Services at the law firm Venable, where I help our clients, both large and small from across all sectors, enhance their cybersecurity programs through the development and implementation of risk management strategies, as well as assisting with the preparation, response, and recovery from various cybersecurity incidents, including ransomware attacks.

I want to thank the committee for taking up the very important issues related to the security of our Nation's Federal information and information systems. Over the years, FISMA legislation has focused agencies' attention on cybersecurity and made them more secure. However, FISMA must evolve, just as the threats and the nature of our information technology environments continue to evolve.

The threat surface for Federal agencies and private sector organizations increases as organizations interconnect systems and move more sensitive information and transactions online. This started well before the global pandemic and has only accelerated over the past two years. To be clear, these digital enhancements increase productivity, increase convenience, and increase access to services.

At the same time, malicious cyber actors have increased their capabilities and demonstrated a willingness to exploit any system to achieve their objectives, whether they be monetary gain, espionage, or some form of activism. Most recently, public and private sector organizations have been responding to the exploitation of the Log4j vulnerability. Over the past year, organizations have responded to the attack on SolarWinds, the Microsoft Exchange Server incident, and countless ransomware attacks, including the one involving the Colonial Pipeline. These are but a few of the many incidents highlighting the importance of cybersecurity for both public and private institutions.

FISMA is focused on directing Federal agencies to develop and implement risk management programs to secure Federal information and information systems. As you consider updates to this keystone piece of legislation, I encourage you to address five key areas.

First, clarify Federal cybersecurity roles and responsibilities. Since the last update to FISMA, Congress has established the Cybersecurity and Infrastructure Security Agency, as well as the National Cyber Director. These are important additions to the Federal cybersecurity ecosystem. However, they also require clarification of the roles and responsibilities with respect to Federal cybersecurity. I recommend Congress clarify the roles and responsibilities at a high level and then direct the President to clarify them in more detail.

Second, codify the role of the Federal Chief Information Security Officer as a Presidentially appointed position within the Office of Management and Budget with appropriate budget and oversight authorities, including approval of CISA's budget and approval of agency cybersecurity budgets.

Third, as part of risk management programs, require agencies to have greater situational awareness of their technology environments. This includes inventories of hardware and software, supply chain assessments of those inventories, understanding the actions being performed within their environment, and fully inspecting network sessions to identify and mitigate techniques used to compromise systems.

Four, hold OMB accountable to maintaining the definition of a major incident to ensure that the right level of information is being reported to Congress.

And five, require greater alignment of core cybersecurity requirements based on the National Institute of Standards and Technology guidance for both national security systems and non-national security systems.

Thank you again for the opportunity to speak with you today, and I look forward to your questions.

Chairwoman MALONEY. Thank you very much.

Ms. Wynn, you are now recognized for your testimony.

Oh, no, no. It should be Mr. Nodurft. You are now recognized for your testimony. Mr. Nodurft?

STATEMENT OF ROSS NODURFT, EXECUTIVE DIRECTOR, ALLIANCE FOR DIGITAL INNOVATION, FORMER CHIEF, OFFICE OF MANAGEMENT AND BUDGET CYBERSECURITY TEAM

Mr. NODURFT. Thank you, Chairwoman Maloney, Ranking Member Comer, and members of the committee, for holding this hearing on FISMA reform.

My name is Ross Nodurft. I'm the executive director of the Alliance for Digital Innovation. It's a coalition of innovative commercial companies whose mission it is to bring IT modernization and emerging technologies to Government.

ADI engages with policymakers and thought leaders to break down bureaucratic, institutional, and cultural barriers to change and to enable Government access to secure, modern technology that can empower a truly digital Government.

ADI focuses on four key areas in our advocacy efforts. One, accelerating technology modernization in Government. Two, enabling acquisition policies that facilitate greater use of innovative technologies. Three, promoting cybersecurity initiatives to better protect the public and private sectors. And four, improving the Federal Government's technology work force. Each of these areas must work closely with each other to allow for Government mission owners to partner with industry to build a modern digital Government.

My experience prior to taking on the role of executive director at ADI includes both operational and strategic roles in the Government and the private sector focused on cybersecurity. More specifically to today's discussion, I led the Office of Management and Budget's cybersecurity team, reporting to the Federal CISO and CIO. During my time, my team was responsible for drafting the annual FISMA report to Congress, developing and reporting the FISMA metrics, writing and implementing Government-wide cybersecurity policies, aggregating and producing the annual cybersecurity budget, and managing the team that conducted oversight of the Federal civilian agencies' cybersecurity programs.

Since leaving Government, I've worked closely with many companies to build, expand, and institutionalize their own cybersecurity programs and to develop an approach to cybersecurity risk management that effectively uses resources to buy down and manage enterprise risk. Since joining ADI, I've worked closely with some of the leading technology cybersecurity professional services providers to the public sector.

The technologies and services delivered by ADI member companies underpin the Federal Government's modernization efforts and provide the backbone for many agencies' zero trust architectures and cybersecurity plans. Given the roles that many of our member companies play in the Federal cybersecurity and technology ecosystem, ADI appreciates the committee's focus on this important topic.

With the spate of cybersecurity incidents and vulnerabilities over the last several years, the need for continued oversight and support from Congress is necessary to combat the constantly evolving threats facing the Federal departments and agencies. The proposed FISMA legislation that was recently approved in the committee in the Senate contains several important changes but could be more comprehensive in its handling of cybersecurity as a holistic public sector priority.

As Congress considers an update to FISMA, ADI encourages this committee and others in the House and Senate to also look to update other key laws dealing with Government information technology policy acquisition and governance. Updating the E-Government Act, the Clinger-Cohen Act, the Federal Information Technology Acquisition Reform Act—which you guys have a hearing on coming up—and aligning proposed legislation such as the House-passed FedRAMP Authorization Act would enable agencies, as well as the oversight entities and program offices that govern Federal IT policy, to modernize and secure their environments more quickly.

On the topic of FISMA reform, ADI believes there are several important areas that warrant attention from the members of this committee. These include the need to update and align cybersecurity roles and responsibilities so changes to FISMA should reflect the new roles and authorities of the National Cyber Director, as well as the responsibilities of the Federal CISO at OMB and the Director of the Cybersecurity and Infrastructure Security Agency.

Another area that warrants the committee's attention is the need to address incident response, breach notification, and vulnerability management. Given the proliferation of incidents, breaches, and vulnerabilities, updated FISMA legislation should codify practices and policies that keep Congress informed in a way that will allow for effective oversight while giving the departments and agencies the flexibility and time to respond and report these incidents, breaches, and vulnerabilities without disrupting or impacting those responses.

Another area is to reinforce Government shift to commercial technologies through use of automation and focus on meaningful reciprocity. As the Government's information technology ecosystem shifts to more modern cloud-based solutions, agencies should embrace technologies and services that enable security in these zero trust environments and leverage best-in-class industry partners to assist with the buildout of those environments.

This bill should make it easier for agencies to issue authorizations to operate through strategies that include use of automation and offer reciprocity across agencies and across compliance regimes.

Effectively budget—another area to look at is to effectively budget for cybersecurity and invest in risk management. Securing large enterprises, especially those that have legacy technology and modernization backlogs, can be expensive. Congress must encourage agencies to budget for technology and services that can effectively buy down the risks to their environments. As agencies continue to modernize their systems, agencies should pivot their cybersecurity spend to move toward tools and services that enable zero trust environments.

And finally, a final area that warrants the committee's attention, to modernize and standardize cybersecurity performance metrics and measurements. As agencies modernize technology and move toward cloud-based environments, take steps to enhance security, and migrate to zero trust architectures, oversight offices must also modernize the measurements used to track agency progress and measure security. Successful cybersecurity must be defined through outcomes, and those outcome-driven, risk-based metrics must be consistent across all the oversight entities.

Thank you again to the committee for this opportunity to discuss the important topic, and I look forward to your questions.

Chairwoman MALONEY. Thank you so much.

Ms. Wynn, you are now recognized for your testimony.

STATEMENT OF RENEE WYNN, CONSULTANT, FORMER CHIEF INFORMATION OFFICER, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Ms. WYNN. Good morning, Chairwoman Maloney, Ranking Member Comer, and distinguished members of the committee.

I am honored to testify today on the importance of cybersecurity and examine the transformation of the cyber threat landscape since the Federal Information Security Management Act, FISMA, was created. Now is the ideal time to update this law to meet the evolving cyber threats.

My recommendations are based upon 30 years of Federal service, 10 of which were spent as a Deputy Chief Information Officer or the Chief Information Officer at two Federal agencies—the Environmental Protection Agency, EPA, and the National Aeronautics and Space Administration, NASA.

The implementation of information security laws of yesterday and today are dependent upon Government employees and contractors. Their leadership to address cybersecurity risks should be lauded, and they are the reason the Federal Government has made so much progress. I am proud of the progress achieved by the teams I led at both the EPA and NASA.

The original FISMA of 2002 set the Federal Government on the path to strengthen its approach to information security, a bold and necessary move. The act recognized the importance of information security to our economic and national security interests and the importance of protecting individuals' data.

In 2014, Congress updated FISMA through the Federal Information Security Modernization Act to address the rapidly evolving information security threat landscape. Continuing to upgrade information security laws, regulations, and policies for the Federal Government is a must if we are to maintain our economic position in the world and national security.

As the refresh just contemplated, I urge you to continue a risk-based approach that emphasizes all types of technology—information technology, or IT; operational technology, or OT; and the fastest-growing segment, Internet of Things, IoT. All of these elements of technology are used by the Federal Government to improve mission effectiveness, efficiencies, and the customer experience.

There are several FISMA areas ripe for refresh. Some areas for your consideration, cyber aspects of supply chain risk management, the interconnectivity of Government operations, and the IoT.

The Federal Government must assess the potential risks posed through IT and OT and IoT supply chain prior to purchasing and deploying on Federal networks. There are well-resourced nation state cyber threat actors that intentionally target all tiers of the technology supply chain by embedding malicious functionality.

The Federal Government relies upon networks and devices that are interconnected between departments and agencies. There are only a few service centers for processing Federal payments. Thus, every department and agency are connected. These points of connection, if not properly upgraded, managed, and monitored, create greater cyber risk, including the easy transmission of malicious code. Also, the data while in transit are at risk of compromise if poor cybersecurity practices are employed.

Technological advances have provided opportunities for Government operations to be more effective and efficient. These advances increase complexity and risk, including cybersecurity risk. For example, the growth of telehealth and the Internet of Things medical devices such as heart and glucose monitors. This growth, especially during the pandemic, has allowed medical services to be delivered during a trying time, but they add risk.

The next iteration of FISMA must mandate Federal Government buy, use, and manage secure IoT. The adoption of technology has provided and will continue to provide opportunities to better serve the public. This adds cyber risk. Congress must continue to ensure that our Nation's laws keep pace with these advances.

Finally, and in addition to legislative changes, Congress must continue to hold the heads of departments and agencies accountable for addressing cybersecurity risks. This is about ensuring a culture attentive to cybersecurity risks. Please consider asking cybersecurity questions during all budget authorization and program hearings.

Thank you for the opportunity to appear before the committee today and testify on the changing cyber threat landscape and modernizing FISMA to meet this challenge. I stand ready to answer your questions.

Chairwoman MALONEY. Thank you.

Mr. Bitko, you are now recognized for your testimony.

STATEMENT OF GORDON BITKO, SENIOR VICE PRESIDENT OF POLICY, PUBLIC SECTOR, INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI), FORMER CHIEF INFORMATION OFFICER, FEDERAL BUREAU OF INVESTIGATION

Mr. BITKO. Thank you, and good morning, Chairwoman Maloney, Ranking Member Comer, and distinguished members of the committee. Thank you for holding this hearing today.

A recently released Harris and MITRE survey showed that more than 75 percent of U.S. residents are concerned about cyber attacks. Given the effect on Government operations of incidents like Log4j and SolarWinds, they have good reason to be concerned, and it's critical that we discuss here what can be done.

I'm currently the Senior Vice President for Public Sector Policy at ITI, the Information Technology Industry Council. Previously, I was the FBI's Chief Information Officer, and I have more than 25 years of experience with technology and policy issues across the public and private sectors.

At ITI, I work on behalf of 80 of the world's leading IT and cybersecurity companies. We believe that in an increasingly digital world, it's never been more important for Government to work with industry to promote effective, reliable, and secure Government services.

2021 began with the Federal Government responding to the SolarWinds cyber attack, a very sophisticated nation state supply chain exploitation that's one of the most widespread and damaging cyber intrusions ever. Only a year later, 2022 is beginning with the Federal Government responding to yet another cyber incident, a widespread vulnerability in Log4j, a very commonly used piece of open-source software. Log4j is so widely used that this vulnerability is one of the most significant cyber threats of at least the past decade.

In both cases, Government operations suffered serious adverse impact. Systems and capabilities had to go offline to limit the risk. Extensive manual work, including searching deep into logs and source code, was needed to find evidence of intrusions, and IT specialists had to test fixes to deploy them safely while minimizing impact on all the other interconnected systems.

There's a huge opportunity cost to doing such recovery work instead of planned activities such as system upgrades, which had to be delayed or even deferred.

Those major events bookended countless other major cyber attacks on critical industries, service providers, the defense industrial base, governments around the world, and other victims. Some widely reported, but others not. They show the need for new cyber policies that place continuous risk management at the forefront of the enormous demand for digital services and data.

Today, many Federal agencies struggle with cybersecurity stemming from three FISMA issues that prevent effective risk management decisionmaking. First, the law is overly focused on process and compliance rather than on outcomes. FISMA requires careful implementation of processes like inventories of systems, the use of approved security measures, and annual cybersecurity program reports. But it doesn't look at the real-time effectiveness of those processes, and therefore, it doesn't promote real risk management.

Second, FISMA creates duplication of effort across agencies. Today, each agency is individually obliged to develop its own information security programs with little incentive for leveraging shared services, sharing information, or accepting security assessments or best practices from other agencies. This can lead to considerable redundancies as agency security officials are frequently unable or simply unwilling to use the good work already done elsewhere in the Government.

And third, a comprehensive lack—a lack of comprehensive real-time information. Too much cybersecurity information collection comes from manual processes, annual updates, and according to agency-unique definitions. As a result, it's nearly impossible to obtain a clear, timely view of the state of information security across the whole of the Federal enterprise.

FISMA modernization must enable and promote continuous assessment of cyber risk. Better risk management, along with improved collaboration and communication, will enable Federal network defenders to have a more comprehensive view of all Federal IT infrastructure while allowing for increased efficiency and better outcomes.

In my full written testimony, I offer six recommendations as necessary steps to improve FISMA, reduce compliance burdens, and better protect our Federal networks and systems. Two key elements are the shift to managing risk based on measuring and evaluating security outcomes and breaking down across governmental barriers through increased sharing of security information and increased reciprocity across Government.

These recommendations and others are discussed in detail in my written testimony. While no recommendations can offer complete, ironclad protection against every newly discovered vulnerability or zero-day, an improved FISMA that includes these measures will help ensure Government is well prepared to prevent attacks and quickly respond even in the worst cases.

These improvements will help ensure agencies have a thorough understanding of the risks and invest resources appropriately, will increase confidence in the effectiveness of cyber defenses and response preparations, and ensure that Federal organizations coordinate and contribute to the whole of government cybersecurity. As well, these principles help to guarantee that CISA and OMB have the visibility they need without manual data calls. They help codify consistent cybersecurity strategy that enables the Government to deliver services more securely to its constituents while raising preparedness and the ability to respond to global threats.

Thank you again for inviting me. I look forward to your questions.

Chairwoman MALONEY. I now recognize myself for five minutes for questions.

The SolarWinds and Microsoft Exchange Server attacks show just how vulnerable the Federal Government is to sophisticated attacks from nation states such as Russia and China. Unfortunately, OMB and DHS did not have the full picture when assessing these attacks. They had to issue multiple calls for data from agencies, and some of the information they collected was incomplete.

Mr. Schneider, how did these weaknesses in data collection impact the Federal Government's response to the SolarWinds attack?

Mr. SCHNEIDER. Chairwoman, thank you for the question.

I think, and from my perspective—and I wasn't in the Government at the time when the Government was responding to those. But I think in general, the lack of having and agencies having accurate situational awareness of their environments slows down any response activity. And so when OMB and CISA need to issue a data call and agencies need to go hunt for and search for the information just to understand where their vulnerabilities may lie and where their potential exposure is to a particular incident, such as SolarWinds or the Exchange Server incident, they're already behind the eight ball.

And so, it just slows down any activity that they have to actually be able to respond and recover appropriately to such an incident.

Chairwoman MALONEY. And Mr. Schneider, what are the biggest problems with the current version of FISMA that was exposed by the SolarWinds attack?

Mr. SCHNEIDER. So, I think, and Gordon mentioned, the overly focus on compliance and on process. And I think a lot of compliance activities are necessary, but not sufficient for cybersecurity. They can be helpful. However, I really do think and agree with Gordon that if we have a FISMA, as we look at updates, that is more focused on agencies' risk management programs and their ability to, you know, protect wherever possible. But I think more and more we have to be in a position of presuming that a compromise either exists or is going to happen, be able to quickly detect those compromises and incidents, and be able to respond and recover to them, you know, swiftly and adequately is going to be an approach that will be more successful for Federal security.

Chairwoman MALONEY. Well, one of the weaknesses to me was the fact that once they got in, they could roam through nine different agencies. Seems to me we would want to ward off certain agencies from allowing them to roam and went massively through the private sector.

Is there any way we could sort of block off or protect that information? You don't have to answer now. Maybe we can talk about it later. But that seemed to me outrageous that they could gain so much information from one breach. They were able to get throughout America in so many areas gathering information.

Mr. SCHNEIDER. Yes, and——

Chairwoman MALONEY. The discussion—yes. Yes, Mr. Grant—Mr. Schneider?

Mr. SCHNEIDER. I mean, quickly, there are techniques to kind of minimize lateral movement once someone gets in while you're trying to deal with it. And we can certainly work with your staff on some ideas around those.

Chairwoman MALONEY. I would like to hear them.

The discussion draft that Ranking Member Comer and I released today would enhance information sharing on cyber attacks. This bill would also promote another important tool called endpoint detection and response. This tool uses data from every endpoint in an organization's network to automatically detect and block threats.

Mr. Nodurft, is it possible that endpoint threat detection would have made a difference if it had been adequately in place during the SolarWinds attack, and how would it protect against future attacks?

Mr. NODURFT. Yes, ma'am. Thank you for the question.

So, absolutely, endpoint detection and response capabilities can identify supply chain attacks and certain other attacks depending on the configuration setting if—EDR works if you have an understanding of the endpoints, and have it deployed across your environment in a way that allows you to track ongoing behavior.

I think the EDR deployed across the Government, to your question, would have been helpful against SolarWinds attack, and it's very important. That said, it has to be part of a larger solution set that fits into the broader zero trust architecture, which your bill also does. And I think it's important not to lose sight of that.

EDR is one aspect. We also need strong identity solutions. We need best in breed networking solutions. We need to have encryption across all of our networks.

That, combined with EDR, would be—would create a robust environment that really could help prevent future attacks that are similar to or even threats that we can't even—we don't even know about right now.

Chairwoman MALONEY. Thank you.

China has been trying to steal American intellectual property and trade secrets and health secrets for many years to support its own economy.

Ms. Wynn, as you know, NASA has been a repeated target of Chinese cyber criminals and other nation state actors desperate for American intellectual property. How have these attacks evolved in recent years, and what updates to FISMA would be most important to address these kinds of attacks?

Ms. WYNN. Thank you for the question.

Yes, NASA, like other scientific agencies, certainly see its fair share of attacks. There are several things within FISMA that will help, but to be brief, I want to emphasize the identity management piece. When you collaborate across the globe with your allies, it creates a very challenging and complex cybersecurity threat landscape. So, we do have to take hold and get to a better method for identification, matching who somebody is physically with who they are logically.

And then I want to emphasize the remarks regarding zero trust networks. If the networks that are used across the U.S. Government really say that I should never be let in until there is an appropriate handshake, that better protects us as individuals, as well as protecting the mission and the intellectual property created across the U.S. Government on a daily basis, and you have considered this.

And my final add to this one, to stay brief, is supply chain risk. Certain companies are targeted for insertion of malware, and the U.S. Government uses these companies on a regular basis. Taking a hard look at what we use in the United States Federal Government and making sure it's appropriate to use prior to deployment are ways that should help strengthen the network security as well as the identity necessary for us to do work with those that we want to collaborate with. And FISMA proposes many changes that help advance this area—these areas.

Chairwoman MALONEY. Thank you. I have many more questions, but my time has expired.

Attacks like SolarWinds underscore how quickly cyber threats evolve. Our bill, our bipartisan bill, the FISMA Act of 2022, will help the Federal Government stay ahead of the curve. I look forward to working with the ranking member to move this legislation forward.

I now yield to the gentleman from Georgia. Mr. Hice, you are now recognized for five minutes. Mr. Hice?

Mr. HICE. Thank you so much, Madam Chair.

And I want to thank all our witnesses for being here and for the testimony that each of you have provided.

Ms. Franks, I would like to begin with you. Next week, we will be having a hearing dealing with the latest installment of the FITARA scorecard, and I guess I just would like to hear from you, in your opinion, does the cyber—the current cyber assessments that are required by FITARA, does that give Congress an adequate and accurate view of agencies' cybersecurity posture and security?

Ms. FRANKS. So, unfortunately, the short answer is no. There are some significant gaps in the scorecard metrics that would make it a little bit challenging for those sensitive cybersecurity details to be shared.

Presently, the scorecards' data is all available publicly and is accessible by anyone that needs to kind of pull and review that context of data. But a lot of the work we do at GAO and even the other agencies with their IGs are investigating specific security controls that provide those necessary cybersecurity protections for those various unique environments. And oftentimes, even for our own reports, we have to go through sensitivity reviews, given the context of what we've seen and what we've done.

So, if going toward a scorecard where you're identifying some of the needed cybersecurity controls, some kind of bringing some light to them, it's going to have to be an effort where the committee works with the executive committee's leadership to look at what types of information would be best suited for a publicly available report. And absolutely, GAO can assist in that effort as well.

Mr. HICE. Thank you very much for that answer.

Mr. Nodurft, let me swing over to you. Do you believe, as we are talking about FISMA legislation, are there parts of this or similar legislation that you believe should sunset in order to prevent current reforms from becoming outdated or even counterproductive as the threat landscape changes, as we all know, with technology?

Mr. NODURFT. Absolutely, Congressman. Thank you for the question.

Look, FISMA went for 12 years without a legislative update, followed by another seven years without a legislative update, eight—will be eight. So, I think that the frequency in changing of technology and the frequency in changing of tactics and threats that attack that technology is moving at a blistering pace. So, I think we need to take a very hard look at the legislation in its entirety on a more regular basis.

So, I think that sunsetting the legislation is extraordinarily important. I think that there are certain provisions that probably could stand longer than some other periods. But I do think that it is important for Congress to really take a hard look at how we're approaching security holistically over this piece of legislation and, like I mentioned in my testimony, several others to include FITARA, which you guys are going to cover, earlier on a more frequent basis and really consider how these pieces of legislation that were built around legacy technology, that were insular, that were at different departments and agencies, that were built on mainframes and closets, how this has evolved to—to—and look at the laws that are governing these new systems, these cloud-based environments and figure out how the laws interact with each other.

So, yes, I think some of these provisions could sunset, and I think that this is an opportunity for you guys to really consider how to drive good, secure policy for the next five years.

Mr. HICE. Well said. And I agree with you.

Let me ask you just one more question, and I will yield back. In your experience, are there any Government procurement or contracting rules that potentially could hinder the strengthening of our cybersecurity that needs to be addressed in the FISMA legislation?

Mr. NODURFT. So, yes, I appreciate that question as well.

I think that there are—I think when you look at procurement policy, it's not so much the procurement legislation as it is the compliance that underpins the procurement. And you know, Gordon covered it earlier. I think we'll hear about it some more. But I really think it's imperative that we take a hard look at what the compliance is for the security parameters that we've defined.

So, we've set the standards. We've said you—agencies, you need to—you need to make sure that your vendors that you bring in are maintaining the standards. But what we see sometimes, and whether it's because the work force is stretched too thin or people don't understand the systems, there is an overemphasis on compliance as opposed to doing the hard work to say, OK, here is my risk. Here is the security that meets my risk, and therefore, I can bring in more technology faster. So——

Mr. HICE. Well, you—just for example, you mentioned a moment ago the cloud. All right? So, here we go. We have a broad, wide

Federal adoption of a more secure and modern cloud protection. But it is so—it is so broad. Does that type of requirement in procurement or contracting, does that hurt us? I mean, what needs to be done to help in that area?

Mr. NODURFT. Well, honestly, I think the bill that you guys have passed recently, the FedRAMP, to modernize the way that the FedRAMP process is working really pushed that forward and can do yeoman's work into bringing the compliance process forward that will allow more innovative technologies to enter the marketplace.

That said, what we need to do is we need to really elevate the compliance policy that we're getting behind and drive reciprocity across the other compliance regimes that we have. We've got some different compliance regimes over at DOD. We've got different compliance regimes for on-prem and hybrid systems.

The companies that are trying to bring their technology to bear want to be able to come in, prove that they're doing what they need to do to be secure, and then be able to leverage that one set of proof across all these agencies and across all these compliance regimes. So, I think the start with FedRAMP is great and looking forward to working with you more on that.

Mr. HICE. Very good. I yield back, Madam Chair. Thank you.

Chairwoman MALONEY. Thank you. The gentlelady from the District of Columbia, Ms. Norton, is recognized for five minutes.

Ms. NORTON. Thank you, Chairwoman Maloney, for this important hearing, and I thank all the witnesses.

I was here when the 2015 data breach occurred. Twenty-one—the personally identifiable information of 21 million people was breached. As a result, I have repeatedly introduced legislation that will require OPM to make permanent free identity protection coverage that Congress required OPM to provide for only—excuse me, for only 10 years.

Mr. Schneider, I believe you were involved in OPM's response to the 2015 breach. How long after the breach was discovered were congressional leaders notified?

Mr. SCHNEIDER. Ma'am, thank you for the question.

I was. I went over to OPM shortly after the breach was, I guess, notified to the White House. I was working at the Office of Management and Budget at the time. As I tell people, I went to OPM for three days and got to leave nine months later.

I don't have a specific answer. I don't recall the answer because I wasn't there on the timeline between when it was identified and when—when the notification took place.

Ms. NORTON. So, you don't have any idea how long—how long individuals, it took to notify individuals as well?

Mr. SCHNEIDER. So, the individual notifications, there were broad notifications put out publicly that of the fact once—you know, after Congress was notified, the White House was notified, and Congress was notified, there were broad notifications put out in the media of the incident.

The individual notification, the letter that probably many of the people here received from OPM that was many months later, after extensive forensics work and research into identifying who was impacted.

Ms. NORTON. Yes, that is the point I am trying—that is really the point I am trying to make.

Mr. SCHNEIDER. Yep.

Ms. NORTON. Public notification is an important component of the response to any Government data breach. That was why I asked that question.

Now, Mr. Schneider, the chairwoman, Chairwoman Maloney, the legislation she and the ranking member have introduced would clarify requirements for notification of both the public and appropriate Government entities. So, how would the requirement in the chairwoman's draft bill improve public trust—that is my interest, public trust—that they will be notified in a timely manner in the event of another data breach?

Mr. SCHNEIDER. Yes. And my recollection from looking through the House discussion draft last night is that I think the congressional notifications would have to take place within 72 hours of when an agency had determined a major incident. So, I think, you know, that's a much accelerated—currently, the FISMA 2014 legislation is seven days. So, that accelerates that significantly.

It also puts in, and I believe it was a 45-day timeline, to begin the individual notifications in the event that an agency had determined that, you know, notifications of breach is necessary to individuals. And so, I think from a public confidence standpoint, certainly as a citizen being on the receiving end of that, that is a much more aggressive timeline, and I think that will increase public confidence in, you know, the notification.

Obviously, your confidence is low any time you learn that your data has been breached. But understanding how that's being handled and how it's being dealt with can help to, you know, re-establish some of the credibility with the public during those times.

Ms. NORTON. Well, several months went by before cyber attacks were able—went by before they were detected, the cyber attacks were detected, presumably increasing the amount of data they were able to access.

Ms. Wynn, how would you characterize the ability of agency Chief Information Officers to perform ongoing monitoring of cyber threats today?

Ms. WYNN. In my assessment and experience, those agencies that either embrace continuing diagnostic and mitigation programs or had already deployed tools on their network to answer two important and basic questions regarding network management. Who is on your network, and what is on your network? And when the Chief Information Officers, in partnership with the heads of agencies and the Chief Information Security Officers, took very seriously the responsibility of monitoring, you see the ability to respond decrease, which is the right thing that you want to do.

When you don't monitor your systems or have poor monitoring systems or don't look at the data on a regular basis by using artificial intelligence, robotics, and other tools available to you, then you increase the likelihood of significant damage, and it—because it takes you so much longer to respond, and therefore, you can't inform those that have been impacted by that breach.

Ms. NORTON. Ms. Franks, because GAO is auditing FISMA implementation of Government by interviewing cyber experts across the agencies, my question to you is what has the feedback from agencies been regarding the guidance pursuant to FISMA about continuous monitoring and how best to access the security of their systems? Ms. Franks?

Chairwoman MALONEY. The gentlelady's time has expired. The gentlewoman may respond, but her time has expired.

Thank you.

Ms. FRANKS. I can certainly respond. For GAO, the ongoing review, we didn't get into the details of the CDM process with FISMA implementation. But the new legislation that's being proposed does cover increased data automation, and as Ms. Wynn just discussed, increased data automation comes from CDM implementation.

There are certainly other tools and technologies out there, as well as the guidance from the binding operational directives, as well as OMB, who have already kind of distributed the guidance to the Federal agencies as to what they should be doing and how they should be acquiring those tools and then identifying what's needed specifically for their various unique environments.

We did do a CDM tailored review. That report came out August 2020. And in that review, we did a case study of three agencies, and all of the agencies had acquired the necessary tools for continuous monitoring services in their environment. Where they lacked was in the implementation.

And this FISMA reform effort will cover all of those lack of compliance, lack of assessment that were needed to be complete to make that CDM process whole.

Chairwoman MALONEY. Thank you.

Ms. FRANKS. You're welcome.

Chairwoman MALONEY. All right. The gentleman from Wisconsin, Mr. Grothman, is recognized for five minutes.

Mr. GROTHMAN. Thank you. And thank you for having this hearing.

I got a couple of questions for Mr. Nodurft. OK, the first one. What do you think the current status of the Federal Government's software supply chain—how does the current status of the Federal Government's software supply chain place agencies at risk?

Mr. NODURFT. Thank you for the question, Congressman.

I think that we have it's across Federal departments and agencies as well as most IT ecosystems, we are at the stages where we don't have a robust software development lifecycle process fully implemented across Federal departments and agencies. And I think that as NIST is developing those requirements, we—we—the Government needs to do a better job of recognizing where and how they need to implement those software development lifecycle processes and to govern their supply chain risks more broadly.

Mr. GROTHMAN. If you wanted to grade us between an A to an F, how you would grade us right now?

Mr. NODURFT. I think it depends on the agency, Congressman, to be perfectly honest with you. I think some agencies that I have interacted with are doing a very, very good job of it, and some agencies right now are at their infancy stage.

Mr. GROTHMAN. OK. To what do you attribute the difference?

Mr. NODURFT. It's resourcing is one. I think maturity in thinking, frankly. I think what you tend to find or what I've tended to find in my previous role is that some of the agencies whose missions are core and foundational around security tend to have a more forward-leaning security mindset, whereas others who are less focused on that tend to not.

Now that's not a conclusive statement. There may be some agencies that have moved forward, but I would say that in general, it's—some of it's core to certain agencies' DNA, and then other ones that have more resources tend to do a better job.

Mr. GROTHMAN. OK. How have agencies successfully implemented FISMA lines of authority in responding to cybersecurity threats?

Mr. NODURFT. I'm sorry, Congressman. I couldn't catch that. Could you say that one more time?

Mr. GROTHMAN. How, in your opinion, have agencies successfully implemented FISMA lines of authority in responding to cybersecurity threats?

Mr. NODURFT. I think—so agencies have—I would say over the past 5 to 7 years, we have seen agencies move their FISMA slowly away from some of the compliance-based efforts and started to invest in more risk-based approaches to security. I would say that a lot of that has to do with investments in cloud technology and investments in some of the zero trust technologies that have really helped drive some of the modernization efforts that help them comply with the FISMA risk-based outcomes that they're looking for.

Mr. GROTHMAN. OK. I will give you one more question. I think that is going to be all we have time for.

Some companies offer services that provide a unified view of an organization's devices and digital infrastructure and, thus, a clearer picture of potential areas of risk and vulnerabilities. Why is it that there remains broad ignorance on the full scope of vulnerabilities posed by disparate systems and hardware used within many organizations when widely adopted private sector management tools are available to offer such insight?

Mr. NODURFT. Yes, and Congressman, I think that's a great question, and I think your point is well taken. We are—the Government right now is at a turning point, and it needs to shift the way that it invests and partners with the private sector to leverage some of the technologies that are out there to enable broader access.

I think the work that the committee is doing on the bill today is going to really push the ball forward and enable agencies to focus on some of the technologies like what we covered with EDR and like some of these zero trust technologies that are going to enable access.

What I would—what I would double down on here is that we have an—or the committee has an opportunity to open the aperture for how we do compliance, security compliance, and make sure that we are removing as many barriers as possible so that these innovative technology companies can come in and provide their services across agencies and across compliance regimes. "Check once, do many" type approach.

Mr. GROTHMAN. Thank you very much.

Mr. NODURFT. Thank you.

Chairwoman MALONEY. Thank you. The gentleman from Massachusetts, Mr. Lynch, is now recognized for five minutes. Mr. Lynch?

Mr. LYNCH. Thank you very much, Madam Chair, and I thank the ranking member.

Before we go into zero trust principles and architecture, I do have a question about where we are with the Log4j software vulnerability. We have a great group of witnesses. Can anybody tell me where we are in terms of patching that vulnerability?

I understand that that code is ubiquitous. It is very, very widespread. Do we have a sense on where we are in patching that vulnerability, both Government side and also private sector? Anybody?

[No response.]

Mr. LYNCH. Yes, OK. That is what I was worried about. I do realize that is no easy task. So, it would be helpful, Madam Chair, if we could get somebody to give us a read on that.

Let us talk about zero trust architecture and the principles that are contained in the ranking member and the chair's draft legislation. Now zero trust principles require that users be continually validated so that we don't have to run the risk that a bad actor is actively engaged in one of our—one of our programs.

But I know that several of you, several of our witnesses have expressed a little bit of concern about whether or not our Federal employees and the users of zero trust technology and architecture could adopt that quickly. I think, Ms. Franks, you might have said it is going to take—it is going to take a change in lifestyle and patterns of behavior in order to adopt that. Could you elaborate on that? Are we going to have problems in moving to that type of architecture?

Ms. FRANKS. Yes, absolutely. I do believe I have said that several times in recent settings.

So, the fundamental problem across Federal agencies, and I have been with GAO since 2006, and I've audited several agencies at this point—Government-wide reviews, agency-specific reviews—and the fundamental problem across the agencies is identifying what's in your inventory of systems. So, with zero trust architecture, knowing what you have before you can even protect it is key. That's going to be your No. 1.

And with agencies unable to really give us a firm attestation as to the inventory of their major information systems and then the data that resides on those systems, we're going to have difficulty preventing those that may need access or may not need access to those systems and services. How will we protect? How will we be assured that the adequate protections are in place to prevent certain situations from happening?

So, with the zero-trust making us not—not permit anyone and making everyone be reauthenticated into the services continually through the day is going to be helpful for agencies, but what's not going to be helpful is if the agencies can't really just get that fundamental handle on their networks.

And you asked a question about Log4j, and I know what GAO has been doing because I do have that sit at the table for our agency. But agency wide—I mean, Federal Government wide, I cannot say that they have the necessary procedures in place to quickly contain that vulnerability and then perform the necessary eradication procedures.

Mr. LYNCH. OK, thank you.

Mr. Nodurft, Mr. Schneider, or Mr. Bitko, any thoughts on the adoption and implementation of zero trust architecture and principles across Government?

Mr. BITKO. Sure, Representative Lynch, I'll jump in with an answer on that.

I think the challenge is what Ms. Franks was starting to hint at. Agencies don't have a comprehensive understanding of their data assets, and at the core, for zero trust to be effective, it's about what that data is, what that information is, and who should have access to it. Today, that's a very challenging thing for most agencies because of the dispersed nature, the federated nature of their infrastructure, the fact that the data can be dynamic, the people can be dynamic because they change roles over time.

So, when you put all that together, zero trust is absolutely the right thing to be doing, but at the same time, having the visibility to do it effectively is really, really difficult. That's one of the reasons why we've talked a lot about focusing on risk and understanding where the highest risks are and start there.

You cannot possibly boil the ocean of all of your data and zero trust at one time. You have to pick what are the most critical assets, what are the things that are the crown jewels of the agency, so to speak, that if they are compromised, the cost to the agency is unacceptable.

Start with them and manage them and manage those data and the rules around them first, and then expand outwards. There's got to be an understanding that that's going to take a long time. There's so much legacy technology. There is so much in the federated landscape that it's not going to happen overnight.

And I think, sir, by the way, that that's the same answer to your Log4j question. People will know up front at the high level where does Log4j exist. But when you have this dispersed federated enterprise, and Log4j might not be the product that you're using yourself. It might be buried three or four or five layers down in a product that was provided and acquired years ago. And that's hard to have visibility into, and agencies are struggling with that.

Chairwoman MALONEY. Thank you. The gentleman's time has expired.

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

Chairwoman MALONEY. And I thank you for your questioning, and we will have a briefing on the challenges of Log4j, as you requested.

Thank you.

The gentleman from Ohio, Mr. Gibbs, is now recognized for five minutes. Mr. Gibbs?

Mr. GIBBS. Thank you, Madam Chair.

To the panel, back in FISMA 2014, the main emphasis, my understanding and my memory, was to build more collaboration and coordination with the public program and the private sector and especially through the Infrastructure Security Division. I was wondering if anybody on the panel can maybe give me an update how successful since 2014 building more coordination and collaboration with the private sector entities, or has it been a real challenge? What is the status?

Ms. FRANKS. Well, I can go first. I do cover the COVID–19 portfolio for the Government Accountability Office, and in that, there was a report issued November 2020 and a subsequent full report on HHS's cybersecurity roles and responsibilities issued June of last year. And in both of those reports, we highlight the coordination and collaboration that the Department was performing across its public health sector as well as all of their component agencies.

Given the uptick of cyber-related vulnerabilities that were impacting the healthcare organizations due to the coronavirus pandemic, they had to lean on the coordination and collaboration, starting at the CIOs and then to the CISOs. They definitely leveraged all of the communication that we had—that was supplemented by CISA and the FBI and the like.

But they communicated with the states and local departments as much as they needed to, to make sure that all entities that were impacted on the Federal level that could perhaps be impacted on those state and local levels, as well as some of those private industries—you know, there is patient research institutions and pharmacies and the like. So, they were always collaborating and still to this day doing so.

Mr. GIBBS. OK. Just to kind of followup, maybe Ms. Wynn or somebody else might want to jump in, when we are looking at certain sectors like banking, utilities, transportation, and defense, has that status with the private sector improved, or is there challenges there? Is there challenges because they are afraid of liability issues, or you know, can you expound on that? Maybe Ms. Wynn might be a good one on that?

Ms. WYNN. Yes. Thank you for that.

I think it is domain-specific in terms of whether you experience some challenges in that and where the trust lies between the private sector and the public sector in terms of collaboration. We're seeing certainly in the space domain, where I last served, is they definitely collaborate across international space agencies and with some of the main contractors that focus on space and specifically in low-Earth orbit. But there's always more that can be done in this area because the threats change, the entry points change and that.

And so, a concerted effort to collaborate across critical infrastructure or the whatever domain that you have to work in is absolutely critical in order to secure for national security purposes.

Mr. GIBBS. Do you think we can do this on a voluntary approach or legislation that mandates more collaboration with the private sector?

Ms. WYNN. I would say I would suggest a framework from a legislative perspective, and then—that would be at the high level. And then how some of that effort is done and where the recommendations flow, I think I would leave it up to the teams that are established in order to put the information in the right hands. But the framework and requiring collaboration is definitely a piece to the cybersecurity mindset.

Mr. GIBBS. OK, thank you.

Mr. Bitko, why is it we are seeing so many vulnerabilities in widely used software produced and developed by large private sector companies?

Mr. BITKO. Congressman, thank you for the question.

I think that the answer is software technology is just incredibly complex. And the adversaries who are out there are really sophisticated, and so they are going to find weaknesses when they exist. It highlights the importance of us collaborating together, and I'm going to tie this back to your last question.

I think that there is a lot of room still to increase trust between Government and industry to ensure that that information is flowing in a timely manner. Today, a lot of the time—and it's understandable—there are investigative or intelligence priorities which limit the ability of information to be shared back, but that sometimes is what reduces the trust that we have on the industry side now because what we get back from the Government is sometimes a day late and a dollar short.

And so, it's important to share that information, to have vulnerability discussions, to have that all going in a regular and continuous and ongoing basis. And we've improved. The JCDC with CISA, for example, is a good step forward, but there's still more work to be done there.

Mr. GIBBS. It sounds like build trust to make sure that the private sector can trust the Federal Government. Maybe we need some sentences in there that gives us some protections to try and do the good things.

You know, obviously, if there are bad actors, we have to go after them. But to try and do the right thing if it doesn't go quite right, you know, maybe it has to add some protections. Would you agree?

Mr. BITKO. Yes, absolutely.

Mr. GIBBS. Thank you. I yield.

Chairwoman MALONEY. The gentleman's time has expired, but you may answer—OK, it is over? All right.

Let us now go to Mr. Cooper. Mr. Cooper, you are now recognized. Mr. Cooper?

Mr. COOPER. Thank you, Madam Chair and Ranking Member.

I am glad that we are considering bipartisan legislation today, but I am still deeply worried. If I were the average person sitting back home watching this hearing, I think I would doubt that any of our Nation state adversaries were shaking in their boots, especially now that they have franchised a lot of their activities to criminal gangs that are even doing things like conducting ransomware attacks on small businesses across America.

So, I think the first question in a hearing like this really should be what is Congress' role, if we have a role at all in this? It has already been cited by one of the witnesses that we took 12 years one time to update the legislation. It took seven years another time. That sounds to me like too little too late. We can't always be playing catch-up.

So, is there a way that Congress could delegate or step aside or get this done faster? Because I am worried, we will always be late and slow.

Mr. BITKO. Congressman, if the approach is to provide recommendations on specific technologies, then absolutely. That's setting everybody up for failing, to be too late and be too slow. The pace that technology moves at just does not allow for legislation to keep up with that.

But I think if you have a risk framework and you have clear authorities within the Government about who is responsible for saying this is the highest risk or highest risks and these are the things that we need to hold agencies accountable to do, you can have the right balance of centralized control and prescription with flexibility that you need for each agency to deal with its own risks, to understand that its landscape is different, that the threats it faces might be—might be varied.

So, I think you need to strive to find the right balance there, not have legislation that is super prescriptive but allows the right framework to have that flexibility within agencies to provide particular technology solutions.

Mr. COOPER. Thank you. My second question is even more aggravating. Isn't this all just a vendor gold mine? Companies sell us software that turns out to be easily hackable. We get hacked, and then they sell us more software that is also easily hackable.

And people know out there that the Federal Government is one of the biggest, dumbest customers in the world. We also have the slowest reaction time. So, that makes the breaking and entry even more violative, even more dangerous for us, and yet we are not asking vendors for warranties or closer collaboration. It just, as I say, ends up being a gold mine for the companies.

How am I wrong?

Mr. SCHNEIDER. So, Congressman, I think I would say that, you know, certainly the vast majority of the companies and the ones that I work with are seeking to produce tools and capabilities that are resilient and are defendable and don't have vulnerability. As Gordon mentioned earlier, you know, technology is immensely complex, and technology is written by humans and ends up having failures.

And you're certainly right. You know, some of the companies that are bringing us solutions are getting hacked and then claiming to be the solution to the hacks as well. And you know, I do think, you know, we need more diligence, and we need more accountability, and we need to expose that type of behavior and those instances. But at the same time, I don't know what another solution would be.

We are dependent on commercial industries to bring us these capabilities. I would also say that it's not unique to Government. Government is buying commercial capabilities are the same ones being employed in industry, and industry is facing a lot of the same challenges.

Mr. COOPER. I only have a minute left. Government is well known to have a slower reaction time. Remember, in many other areas of commerce, the products come with warranties and guarantees.

Final question. There are some major utilities in the United States who have a day without cyber. That is even a day without cell phones, a day without smartphones, so that they can guarantee to their customers that they know how to run a business in the event of a major catastrophic hack. Is that too catastrophic of planning techniques? Is that too much red-teaming or preparing for the worst?

How can we guarantee our folks back home that they are going to be safe from electricity outages in cold weather or communications outages if companies don't even know how to run in the event of a major hack?

Mr. BITKO. Congressman, companies and the Government need to be prepared for all scenarios. The core of the cybersecurity framework, which I think has come up already a couple of times, has in it how do you respond when an incident happens, and how do you recover? Agencies and companies, if they're not taking that seriously, and that means senior management in the companies or the agencies actually exercising that and being prepared, then they're being delinquent.

They need to understand that that's a risk that they face, just like if you're a utility and you're faced with a natural disaster and that takes your capability offline. You need to have a response plan for that, the same way you need to have a response plan for a major cyber attack. And we should expect the same of Government agencies.

That's just the world that we live in, as Grant noted. And you know, it's been said by cyber experts the only way to be secure is to take your computer, unplug it, disconnect it, turn it off, and bury it underground. And then maybe it will be—it will be safe, right?

But that's not what Americans expect as the services that they're going to get from Government. So, I don't think that that's a viable solution. We've got to find ways to work together.

Chairwoman MALONEY. The gentleman's time has expired. The gentleman from Texas, Mr. Sessions, is now recognized for five minutes.

Mr. SESSIONS. Madam Chairwoman, thank you very much.

And by the way, this is a very successful hearing, and I want to thank you and Mr. Comer and, in particular, both staffs for the preparation.

I would like to focus on two things. No. 1, we received in our packet what is called GAO at 100 Highlights, and it says, "Preliminary results show that agencies' implementation of FISMA requirements was inconsistent." And this tends to show at least preliminary in—preliminarily that consistently 2017, 2018, 2019, and 2020, about 6 or 7 agencies had effective rating scores, and the others were called, some 17 or 18, not effective.

We are now talking about us updating, highlighting, and revising things that we have since learned in law, and yet it is taking agencies a long time. What keeps them from effectively becoming effective under this rating system by GAO?

Mr. Bitko, I will go with you.

Mr. BITKO. Congressman, thank you for the question.

I think that there's a few things that are inherent challenges to agencies' ability to be effective when it comes to FISMA scoring. They do not appropriately prioritize it at senior-most levels in the agency sometimes to ensure that the right resources are focused on the right activities. And it's got to really start there. So, that's—that's No. 1.

But then I would say that they faced a lot of the challenges that we've talked about during the course of this hearing. The lack of reciprocity means work needing to be redone from agency to agency, and that's not the most effective solution.

The focus on purely the compliance and the implementation of the upfront activities, rather than looking at the outcomes in themselves, I think that all of those, when you take them together, mean that agencies just are not focused on the right things when it comes to successful cybersecurity a lot of the time, unfortunately.

Mr. SESSIONS. Very interesting. And that goes back to your comments about compliance rather than outcomes or processes, that the management of the organizations find a way to move, kick the ball down the road perhaps. Perhaps it is difficult. Perhaps it is muddy. Perhaps it is lack of management intent.

I would like to now shift the other half of my time—and Chairwoman, thank you very much. We have not talked about prosecution levels and the ability—and, sir, you represented the Federal Bureau of Investigation for a number of years, and I know it is essentially an internal process that you did. But I have not the word really "FBI" or "Secret Service" today from the perspective of their deterrence to actually go and prosecute.

Do any of you have an opinion, while it may not be your main source, an opinion about what we need to do proactively to have a strong law enforcement perspective of prosecution?

Mr. BITKO. You're talking, Congressman, about cyber threats and criminal investigations of cyber actors?

Mr. SESSIONS. Yes, sir. I am talking about once you have figured out that you had an intrusion and then you then go to law enforcement and share that information, I have not heard the word "Secret Service" today. I have not really heard the word "Homeland Security." But how are we doing at then passing this to law enforcement and expecting them to do something about these bad actors?

Mr. BITKO. Well, I think that there have been steps taken. It's clear that—I'll speak a little bit to what I know from the FBI Department of Justice perspective. They have certainly elevated cyber threats and cyber crime, ransomware, and things like as priorities that they look at and focus on.

It takes a lot of work and a lot of resources for sometimes difficult returns because the bad actors are not in a territory where we can actually arrest them a lot of the time, right? And so it's particularly challenging. I think it's something that's got to be continually discussed by all stakeholders.

I also think, Congressman, it's important to ensure that there are the right mechanisms within Government to find the right balance of offensive and defensive. I don't know that those conversations are always happening today at the right levels within Government to make a determination about what is the right mechanism in this case. Does it continue to live with the vulnerability because it's allowing for a law enforcement investigation to continue? But there's a cost to Government agencies or the private citizens who might be compromised.

I think that in the roles and responsibilities in FISMA that you're looking to define where there's clarity for the National Cyber

Director and others, that's got to be a part of their responsibility, too, to help figure out what that balance is.

Mr. SESSIONS. Just as a response back to you and our other witnesses, I believe our chairwoman, I believe our ranking members on both sides have done a very good job at trying to highlight this. We had a hearing a few weeks ago from Homeland Security and others, and I have now heard it from your perspective.

Madam Chairwoman, I want to thank you for conducting this hearing and the quality of witnesses we have had. Madam Chairman, I yield back my time.

Chairwoman MALONEY. Thank you. The gentleman from Virginia, Mr. Connolly, is now recognized. Mr. Connolly?

Mr. CONNOLLY. Thank you, Madam Chairwoman.

And let me just begin by responding to our friend Mr. Cooper and some of his observations about the Federal Government. I do think we in Congress need to take responsibility for the fact that, frankly, this is a much neglected subject.

The fact that it took 12 years to update FISMA, you know, and another seven years to have a hearing about it, I don't think speaks well about the legislative branch and the priorities we put on information technology and its security. And you know, the President asked for $10 billion as part of his COVID relief bill earlier in March, and the Senate zeroed it out, zeroed it out, arguing that IT wasn't directly relevant to COVID.

Well, everything we do sits on an IT platform, and yet the lack of awareness of that by Members of Congress, serious Members of Congress who control appropriated dollars, was—you know, told us we still have a lot of work to do in educating ourselves and our colleagues about the criticality of IT, protecting it, making it efficient, upgrading it, and making investments in it. And that has been the work of our subcommittee for the time I have been on the committee.

Ms. Franks, in your testimony, you talk about impediments for agencies to address 900 open GAO recommendations related to cybersecurity. Is that right? Nine hundred?

Ms. FRANKS. Yes, it's 900 open recommendations.

Mr. CONNOLLY. That is a lot of recommendations. Just really quickly, but I mean, what are these impediments to addressing those recommendations?

Ms. FRANKS. So, starting with the lack of resources, both financial and people. Obviously, we know talent acquisition across the Federal Government is a significant concern and has been since we put cybersecurity on the high-risk report 25 years ago. So, looking at the IT and cyber work force issues, a lot of agencies have to contract out certain services because of those resources.

Management attention, like you just noted. A lot of folks understand a breach once it's happened because it significantly perhaps may impact you as an individual and compromise your personally identifiable information. However, there is a lot of work to do with just understanding that almost all processes that we have operating through the Government to service the American people come from an automated service.

So, like we noted the example earlier of shutting it off and then burying your device. That is the only way to prevent some type of cybersecurity event from perhaps causing a vulnerability in those networks. And with the increasing technologies, as Ms. Wynn discussed earlier, and the growing rate that they're increasing, it's hard for some agencies to kind of stay ahead of looking at open recommendations while they're also trying to implement new strategies to ward off these cybersecurity threats in their environments.

So, it's not from a lack of trying. I do highlight of those 900, it's fully implemented. We do work with the agencies quite a bit to understand where they are in the progress of meeting the intent of closing those recommendations, but sometimes even their partial addressing doesn't fully close a recommendation.

Mr. CONNOLLY. So, we may want to work with you and followup on that. You know, we are getting ready for the FITARA hearing, our 13th FITARA hearing, and we are working very closely with your agency. We may want to fold what you just talked about into that in terms of how we can help in encouraging compliance.

Final question, Mr. Bitko. You talk about ensuring consistency through a holistic Government-wide approach to updating FISMA. That sounds like a lot of buzz words. Could you in plain English tell us what you mean, what we have to do as we look at this draft legislation?

Mr. BITKO. Congressman, thanks for the question.

A few things I think are important to bear in mind. One when I say that is consistency in definitions. We have in FISMA—and it's been discussed here a little bit already—incident reporting and what the Government's responsibilities are, what their responsibilities are internally to report to you and to report to private citizens. Separately, Congress is considering incident reporting legislation. So, that's an example where it's important to have, I think, consistency in the language, in the terms and the definitions as much as possible.

Every time we don't, it creates additional work, additional overhead, additional things that get in the way of people being able to be effective and efficient.

I'll translate that to in the specifics of FISMA and security approvals. A company sells a product to one agency. They go through the full ATO process, the authority to operate. They get all the security controls that they've got in place approved, and that's great. Then they can use it in that agency. It does not always directly translate to another agency being able to just take all of that good work that's been done and say we can apply that in our environment.

Frequently, what happens is they go through the same exercise all over again themselves. They find all the same issues. They come up with all the same solutions, but they've just spent a lot of time and energy being inefficient instead of leveraging the work that's already been done.

Mr. CONNOLLY. Thank you.

Chairwoman MALONEY. The gentleman's time has expired. Thank you so much.

The gentleman from Florida, Mr. Franklin, is now recognized for five minutes.

Mr. FRANKLIN. Thank you, Madam Chairwoman.

My first question is for Mr. Nodurft. In the wake of the disclosure of the Log4j vulnerabilities, the Director of CISA cited this as another reason for agencies to gather and utilize software bills of materials, SBOMs, which was a new term for me, as part of their cybersecurity programs. Do you recommend we codify in law the requirement for agencies to collect these software bills of materials from their vendors for critical assets?

Mr. NODURFT. Thank you for the question, Congressman. I appreciate it.

I think that there is a lot of work right now going on in the administration in the wake of the cybersecurity executive order that talks about what exactly is in an SBOM. So, I think when the committee discusses what it would look like to codify SBOM language, it's important to—to consider the availability of SBOMs, what the extent of them looks like, how those SBOMs are going to be utilized, what the definition of what's incorporated inside those SBOMs look like.

So, to answer your question, I think that it is a—you have—the committee would have to give, if they were going to codify it, they would have to give the flexibility to apply the use of SBOMs in targeted manners that make sense for the risk-based environment. And I know that's a nuanced answer, but you may not need an SBOM for every piece of software everywhere across all of the environments if they're not really risky assets.

So, I think we need to be very conscious, the committee should be very conscious about how—if they were to consider codifying it, how that would be applicable in the Federal environment. We don't want to—we don't want to overburden the industry providers that are building this backbone for the departments and agencies.

Mr. FRANKLIN. Great. Appreciate that.

Ms. Wynn, speaking of—and you talked about supply chain risk management and the burden on our vendors. This had me thinking there are—there are already a number of provisions that codified there in law that require vendors to use trusted sources and their components. Unfortunately, though, we know that many times vendors are accepting attestations of compliance from their subcontractors instead of doing the asset security training themselves to verify.

How do you recommend that we enforce the existing provisions? Are those necessary? Are they stringent enough? Are they over-stringent on these vendors supplying assets to the Federal agencies?

Ms. WYNN. Thank you for the question.

I personally believe that you need to take very strong action regarding supply chain risk and cybersecurity. This is—we have seen in the classified world actual efforts to target various aspects of software by well-resourced nation states, and then they go after the software that the U.S. Government and other government agencies use.

And so, if we take a strong stance and enforce against this and go further than attestation or accept attestation and when your attestation is proven to be false, then maybe that's where you need to place some of your enforcement.

Another thing, and then I'll give you your time back, is we also see that businesses may not always be very responsible in terms of the software that they hand back to the U.S. Government and how to use it. And so we need to be able to ensure and set the stage that if you're going to provide services and software to the U.S. Government, we need you to give us the best that you've got possible, and you've got to be responsible for the cyber threats that could come through that software.

Mr. FRANKLIN. And what sort of teeth should we put in that, in your view?

Ms. WYNN. Well, you know, having been penalized as an individual through my schooling quite a bit, I preferred the lighter method first, right? Let's have the discussion with the principal to talk about the behaviors that were not acceptable in terms of that, and then a few times there were needed to be some elevation, both to parents and then when we got to detention, fortunately not suspension. And I do believe that the elevation and layering the amount of enforcement matters first because sometimes people really do just make a mistake.

Humans do make mistakes. And so maybe making it on a tiered level so that the repeat offenders are actually called out a lot more harshly.

Mr. FRANKLIN. Thank you.

In the little time we have left, Mr. Schneider, I am encouraged by that the bill has strong language around zero trust but concerned that securing the Federal agencies isn't enough considering our reliance on the outside industrial base. What recommendations would you have for extending zero trust and other requirements beyond to the broader industrial base? And I realize I have given you 10 seconds left to answer that, so that may be unfair.

Mr. SCHNEIDER. Yes, I mean, I'll try to be brief. It's going to be really important to flow down, you know, the key cybersecurity requirements to vendors and contractors that are providing capabilities, and we're very dependent on, you know, DOD, the defense industrial base, but industry writ large. And we need industry to be providing and, you know, A, protecting their tools and then delivering us tools that are secure and resilient. So, I think there's a lot of work that we need to do, and it's going to have to be a collaboration with industry.

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

Chairwoman MALONEY. The gentleman yields back. The gentleman from Illinois, Mr. Krishnamoorthi, is recognized.

Mr. KRISHNAMOORTHI. I thank you so much, Chairwoman Maloney, and thanks for a great hearing.

I find this subject to be incredibly fascinating, but so frustrating because it seems like we are constantly on the defense in this particular space.

Mr. Schneider, I read an article in the *New York Times* talking about how in the last 18 months of the Obama Administration, security researchers and intelligence officials observed a notable drop in Chinese hacking. That is during the last 18 months of the Obama Administration. I wanted to ask you why did that happen?

Mr. SCHNEIDER. So, thank you for the question, Congressman.

The short answer is we don't know. I will say what we think is that we think there was an aspect of the engagement post the OPM brief—breach, excuse me, with the Chinese government with President Obama directly making a case to President Xi, and that perhaps had a direct impact.

And I think that, you know, that said, I don't think we're going to—well, I guess what I would say is in order to get at this, we need a whole of government response, right? We need diplomatic actions. We need offensive cybersecurity capabilities in order——

Mr. KRISHNAMOORTHI. Let me—let me——

Mr. SCHNEIDER. Sorry.

Mr. KRISHNAMOORTHI. Let me jump in because, otherwise, I know my time is limited. I think I know where you are going, and so I want to ask you a related question, which is in the law, you know, when you are attacked, there is a concept of self-defense. And most jurisdictions allow for self-defense measures.

In cyber crime or in a cyber attack situation, is there a similar concept of cyber self-defense where let us say a private company was attacked. Is it allowed to take any offensive measures to defend itself and to exact a price on the attacker in the name of self-defense?

Mr. SCHNEIDER. Sir, today, organizations are not able to do that. And I personally don't believe that we want commercial entities doing what's often to as "hack back," right? Attacking hackers. I think that there need to be consequences——

Mr. KRISHNAMOORTHI. Let me—let me—can I jump in? Because I want to—I want to build on that. Not so much hack back or an offensive strike on the source, but what if it were something that would exact a price on the attacker at the time of the attack?

In other words, is there any deterrent whatsoever for a Chinese criminal gang hacker who was attacking a U.S. entity or agency that would prevent them from doing it continuously and without any stoppage?

Mr. SCHNEIDER. I think those deterrents are going to need to be—come diplomatically and come from the Department of Justice perhaps in sanctions. But I think they're going to have to be Government-led deterrents and responses as opposed to individual company-led responses.

Mr. KRISHNAMOORTHI. OK. I guess it just sounds pretty weak to me at this point, given the merciless attacks from these criminal gangs. Secretary Blinken said that the Chinese Ministry of State Security has fostered an ecosystem of criminal contract hackers to go after our companies and our agencies at this point, both for state-sponsored activities and for private gain.

Is there a concept or an idea or a vision for us to employ a set of legal, almost contract bounty hunters on our side to defend our agencies against these criminal gangs from China, Russia, or elsewhere? How do we employ individuals or the best minds on our side, just the way that they are in going after us, in defending us as well?

Mr. SCHNEIDER. I think the—I think the current structures allow for the people with those authorities and the intelligence community and the Department of Defense to bring in outside support and help and assist them, but I personally think they need to do that under the authorities that exist, as opposed to any sort of like a vigilante or bounty system.

Mr. KRISHNAMOORTHI. I understand, but it is not working. It is just not working right now.

Last question. Is there another government that does it better than the U.S. Government in defending its cybersecurity assets?

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

Mr. SCHNEIDER. So, I don't know about specifics. I certainly think smaller governments and smaller organizations have an advantage. We have an advantage to our Nation of size and scope, but it's a bit of a disadvantage when it comes to cyber defense.

Mr. KRISHNAMOORTHI. Thank you.

Chairwoman MALONEY. The gentleman from Kansas, Mr. LaTurner, is recognized for five minutes.

Mr. LATURNER. Thank you, Madam Chairwoman.

And welcome to all of the panelists today. I appreciate you being here, and Happy New Year.

My first question is for Mr. Nodurft. The SolarWinds attack exposed a lot of confusion among different Government agencies on how to organize information and who was responsible. Do you agree that assigning the National Cyber Director as the primary executive branch official under FISMA to coordinate and report major Federal cyber incidents to Congress would effectively streamline the flow of information?

Mr. NODURFT. Thank you, Congressman, very much for the question.

I think that the legislation you're considering right now has an opportunity to ensure that what you're speaking about, which is aligning and streamlining reporting requirements and reporting to Congress, is enacted appropriately. I think right now we have several different leaders within the Federal Government space who are monitoring incident response, monitoring breach response, monitoring vulnerability response, and I think that this is an opportunity for the members of this committee to really direct—direct the Federal Government on ensuring that that flow occurs.

So, the National Cyber Director is just standing up, and I'm encouraged and bullish that that is going to be a great addition to the ecosystem to allow you guys—to allow the members of the committee to have the oversight and interaction that the committee is looking for.

Mr. LATURNER. Thank you.

Let us stick with you. What is the most effective way to update FISMA metrics and reporting to ensure necessary agency administrative compliance burdens don't take—that they don't overtake the mission immediate security workflow?

Mr. NODURFT. Thank you again for that question.

So, I want to talk about two separate parts of that. First, I think updating—updating the metrics is going to be very important, given the migration to more modern ecosystems, whether it's cloud-based, zero trust architectures. So, I think right now directing OMB to make sure that we are focusing less on how many controls and piece parts are in place and more on are we actually stopping and preventing outcomes is a key part of updating FISMA metrics.

For the second part, I want to discuss the—your question around how are we streamlining compliance requirements. And I think that—I said this in my testimony, I've heard Gordon talk about it as well—this is an opportunity for the committee to look across the different compliance frameworks that we have within Government right now, whether it's FedRAMP, whether it's FISMA, whether it's the impact levels of DOD, the forthcoming CMMC, and make sure that when a—when an innovative company comes forward and says we have the following solutions in place to ensure that our product or service is secure enough to go into the Federal ecosystem, that that process is reusable and is reused across both the agencies and the compliance frameworks that we just talked about.

Mr. LATURNER. Thank you for that.

Ms. Wynn, in your experience as a former agency CIO, can you explain the role of FISMA reporting requirements and how they affect the day-to-day operations of an agency?

Ms. WYNN. The reporting requirements did begin to drive behaviors within the organizations that I had worked, and I liked to see that. But what it took was actually paying attention to the metrics at a level outside of the agencies where I served and coming back to the heads of the agencies and saying here's where you are on the spectrum of performance.

I happen to, unfortunately, have sat in the seat of being at the end of the pack in terms of that performance, but having that conversation, having those metrics, and talking to the heads of the agencies gave the head of the agency the energy to delegate to me and to the CISO to go get stuff done. And we looked at every single network within the agency, which meant the complex mission networks were assessed on this one.

So, it has some really good benefit as long as you actually hold the agencies accountable to it.

Mr. LATURNER. Thank you very much.

Madam Chairwoman, I yield back.

Chairwoman MALONEY. The gentleman from Maryland, Mr. Raskin, you are now recognized.

Mr. RASKIN. Well, thank you very much, Madam Chair, and thanks for organizing this great hearing. I think we are all concluding that it is time to really modernize and kind of uproot and improve our Federal cybersecurity policies to meet the challenges of the cyber threats that are out there.

During our investigation into the SolarWinds cyber attack, we found several differences in how agencies viewed their responsibilities under FISMA, particularly whether a cyber attack counted as a "major incident." Some agencies, like Commerce, reported the SolarWinds breach as a major incident, but other agencies, like HHS, did not. Under current law, OMB is the one responsible for defining "major incident," and Federal agencies determine if an incident they have identified counts as one.

Mr. Schneider and Mr. Nodurft, I understand that both of you worked on furnishing the definition of "major incident" while at OMB. Can you describe the process of crafting the definition and what kinds of challenges you faced in creating a definition that would be both comprehensive and flexible and that reflects the evolving nature of cyber attacks?

Mr. Schneider?

Mr. SCHNEIDER. Yes. No, happy to. Thank you for the question, Congressman.

And you absolutely nailed it. The challenge is in having something that is specific enough to drive the behavior that we're looking for and make sure that Congress is getting reported to appropriately, as well as being flexible enough to allow agencies to have a risk management approach. And in SolarWinds, you know, it could be that an agency had SolarWinds installed in a lab on some network that was only in a lab and, therefore, didn't meet the threshold of—of, you know, rising to a major incident in the determination of that agency head. And that's understandable.

When we were building the definition, there were two parts to it. One about the severity of the impact of a particular incident, and then one around the breach of potentially sensitive or personally identifiable information. And you know, and I think Ross can talk to or would concur that when we first did the breach piece, we set a threshold at 10,000 individuals' information being compromised, and we rapidly realized we were going to overwhelm Congress with a whole bunch of reporting and, in some cases, unauthorized access that really hadn't met the threshold for a compromise.

And so, we raised that number to 100,000, which is where OMB has kept it. But you're absolutely right. It's fine-tuning, and I think having that done in the executive branch, where they can fine-tune it regularly and Congress can hold OMB accountable to that.

Sorry for the long answer.

Mr. RASKIN. So, thank you—well, Mr. Nodurft, let me ask you, do you think that defining "major incident" in statute and embodying one definition in the law would be beneficial or detrimental to the flexibility of our responses?

Mr. NODURFT. Thank you for that question, Congressman.

I think that from my experience, prescriptive codification would be extremely detrimental. Given again the timeframes between—between FISMA reform efforts in Congress, it makes it very challenging to tweak the—especially if you're prescriptive about the number or the scope or the scale of the incident.

And frankly, I know Grant mentioned it, when we had the 10,000 instances of PII as the threshold, not only were we reporting more incidents than were necessary, there was a numbness that occurred with our interactions with the committees of jurisdiction. It was that at first it was a very—it was a very robust response. There was a lot of interaction with members of this committee, members of other committees that do oversight over incident response.

But to be honest, after—after probably the 10th or 11th incident that really may not have been a good incident, the interaction dropped precipitously. So, I think that what I would caution as you—as the committee considers whether or not to codify major incident is make sure that if the committee does do that, it is not prescriptive and allows for flexibilities for change when necessary.

Mr. RASKIN. Thank you for that.

Ms. Franks, I wonder if you would weigh in on this same question. There is the danger that Mr. Nodurft recommends to us, which is the problem of an overly rigid definition that has a numbing effect on people. But do you think that Federal agencies today have the tools to adequately make the determination themselves on a case-by-base basis to determine whether there is a major incident, and is it a problem to have the situation that Mr. Schneider discusses when different agencies are calling the same incident different things?

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

Ms. FRANKS. OK. So, the short answer is, yes, most agencies definitely have tools in place to be able to identify what incident has taken place and even perform some of those necessary forensic analyses to further contain whatever vulnerability has impacted their environment and then start those eradication procedures.

What's different is that timeframe we discussed a little earlier, and so agencies definitely take their time to really comb through what forensically could have happened, starting at the indicator of compromise and then perhaps looking at if that malicious actor was able to laterally move throughout their environment, what were they able to touch? What were they able to access once they did find another system, another service?

Because of that, such as the SolarWinds incident, agencies did identify it as impacting their environments differently from another. For example, you mentioned Commerce. But Homeland—HHS basically did not. They—NIH was mainly impacted, but NIH's data was not breached in the sense of where Commerce's data was compromised.

So, it just depends on the agency. It depends on the leadership. All the agencies have applicable security response teams in place to make those necessary identifications, but it becomes a risk process of really combing through that data to really figure out if it's major for their environment versus another environment. So, no two environments or two agencies are alike.

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

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

Mr. KELLER. Thank you, Madam Chairwoman, and thank you to our witnesses for taking time to be here today.

As we continue to move toward heavier reliance on automated systems, cybersecurity becomes more and more important to protecting our national interests. The annual Office of Management and Budget's Federal Information Security Management Act report disclosed over 30,000 agency cyber incidents in Fiscal Year 2020 alone. Congress must ensure that our Nation's cybersecurity laws offer the framework and the flexibility to allow agencies to handle cyber attacks quickly and efficiently.

Mr. Bitko, the FBI executes most enforcement actions regarding Federal criminal laws dealing with cybersecurity, including investigating cyber attacks by bad actors both foreign and domestic. In your former role as the FBI's Chief Information Officer, did you run into any interagency legal or jurisdictional difficulties as you worked to investigate or enforce cybersecurity issues? And if you did, what recommendations would you give Congress to streamline Government reaction to cyber attacks?

Mr. BITKO. Congressman, thank you for the question.

My role was largely internal, looking at the FBI's own enterprise technology, not directly involved in the authority or their ability to conduct investigations. I don't know that I can give you too much deep insight, but I can tell you for sure that there are—there are issues and challenges that exist just within the Government today over what authorities does CISA, for example, have to help in investigating, to going onto other agencies' networks, to having access to sensitive data. All those are things I think it's important and there's an opportunity for FISMA, for Congress to establish clearly where those authorities lie so there is direct authority and responsibility for CISA, for the FBI, for other agencies to ensure that they can—they don't need to get those authorities resolved in the heat of the battle, but that they've been clearly defined in advance.

Mr. KELLER. Thank you. I appreciate that.

And if I could, you know, for Mr. Schneider, attacks such as the SolarWinds hack in 2020, while conducted on a private company, are an immense threat to our national security. So, Mr. Schneider, how does the public sector work in tandem with the private sector to ensure the safety and privacy for all Americans?

Mr. SCHNEIDER. Yes, thank you, Congressman, for the question.

And I think one of the areas, and I think that CISA, the Cybersecurity and Infrastructure Security Agency, has really done an excellent job over—you know, since it came into existence in 2015 of working closely with private industry, helping with the creation of information-sharing analysis centers, which are industry driven, industry run by different sectors. You know, opportunities to share threat information and share vulnerability information, and I think that, you know, we have to have that dialog open.

Gordon mentioned earlier that you need trust in order to trust what you're sharing and who you're sharing with. And so, we can't wait until we have an incident to start the sharing. We have to be sharing information continuously, and we have to be building those relationships and that trust continuously because this is truly, you know, it's needed to have a true public-private partnership in cybersecurity for us as a nation to be successful.

Mr. KELLER. Thank you. I appreciate that.

And I guess if I could just ask Mr. Nodurft, can you please detail how zero trust cybersecurity principles might help prevent SolarWinds or other types of cyber attacks in the future?

Mr. NODURFT. Absolutely. Thank you for that question, Congressman.

I think that when you break down zero trust into its core components, what you're—what you're moving agencies toward is a very hardened center, and it's hard all the way out. You are constantly—you are—you are enabling interactions by continuously, continuously authenticating whether or not those interactions need to occur.

And you have to rely on digital identity solutions. You have to rely on encryption. You have to rely on endpoint detection and response. You have to rely on multiple types of cybersecurity tools and services to come together in a uniquely architected way to provide for that no trust environment that is constantly assessing and checking for the interactions that occur and making sure that anything that touches or deals with the data is dealing with it in a way that's approved and validated and authenticated.

Mr. KELLER. Thank you. I appreciate that, and I yield back.

Chairwoman MALONEY. The gentleman yields back. The gentlelady from Ohio, Ms. Brown, is now recognized.

Ms. BROWN. Thank you, Chairwoman Maloney and Ranking Member Comer, for holding this important hearing.

And thank you to all the witnesses for joining us today. I appreciate your contributions to improving FISMA.

Technology is ever evolving, and IT systems are inherently at risk and vulnerable to cyber attacks. In 2002, FISMA became law, requiring each Federal agency to put an agency-wide program in place to ensure the security of its information and systems. Since the enactment of this legislation in 2002 and the subsequent update in 2014, the cyber threat landscape has transformed remarkably.

The slew of harmful cyber-attacks has exposed vulnerabilities and revealed some of the flaws in our existing laws. The fact that DarkSide, a cyber crime group with Russian ties, was able to force the Colonial Pipeline Company to shut down the largest pipeline in the U.S. is a threat to our national security.

In September 2020, the Ashtabula County Medical Center, a Northeast Ohio hospital, spent more than a week offline after being hit by a cyber attack. Just a few months ago, Southern Ohio Medical Center, another hospital in my home state, suffered a cyber attack that resulted in continued cancellations of patient appointments a week later.

These attacks are deeply concerning because they have profound impacts on the lives of real people, in addition to our national security. I thank the chairwoman and ranking member for working to address emerging cyber threats and finding ways to better protect our cyber infrastructure, and I look forward to making positive changes to FISMA that create a clear, coordinated, and holistic approach to Federal information security to meet the ever-changing cyber frontier.

I have a question for Ms. Jennifer Franks. Ms. Franks, let me ask you what the GAO is learning about the effectiveness of risk assessment metrics during its review of FISMA implementation. First, how is the data incorporated into risk assessment currently collected and reported? And second, does GAO have preliminary recommendations about how to improve the coordination between Government agencies responsible for ongoing risk assessment?

Ms. FRANKS. So, thank you for that question.

So, in short, our FISMA review, the ongoing review that we plan to take to agencies this month for comment, didn't necessarily get into what those risk assessments would look like from a FISMA implementation scoring metric timeline. We focused our efforts on what the IGs do and their various evaluations of the metrics they are to use that are prescribed by OMB.

Those metrics definitely at this point do not highlight risk outward facing. But some of the intricacies of identifying what's in your environment, protecting what's within your computing environments, those get to the implications of risk assessments.

NIST does have the Risk Management Framework, and in that framework that agencies do utilize to implement control in their environment, it looks at assessing risk from the identification down to the implementation of whatever likelihood of events and cyber threats that could be impacting the various agencies. We have had cybersecurity risk management work in the past, our last report issued late 2019. As of right now, we do not have any ongoing work specifically to risk management assessments.

Ms. BROWN. OK, thank you so much.

My next question will be for Ms. Renee Wynn. In the past, agencies have had to focus much of their time on making sure they are compliant with FISMA and other cybersecurity measures, which often means they focus less of their time on risk management. I applaud the updated guidance on FISMA implementation that OMB released last month, which aims to shift the focus of FISMA assessment from compliance to actual observable security outcomes.

The draft legislation that the chairwoman and ranking member released today recognizes this shift by requiring ongoing and continuous risk assessment instead of periodic point-in-time assessment. Ms. Wynn, can you explain to us how performing risk assessment on a continuous basis will strengthen an agency's security system?

Ms. WYNN. Thank you for the question.

I think performing continuous risk assessment is an absolute necessity. Environments change rapidly within the Federal Government, as new mission requirements change or new software, new capabilities come out, and you want to bring that, the best of a breed into the United States Federal Government to meet mission requirements. And so doing it on a continuous basis is really critical.

A quick example on that is having assigned numerous authorities to operate, it wasn't shortly after assigning authority to operate when there was a software update, and it actually broke some of the controls that we had put into place. And so, several weeks later, after saying we're good and we've accepted the risk, we discovered this glaring hole, reported it back to the software developer, which then got fixed.

But in this period of time, you've made an assessment. You've made a statement, but then two weeks later, and then ultimately took two more weeks to get that gap closed. So, on a continuous basis, you can get what I'll call red alerts so you can make sure that your holes or your backside is not so exposed.

Ms. BROWN. Thank you, Ms. Wynn, and it appears my time has expired. I will yield back.

Thank you.

Chairwoman MALONEY. Thank you so much. The gentlelady from Florida, Ms. Wasserman Schultz, is now recognized.

Ms. WASSERMAN SCHULTZ. Thank you, Madam Chair, and thank you for having this important hearing, as many others have said.

In recent years, my home state of Florida has been in the crosshairs of the onslaught of devastating cyber attacks. The targets range from large Federal agencies like NASA to local school districts, major hospital systems, and the private sector has faced equally dire threats with far-ranging impacts much like we saw in the ransomware attack on a Miami-based software company, Kaseya. And for them, they endured a ransomware attack that resulted in fallout to hundreds of downstream businesses.

Cyber criminals clearly want the World Wide Web to be a lawless "Wild West," and it is critical that we modernize our approach to meet the challenge of this evolving cyber frontier. One simple fact makes this clear. There are two entities with important roles in Federal cybersecurity, the Cybersecurity and Infrastructure Security Agency, or CISA, and the Office of the National Cyber Director. And that was established in just the last few years after the last FISMA update, which was in 2014.

The draft FISMA reform bill that the chairwoman and ranking member released today integrates these offices into the cybersecurity Government structure, and they are careful to strike the appropriate balance with OMB to create a clear and effective dynamic.

Mr. Schneider, you previously served as the Chief Information Security Officer at OMB, and based on your experience, can you characterize how CISA and the National Cyber Director fit within the FISMA framework and enhance our national cybersecurity defense posture?

Mr. SCHNEIDER. Thank you, Congresswoman. Thank you for the question.

Yes. I think how they fit in is the National Cyber Director is really the overarching voice and specifically to Federal cybersecurity because both organizations have roles beyond that. But for Federal cybersecurity, I view the National Cyber Director as having that overarching voice, being a bit of the conductor. I view CISA as really being the operational partner with agencies. CISA should be there to help agencies who are tasked to implement their risk management programs.

And then the other two really important players are the National Institute of Standards and Technology, who is charged with the establishment of standards and creation of guidance, and then the Office of Management and Budget, who has—and I think should continue to have—the lead for developing policy and overseeing the programs, providing the oversight, being the hammer to agencies while CISA is being the partner to agencies.

And I think the interaction with OMB and the National Cyber Director is going to need to be absolutely seamless to make this work.

Ms. WASSERMAN SCHULTZ. Thank you.

Mr. Nodurft, can you illustrate why it is so important to have these roles clearly defined?

Mr. NODURFT. Yes, Congresswoman. Thank you so much for the question.

The necessity of streamlined reporting requirements from the agencies up makes it much easier for them to know how to respond, when to respond, with whom to speak with on the backend of responding to incidents. So, that's one.

Two, when agencies are proactively trying to mitigate their cyber risks, they need clear reporting channels and clear areas of jurisdiction to go and propose budgets and work on budgeting with. They need clear direction from a strategic standpoint as well as an operational standpoint, and I think by clearly delineating who owns what, agencies will know where to look and where to go, and it will make it much easier for them to work together to build a broader defensive structure.

Ms. WASSERMAN SCHULTZ. Thank you.

The Senate's version of FISMA reform would create a liaison between CISA and each agency by assigning a CISA adviser to each agency, much like every agency has a White House liaison, for example. And this role is intended to be a two-way street, providing additional support to the agency while also helping CISA better understand the agency's nuances and unique needs.

Ms. Wynn, do you think such a dedicated liaison role would be helpful, or would that be an unhelpful intrusion of CISA into agency operations?

Ms. WYNN. From my perspective, I worked—when I was within the Federal Government, I worked very closely with CISA on a couple of matters. I was very proactive in terms of engaging them, the Office of Management and Budget, DHS, and in fact, on a couple of occasions, the FBI. And having somebody to call makes a huge difference.

So, if CISA's effectiveness depends upon having a liaison, and they agree that that's what's necessary for them to operate better within their organizational structure, then absolutely would support codifying having a liaison. The important thing to walk away with is we have to work together in order to solve very hard problems.

Ms. WASSERMAN SCHULTZ. Thank you so much, Madam Chair. My time has expired.

Chairwoman MALONEY. The gentlelady yields back. The gentlewoman from Illinois, Ms. Kelly, you are now recognized. Ms. Kelly?

[No response.]

Chairwoman MALONEY. Move to the gentleman from Illinois, Mr. Davis. You are now recognized for five minutes. Mr. Davis?

Mr. DAVIS. Thank you, Madam Chairman. And like others have already said, thank you for holding this important hearing.

The Department of Homeland Security issued a binding operational directive in 2020 that requires most Federal agencies to have a vulnerability disclosure policy, which describes how someone who uncovers a cybersecurity vulnerability in a Federal system can report that vulnerability to the affected agency without fear of legal action.

According to HackerOne, a cybersecurity firm that employs hackers and cybersecurity researchers to audit security hackers, reported more than 66,000 verified vulnerabilities in 2021, a 21 percent increase from 2020. That is tens of thousands of vulnerabilities that may not have been found by automated process.

It is crucial that these cybersecurity researchers have the ability to report to the Federal Government, and I am pleased that the draft legislation we are discussing includes a provision to codify Federal vulnerability disclosure programs.

Mr. Schneider, before you left OMB, only a handful of Federal agencies had published a vulnerability disclosure policy. Fortunately, today, almost all Federal agencies have such policy. In your opinion, how efficient are Federal agencies at managing their vulnerability disclosure programs?

Mr. SCHNEIDER. Congressman, thank you for the question.

And vulnerability disclosure is a really important area. As you mentioned, and just before I left the Government or as I was departing, we published an OMB memo that went out in conjunction with that binding operational directive, memo—OMB Memo 20–32, which also directed agencies to implement vulnerability disclosure programs.

And the fact that most agencies have one in place today I think is a testament to, A, the agencies' recognition of the importance of being able to leverage the research community to get vulnerabilities in and get them identified. I think the other really important aspect of a vulnerability disclosure program, though, is how you get those vulnerabilities sent back to industry or whoever the responsible party is to develop a mitigation for them, and how do you protect that information in the meantime?

You know, the Log4j vulnerability that we're experiencing, you know, it had been identified by a researcher. It had been, you know, reported to Apache and was being worked on. And then another company identified it, put out a patch to their own software, and then it became public.

So, really the, you know, disclosure of the vulnerability with Log4j got out ahead of the remediation, and that's why we have to be so careful about how we treat that vulnerability information as it's identified before there's a mitigation in place.

Mr. DAVIS. Most agencies respond within a period of about three days. Do you think that is adequate in terms of response time?

Mr. SCHNEIDER. For responding, I think you're talking about responding to the researcher. And I do think three days is adequate. I think, you know, you need to get back to the researcher quickly. They need to know that you're taking it seriously and that you're going to do something about it. Otherwise, they may go disclose—disclose the vulnerability more broadly and more publicly to potentially disastrous results.

Mr. DAVIS. Thank you very much.

Ms. Wynn, let me ask you how can we ensure that agencies have the ability to keep up with the influx of vulnerability reports? A lot of them are coming in.

Ms. WYNN. Thank you for that.

So, I had the pleasure of having well over 100,000 vulnerabilities reported to me on a regular basis because of the complex systems used at NASA. And so, what we ended up doing was we established actually a vulnerability management program, and that's because you can't always address every vulnerability right away. And that sounds like that you might be ignoring risk, but what we would have at NASA are something called the flight freeze, and this was to ensure the risk on a flight was mitigated as fast as possible.

And so during those flight freezes, we wouldn't be able to address the vulnerabilities that the system might have had, but that system, we would put other risk mitigations in place like making sure the system didn't go online, which is very, very much the case on mission control systems and that.

And so you have a spectrum of risks you have to deal with. By having a vulnerability management program, you can hold mission and mission support heads accountable for dealing with their vulnerabilities in the right amount of time so that you don't disrupt operations.

Mr. DAVIS. And quickly, Mr. Bitko——

Chairwoman MALONEY. The gentleman's time has expired. The gentleman——

Mr. DAVIS. I yield back.

Chairwoman MALONEY. Thank you so much, Mr. Davis. The gentlelady from California, Ms. Speier, is recognized for five minutes.

Ms. SPEIER. Thank you, Madam Chair, and I am delighted that this particular hearing is not only happening, but that the American people can see that Democrats and Republicans can work together.

I want to focus on the work force because certainly in my work on the Intelligence Committee, the biggest hole is in getting the talent we need to perform the various functions. So, I would like to ask you, Mr. Schneider and Mr. Nodurft, what your experience was at OMB in terms of the staffing challenges, and what recommendations you would make to us to make sure that we have the talent and are able to afford the payments necessary in terms of salaries to attract the kind of talent we need.

Mr. Schneider?

Mr. SCHNEIDER. Yes. Thank you, Congresswoman.

You are absolutely correct. The work force is—I mean, is so critical in cybersecurity. The work force are the ones that are doing literally all the work, making all the decisions, and it is an immense challenge. We don't have enough skilled cybersecurity professionals nationwide, and then the Federal Government is competing and, as you alluded to, challenged from a wage standpoint, from an ability to—compensation standpoint to bring people in.

And so, what I saw is that we have a lot of really excellent and a lot of really dedicated people who are inside the Federal Government. I think we need more programs that allow people to come into the Government, maybe for a short period of time, or at least thinking it's for a short period of time. Because some of them will find out that they love the mission, and they'll stay.

I think we also need the ability to have people move in and out of Government more easily. There's a whole bunch of challenges associated with——

Ms. SPEIER. Thank you.

Mr. SCHNEIDER. Oh, I'm sorry.

Ms. SPEIER. I need to move on, but is there any—Mr. Nodurft, do you have any ideas on how we can attract this talent——

Mr. NODURFT. Thank you for the question, yes, ma'am.

Ms. SPEIER [continuing]. that Mr. Schneider has suggested?

Mr. NODURFT. So, yes, ma'am. Thank you.

The one idea I want to bring up is you're absolutely right. This is an "all hands on deck" moment. I think we need to or the committee should consider and should encourage the administration to consider new approaches that bring in and leverage industry expertise in certain areas in finite periods of time. And whether that's through contractual relationships, through different GSA vehicles or contract vehicles, or whether it's public-private partnerships that we currently have in place, we need to be able to access the talent that is in whatever part of our ecosystem that is possible.

So, for example, the committee's work on the bill is encouraging agencies to move to zero trust environments. I think, ma'am, the committee has an opportunity to really encourage the administration to put in place specific authorities that allow for folks who are very familiar with the technology to work side by side with the departments and agencies to build out those environments, help them configure them, teach them how to manage and continue to grow them, and then move out.

And we need—we need to be able to do that seamlessly. So, it's big ideas that talk about those types of partnerships that we're proposing.

Ms. SPEIER. OK, thank you.

Ms. Franks, Mr. Connolly had asked you about those 900 recommendations that have not yet been complied with. Could you provide us with—and you can do this offline, but provide to the committee the most critical ones that still haven't been addressed so that we can review it, please?

Ms. FRANKS. Yes, absolutely. I can provide that to you.

Ms. SPEIER. Thank you.

Ms. FRANKS. You're very welcome.

Ms. SPEIER. And Ms. Wynn, you had mentioned that there are companies that repeatedly have, I guess, break-ins that we continue to contract with, if I remember or interpreted your testimony correctly. Could you actually specify those companies, please?

Ms. WYNN. I don't have that list handy. I'm happy to followup maybe afterwards to share some of the information about having to work with vendors and contractors about some of their repeated challenges that they were creating for the agencies that I worked for.

Ms. SPEIER. Thank you. Madam Chair, I think that is really important because we can't continue to contract with those that have inappropriate cyber hygiene. And there are lots of companies out there, new startups, particularly in my district, that are doing some very exciting things, and our procurement process is so long and arduous that we oftentimes get the contract and it is already out of date with a particular software company.

So, I hope that we look at that as well because there is much that needs to be done. I yield back.

Chairwoman MALONEY. The lady yields back, and that is a very important point. Thank you very much, and we will look at that.

Thank you.

We now recognize the gentlewoman from Illinois, Ms. Kelly. You are now recognized.

Ms. KELLY. Thank you, Madam Chair.

The proliferation of smart devices across society has helped to improve some of the everyday functions of our lives. Examples include watches tracking our health analytics, voice-activated light switches, and smart cities where sensors can analyze traffic patterns, water supplies, or energy use to better serve citizens.

These smart devices that connect to the Internet, known as Internet of Things, or IoT devices, that are increasingly part of the market for both home and business operation. Last Congress, my IoT Cybersecurity Improvement Act was signed into law to help create Federal standards for Government-used IoT devices. The law sets minimum security standards for Internet-connected devices purchased by a Federal Government agency and created a vulnerability disclosure program for Government IT.

Despite this law, I am still concerned that our cybersecurity standards have not kept pace with the rise of IoT devices. This is really worrisome because it is not just smart refrigerators that can be at risk to hackers, but as you guys know, medical devices, security cameras, and even automobiles all offer inroads for hackers to enter network systems.

Mr. Schneider, what are some of the important functions of IoT devices on Federal networks?

Mr. SCHNEIDER. Congresswoman, thank you for the question.

I think we're going to see—you know, we're seeing today, you know, numerous places where Internet of Things, where IoT devices are being integrated into Federal agencies. But, and I think some of them are going to serve important purposes. My concern is also about the ones that might not.

You mentioned the Internet-connected refrigerator that might be in a breakroom, and someone might decide it would be a good idea from the facilities to be able to monitor the temperature of that refrigerator and connect it to the agency's network and if that device now could be the access point into the entire agency's network, into truly where the sensitive information is.

So, I think agencies need to pay attention as they're implementing IoT devices. IoT devices need to be more secure. But we also need to find a way, when possible, to keep them segmented within the environment so they're not, you know, an entry point, if you will.

Ms. KELLY. I know you talked about the refrigerator, but how do hackers exploit vulnerable IoT devices on a network? How do they do it?

Mr. SCHNEIDER. So, I mean, hackers will do it like they will with other devices. They will identify a vulnerability. They are often able to remotely determine if the individual device is, you know, still vulnerable. Is it still running the version, the vulnerable version of the software? In some cases, with IoT devices, they can't even be updated. So, they know it's vulnerable.

And then they're able to, you know, use whatever the exploitation is to gain access to that device, and then they're—you know, kind of once they're in, they start working their normal approach of elevating privileges, moving laterally through the system, and starting the reconnaissance phase of what information do they want to steal, gain, get access to. You know, what are they trying to achieve inside and really starting to look around to see what they can do inside the environment.

Ms. KELLY. In 2020, Palo Alto Networks reported that—and I quote—"57 percent of IoT devices are vulnerable to medium or high severity attacks, making IoT the low-hanging fruit for attackers." And the risk of an IoT hack across the Federal Government is even greater since it is not sensitive information at risk for actual equipment or devices that underpin our infrastructure.

Now reporting on these vulnerabilities is also necessary and critical to informing improvements to our cybersecurity system. Again, Mr. Schneider, how will reporting of vulnerabilities improve coordination of the Federal Government's cybersecurity infrastructure?

Mr. SCHNEIDER. Yes, great question and great points, ma'am. And I think it highlights the need to take action when this information is reported, right? We need the vulnerabilities identified. Agencies need to be aware of them, and then agencies need to take action.

It's really exciting for us to talk about something like SolarWinds that was a very sophisticated attack, but quite frankly, most cyber incidents, as the statistics you just mentioned, you know, come from a known vulnerability that could have been mitigated with a known patch that was out there that just had not been applied by organizations. That's where most cyber attacks, successful attacks take place.

Ms. KELLY. Thank you.

And Mr. Nodurft, how is the situation complicated by individual enterprises across the Government/dot-government landscape?

Mr. NODURFT. Thank you very much, ma'am, for the question.

So, we have individual enterprises across the Federal landscape that within them have their own individual enterprises across the Federal landscape. It is a very diverse enterprise environment, and what you have is the diverse set of missions requires technology purchases, acquisitions that want to bring in some of the—and leverage some of the most modern advanced technologies that are out there right now.

I think that we, as a—or the Federal Government should encourage use of the latest and greatest and most modern technologies, whether it's for mission or for enterprise management. Both of those should be highly encouraged. And we just need to think through what are the—what are the frameworks, whether it's the NIST cybersecurity framework. What are the solutions?

Are there—I can tell you that member companies of mine, of the Alliance for Digital Innovation can independently audit IoT environments for these new technologies to make sure that they are up to date, and they are secure. And I think we should take a look at how we are, again, partnering from a public-private standpoint to make sure that the talent that we need to secure these new environments is accessible to the agencies so that they use this modern technology.

Ms. KELLY. Thank you, and I am way over time. I yield back.

Thank you.

Chairwoman MALONEY. The gentlelady yields back, and now I recognize myself.

I, first and foremost, want to thank Ranking Member Comer for working with us in a bipartisan way to confront this tremendous challenge. He has indicated he does not want a closing statement.

But as we have seen here today, the breadth and the complexity of cybersecurity threats to the Federal Government are absolutely staggering. I am grateful to all of our witnesses for sharing their deep knowledge and personal experience from both the Federal

Government and the private sector perspectives. The combined years of Government service represented on our panel must be around 100, and it shows in the high caliber of the recommendations shared today.

I am tremendously grateful to Congressman Comer for his strong partnership on this issue and to all our committee members, Democrat and Republican, for their engagement during this hearing and for our staffs. Today's hearing showed there is a strong bipartisan commitment to modernizing FISMA, and I have been encouraged by similar strong support in the Senate and the Biden administration.

So, we have a real opportunity to pass FISMA reform this year and to protect the intellectual property, sensitive data, and networks that are essential to our country's economy and national security. I am committed to getting FISMA reform done right, and I am looking forward to working in a bipartisan way to achieve this for the American people. And I thank all of the participants.

Before we close, I want to take care of one piece of business. Without objection, Ms. Shontel Brown is added to the Government Operations Subcommittee and the Economic Consumer Policy Subcommittee. Without objection.

I also ask unanimous consent to insert into the br a statement from the SecurityScorecard. Without objection, so ordered[SA1].

Chairwoman MALONEY. In closing, I want to thank again our panelists for their remarks, and I want to commend my colleagues for participating 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 respond as promptly as possible.

This hearing is now adjourned.

[Whereupon, at 12:54 p.m., the committee was adjourned.]

○