EVALUATING CISA'S FEDERAL CIVILIAN EXECUTIVE BRANCH CYBERSECURITY PROGRAMS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

SEPTEMBER 19, 2023

Serial No. 118–29

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

54–816 PDF WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
SHEILA JACKSON LEE, Texas
DONALD M. PAYNE, JR., New Jersey
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
YVETTE D. CLARKE, New York
DINA TITUS, Nevada

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
NATALIE NIXON, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW R. GARBARINO, New York, *Chairman*

CARLOS A. GIMENEZ, Florida
MIKE EZELL, Mississippi
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
MARK E. GREEN, MD, Tennessee *(ex officio)*

ERIC SWALWELL, California, *Ranking Member*
SHEILA JACKSON LEE, Texas
TROY A. CARTER, Louisiana
ROBERT MENENDEZ, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

CARA MUMFORD, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

EVALUATING CISA'S FEDERAL CIVILIAN EXECUTIVE BRANCH CYBERSECURITY PROGRAMS

Tuesday, September 19, 2023

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:05 a.m., at Room 310, Cannon House Office Building, Hon. Andrew R. Garbarino [Chairman of the subcommittee] presiding.

Present: Representatives Garbarino, Gimenez, Ezell, Lee, Carter, and Menendez.

Chairman GARBARINO. The Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection will come to order. Without objection, the Chair may recess at any point. The purpose of this hearing is to receive testimony from industry experts on CISA's two flagship cybersecurity programs for the Federal Civilian Executive branch. I now recognize myself for an opening statement.

Thank you for our witnesses for being here to talk about a very important topic CISA's Federal cybersecurity programs. One of CISA's core missions is the protection of the Federal Civilian Executive branch, or FCEB. Although CISA has been pulled in many different directions in recent years, it is crucial that it continues to focus on its foundational responsibilities, chief among them being the protection of FCEB networks. Today, we will focus on two programs, the Continuous Diagnostic and Mitigation Program, or CDM, and the National Cybersecurity Protection System, or NCPS, which includes EINSTEIN.

In recent years, CISA officials have indicated their intent to revamp and improve these programs. We will discuss with industry partners who participate in and have perspectives on these two programs, some of the successes they have had so far, and the ways they can improve in the future. CDM provides tools to agencies to defend their networks, which feed data into dashboards to allow agencies to monitor their real-time network security. Conceptually, those agency-specific dashboards send data to a Federal Government-wide dashboard that CISA uses to monitor the state of FCEB security. The current model provides 2 years of CISA-sourced funding for CDM tools at agencies, after which point agencies must pick up the bill.

NCPS is a set of capabilities that includes EINSTEIN, CISA's Intrusion Detection and Intrusion Prevention System. EINSTEIN sensors reside on the perimeter of an agency's network and detect and block known malicious traffic. While this perimeter security function is important, it is not sufficient for a cybersecurity program, given the current threat landscape and the ability of bad actors to evade many perimeter security mitigations. What is more, EINSTEIN has faced long-standing downsides, including limitations in detecting and preventing encrypted traffic and focusing only on what we already know is malicious traffic.

NCPS's authorization expires at the end of the fiscal year. In the President's fiscal year 2024 budget request, CISA included a $425 million request for the Cyber Analytics and Data System, or CADS, which is meant to take the place of NCPS. CISA intends to transition certain legacy capabilities of EINSTEIN into the new CAD system, and others will be taken over by new CADS capability. While CISA has not provided many public details about its plans to build CADS, I am looking forward to hearing from our witnesses their thoughts on how CISA should be approaching this new analytic capability.

As the administrator of Federal cybersecurity requirements, CISA has the broad and important role in ensuring the security of Federal networks. While the ultimate responsibility for an individual agency's security is the head of that agency through programs like CDM and EINSTEIN, CISA has the potential to make a real impact on Federal network security. The direction CISA takes with these programs, and to what extent they are administered as true shared service with the CISA covering continued cost, will dictate CISA's posture toward other Federal agencies moving forward.

Whether CISA acts as a service provider or an advisor toward other agencies is a fundamental question, and Congress and CISA must both be consistent in how they approach it across CISA's many missions and programs. I look forward to our witnesses' testimony and to discussing these questions with them in depth.

[The statement of Chairman Garbarino follows:]

STATEMENT OF CHAIRMAN ANDREW R. GARBARINO

SEPTEMBER 19, 2023

Thank you to our witnesses for being here to talk about a very important topic: CISA's Federal cybersecurity programs. One of CISA's core missions is protection of the Federal Civilian Executive branch, or FCEB. Although CISA has been pulled in many different directions in recent years, it's crucial that it continues to focus on its foundational responsibilities, chief among them being the protection of FCEB networks.

Today we will focus on two programs: the Continuous Diagnostics and Mitigation program, or CDM, and the National Cybersecurity Protection System, or NCPS, which includes EINSTEIN. In recent years, CISA officials have indicated their intent to revamp and improve these programs. We will discuss with industry partners, who participate in and have perspectives on these two programs, some of the successes they have had so far and ways they can improve in the future.

CDM provides tools to agencies to defend their networks, which feed data into dashboards to allow agencies to monitor their real-time network security. Conceptually, those agency-specific dashboards send data to a Federal Government-wide dashboard that CISA uses to monitor the state of FCEB cybersecurity. The current model provides 2 years of CISA-sourced funding for CDM tools at agencies, after which point agencies must pick up the bill.

NCPS is a set of capabilities that includes EINSTEIN, CISA's intrusion detection and intrusion prevention system. EINSTEIN sensors reside on the perimeter of an agency's network and detect and block known malicious traffic. While this perimeter security function is important, it is not sufficient for a cybersecurity program given the current threat landscape and the ability of bad actors to evade many perimeter security mitigations. What's more, EINSTEIN has faced long-standing downsides, including limitations on detecting and preventing encrypted traffic and focusing only on what we already know is malicious traffic. NCPS's authorization expires at the end of this fiscal year.

In the President's fiscal year 2024 budget request, CISA included a $425 million request for the Cyber Analytics and Data System, or CADS, which is meant to take the place of NCPS. CISA intends to transition certain legacy capabilities of EINSTEIN into the new CADS system, and others will be taken over by new CADS capabilities. While CISA has not provided many public details about its plans to build CADS, I am looking forward to hearing from our witnesses their thoughts on how CISA should be approaching this new analytic capability.

As the administrator of Federal cybersecurity requirements, CISA has a broad and important role in ensuring the security of Federal networks. While the ultimate responsibility for an individual agency's security is the head of that agency, through programs like CDM and EINSTEIN, CISA has the potential to make a real impact on Federal network security. The direction CISA takes these programs, and to what extent they are administered as true shared services with CISA covering continued costs, will dictate CISA's posture toward other Federal agencies moving forward. Whether CISA acts as a service provider or an advisor toward other agencies is a fundamental question, and Congress and CISA must both be consistent in how they approach it, across CISA's many missions and programs.

I look forward to our witnesses' testimony and to discussing these questions with them in more depth.

Chairman GARBARINO. I now recognize the Ranking Member, the gentleman from New Jersey, Mr. Menendez, for his opening statement.

Mr. MENENDEZ. Good morning. I want to thank Chairman Garbarino for holding this important hearing to assess how CISA is modernizing its signature Federal network security programs to keep pace with the rapidly-evolving threat environment and advancements in technology. Two-and-a-half years ago, the solar wind supply chain attack forced the Federal Government to overhaul its approach to securing its networks and supply chains. The Biden-Harris administration made revamping Federal network security a top priority, issuing an ambitious Executive Order that brought to bear the full resources of every Federal agency with a cybersecurity mission. Together with Congress, the administration made historic investments in improving Federal network security.

Not since the 2015 Office of Personnel Management breach had there been as much momentum for change in how we secure Federal networks. While President Biden and Congress certainly deserve credit for giving needed attention to Federal network security, it is critical that we continue our work to modernize Federal network security to avoid crisis-driven policy making. We must ensure that the programs we rely on to secure our networks can adapt to and integrate with new technologies and modern network architectures. We must endeavor to stay a step ahead of our adversaries, building upon our recent momentum to better detect malicious activity quickly and mitigate the risk posed by cyber intrusions.

CISA plays a central role in securing our Federal networks as the administrator of the National Cybersecurity Protection System, commonly referred to as NCPS, and the Continuous Diagnostics and Mitigation Program, commonly referred to as CDM. These pro-

grams complement CISA's other important powers, including the authority to issue security guidance and best practices, binding operational directives and emergency directives, which require agencies to take expedited action to secure their networks against a pressing threat or vulnerability.

Over the past 2½ years, CISA has laid out its plans to modernize both NCPS and CDM programs. Earlier this year, CISA announced plans to sunset and replace its EINSTEIN intrusion detection system, which has limited effectiveness against novel threats and newer network architectures and shift remaining NCPS capabilities to a new program called the Cyber Analytics and Data System. Together, the legacy EINSTEIN capabilities and CADS will become the joint collaboration environment, commonly referred to as JCE, which CISA predicts will be, "best-in-class analytical environment" that utilizes increased automation to more efficiently analyze classified and unclassified data.

JCE holds tremendous promise, but successful implementation requires a clear vision and buy-in from both Federal and private-sector partners. CISA has worked to rapidly mature its CDM program to ensure that its Federal customers can tailor it to accommodate their unique security requirements. CDM is limited, however, in that it is deployed on IT technologies, not operational technology, or internet of things devices. Moreover, the Government Accountability Office recently found that CISA lacks the authority to test CDM tools on agency networks, which undermines its ability to ensure those tools are working as anticipated. I am interested in learning from witnesses today how we can improve the security value of both programs.

Before I close, I want to remind my colleagues that Government shutdowns are bad for Federal network security. We are nevertheless 2 weeks away from Government funding running out. During the last shutdown, which lasted 35 days, CISA issued its first emergency directive to Federal agencies ever. Having employees and IT contractors across the Government and at CISA furloughed at the time was not helpful. A continuing resolution would also impair CISA's critical work, as it would restrict CISA's ability to start new programs that match the current threat environment.

It is detrimental to our national security to slow investments in our Federal network security programs at such a critical moment in their maturation. Moving forward, the House and Senate need to pass a Homeland Security Appropriations bill that provides needed funding to CISA to carry out its vital missions. Now is not the time to take our foot off the gas. With that, I thank the witnesses for being here today. I look forward to their testimony.

[The statement of Hon. Menendez follows:]

STATEMENT OF HON. ROBERT MENENDEZ

SEPTEMBER 19, 2023

Two-and-a-half years ago, the SolarWinds supply chain attack forced the Federal Government to overhaul its approach to securing its networks and supply chains. The Biden-Harris administration made revamping Federal network security a top priority, issuing an ambitious Executive Order that brought to bear the full resources of every Federal agency with a cybersecurity mission. Together with Congress, the administration made historic investments in improving Federal network security.

Not since the 2015 Office of Personnel Management breach had there been as much momentum for change in how we secure Federal networks. While President Biden and Congress certainly deserve credit for giving needed attention to Federal network security, it is critical that we continue our work to modernize Federal network security to avoid crisis-driven policy making.

We must ensure that the programs we rely on to secure our networks can adapt to and integrate with new technologies and modern network architectures.

And we must endeavor to stay a step ahead of our adversaries, building upon our recent momentum to better detect malicious activity quickly and mitigate the risks posed by cyber intrusions.

CISA plays a central role in securing our Federal networks as the administrator of the National Cybersecurity Protection System, commonly referred to as NCPS, and the Continuous Diagnostics and Mitigation program, commonly referred to as CDM. These programs complement CISA's other important powers, including the authority to issue security guidance and best practices, Binding Operational Directives, and Emergency Directives, which require agencies to take expedited action to secure their networks against a pressing threat or vulnerability. Over the past 2½ years, CISA has laid out its plans to modernize both NCPS and CDM programs.

Earlier this year, CISA announced plans to sunset and replace its EINSTEIN intrusion detection system—which has limited effectiveness against novel threats and newer network architectures—and shift remaining NCPS capabilities to a new program called the Cyber Analytics and Data System (CADS). Together, the legacy EINSTEIN capabilities and CADS will become the Joint Collaboration Environment, commonly referred to as JCE, which CISA predicts will be a "best-in-class analytic environment" that utilizes increased automation to more efficiently analyze classified and unclassified data. JCE holds tremendous promise, but successful implementation requires a clear vision and buy-in from both Federal and private-sector partners.

CISA has also worked to rapidly mature its CDM program to ensure that its Federal customers can tailor it to accommodate their unique security requirements. CDM is limited, however, in that it is deployed on IT technologies, not operational technology or internet of things devices. Moreover, the Government Accountability Office recently found that CISA lacks the authority to test CDM tools on agency networks, which undermines its ability to ensure those tools are working as anticipated. I am interested in learning from witnesses today how we can improve the security value of both programs.

Before I close, I want to remind my colleagues that Government shutdowns are bad for Federal network security. We are nevertheless 2 weeks away from Government funding running out. During the last shutdown—which lasted 35 days—CISA issued its first Emergency Directive to Federal agencies ever. Having employees and IT contractors across the Government—and at CISA—furloughed at the time was not helpful. A continuing resolution would also impair CISA's critical work, as it would restrict CISA's ability to start new programs that match the current threat environment.

It is detrimental to our national security to slow investments in our Federal network security programs at such a critical moment in their maturation. Moving forward, the House and Senate need to pass a Homeland Security appropriations bill that provides needed funding to CISA to carry out its vital missions. Now is not the time to take our foot off the gas.

Chairman GARBARINO. I want to thank the Ranking Member for that rousing opening statement. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statements of Ranking Member Thompson and Honorable Jackson Lee follow:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

SEPTEMBER 19, 2023

We all remember learning about the SolarWinds intrusion in December 2020, which highlighted how vulnerable Federal agencies were to foreign espionage campaigns and how outdated our Federal network cyber defenses were. While the creation of the Cybersecurity and Infrastructure Security Agency in 2018 represented a major step forward in developing an organization charged with leading the oper-

ational defense of Federal networks, Congress did not initially provide the agency with sufficient resources to match the modern threat environment.

Fortunately, upon taking office shortly after the SolarWinds incident, President Biden quickly took critical actions to modernize our cyber defenses. By issuing Executive Order 14028, President Biden began a process of updating the Federal Government's cybersecurity to combat the threats we face from our adversaries. Along with the $650 million Congress provided to CISA in the American Rescue Plan Act and steady increases in CISA's budget, efforts over the last 3 years have brought meaningful gains in improving CISA's visibility and response capabilities throughout the Federal Civilian Executive branch.

Investments in endpoint detection and response technologies across Federal agencies have helped improve the Continuous Diagnostics and Mitigation program and has brought the Federal Government in line with the cybersecurity practices standard in much of the private sector. In recent cyber incidents, we have seen how an improved CDM dashboard and increased visibility have enabled CISA to move quickly to identify vulnerabilities across the Federal Government and mitigate risk. I look forward to hearing from our witnesses about how CISA can continue to improve the CDM program, including how it can gain visibility into operational technology, a priority for me.

In this year's budget request, the administration has now proposed a much-needed restructuring of the National Cybersecurity Protection System. By establishing the Cyber Analytics and Data System, CISA hopes to more efficiently analyze the ever-increasing amount of data it receives from Federal agencies, State and local governments, and critical infrastructure. Hearing from private-sector partners should help ensure CISA develops this new program in a way that reflects the expertise of leading cybersecurity companies, while maintaining and evolving the network detection and prevention capabilities of the EINSTEIN program. Without sustained support for CISA's Federal network security programs going forward, the progress we have made in recent years may stall.

A Government shutdown or a year-long continuing resolution would restrict CISA's ability to move forward with efforts to continue CDM modernization or deploy the new CADS program. Operating under a CR is problematic for any agency; in the world of cybersecurity, where our adversaries are constantly innovating, operating under last year's budget or no budget at all could be devastating for our national security.

I hope my Republican colleagues will stop holding Government funding hostage to their inhumane and ineffective border proposals and instead come to the negotiating table to develop a bipartisan full-year appropriations agreement.

I am proud of the tremendous achievements we have had in recent years to provide CISA the resources and authorities it needs to better secure Federal agencies. Only with bipartisan support for CISA and its mission can we continue to build on our previous work.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

SEPTEMBER 19, 2023

Chairman Garbarino, and Ranking Member Swalwell, thank you for holding today's hearing on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs".

I look forward to the questions that will follow the testimony of:

- Mr. Brian Gumbel, president, Armis;
- Mr. Stephen Zakowicz, vice president—consulting services, CGI Federal;
- Mr. Joe Head, chief technology officer, Intrusion; and
- Mr. Rob Sheldon, senior director of public policy and strategy, Crowdstrike (Democratic Witness).

I welcome the witnesses and thank them for their testimony before the House Homeland Security Committee.

The purpose of this hearing is to assess CISA's efforts to modernize its two signature Federal network security programs, the Continuous Diagnostics and Mitigation program (CDM) and the National Cybersecurity Protection System (NCPS).

The Federal Executive branch is comprised of civilian Federal agencies that provide the full scope of benefits and services to residents of the States and territories as well as support of domestic law enforcement and homeland security needs.

Cybersecurity for non-civilian agencies is primarily managed under the Department of Defense.

The Federal Executive branch cybersecurity coordination was not as robust as national defense networks, but this dramatically changed following the SolarWinds attack.

In December 2020, the Federal Government learned the Russian government had executed a malicious cyber campaign targeting Federal networks and certain critical infrastructure.

Russian hackers used a combination of traditional tactics, techniques, and procedures (e.g.: password guessing) and a supply chain attack to infiltrate targeted networks.

In a supply chain attack, malicious actors infiltrate a target network by exploiting security vulnerabilities in the network of a trusted partner to gain access to the targeted network.

In this case, one of the trusted partners was Solar Winds, a U.S.-based vendor whose Orion Platform provided network monitoring services to entities across the world, including the U.S. Government.

To execute the attack, hackers gained access to SolarWinds and injected malicious code into an Orion software update sent to customers in March 2020.

The malicious code created a backdoor in the affected networks that caused servers to communicate with a U.S. IP address after a dormant period.

In response, hackers sent additional malicious code to some, but not all, affected networks.

Ultimately, the additional malicious code allowed hackers to access elevated credentials and move around a victim's network, monitoring activity and slowly taking data.

To deceive security products on customers' networks, actors disguised their activity as normal network traffic and were able to persist through the creation of additional credentials from other applications.

A total of 18,000 SolarWinds customers downloaded the compromised version of Orion, but far fewer have identified activity beyond the creation of a backdoor.

Nearly 40 Federal agencies downloaded the compromised SolarWinds Orion update.

It is important to note that about 30 percent of both Government and non-Government victims of the Russian cyber campaign had no direct connection with SolarWinds.

According to news reports, hackers also breached networks by "exploiting known bugs in software products, by guessing on-line passwords and by capitalizing on a variety of issues in the way Microsoft Corp.'s cloud-based software is configured."

Bugs can also be called Zero-Day Events that if exploited could cost significant disruption in the function of application or services that rely on computers or remote computing services.

The SolarWind Orion exploit was not intended to damage or disrupt computing systems, it was designed to spy on networks and spread to other systems.

The SolarWinds campaign illustrated many of the shortcomings in the Federal Executive Branch civilian cybersecurity, which lacked the ability to effectively monitor and respond to threats on civilian agency networks.

At that time there was also no overarching Federal law requiring private entities to report cybersecurity incidents, there is little public information on the number of victims that installed the infected versions of Solar Winds Orion or experienced second-stage intrusions.

At the time of the attack, there was a critical need to modernize the Federal Government civilian agency cybersecurity and SolarWinds became the catalysis to begin this important work.

Until the SolarWinds attack civilian Federal agencies had been slow to adapt to the demands of new technologies, network architectures, and the evolving threat landscape.

Harnessing that momentum to revamp Federal civilian agency network security, the Biden-Harris administration implemented ambitious policies to transform how the Federal Government and its contractors secure their networks and supply chains, most notably through Executive Order 14028, Improving the Nation's Cybersecurity.

Under the skilled guidance of the Biden-Harris administration CISA has worked quickly to revamp its signature FCEB network security programs, the National Cybersecurity Protection System (NCPS) and the Continuous Diagnostics and Mitigation program (CDM).

These programs complement other authorities provided to CISA under the Federal Information Security Modernization Act, including the power to issue Binding Operational Directives, Emergency Directives, and technical security guidance to FCEB agencies, among other things.

Additionally, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, authorized CISA to hunt for malicious activity across FCEB's networks, with or without an agency's permission.

CISA's authorities outside NCPS and CDM, though critical to its FCEB network security mission, are outside the scope of this hearing.

Prior to the SolarWinds attack another major civilian agency attack in 2015 involved the Office of Personnel Management.

In 2015, the Office of Personnel Management data breach targeted information provided by security clearance applications submitted under the Standard Form 86 (SF–86).

At the time this attack was one of the largest breaches of Government data in U.S. history, the attack was carried out by an advanced persistent threat based in China.

In the aftermath of the 2015 Office of Personnel Management (OPM) breach, Congress enacted the Federal Cybersecurity Enhancement Act.

That legislation authorized NCPS and directed the department to deploy a Federal intrusion detection and prevention system to better detect breaches of Federal networks.

NCPS is a "system of systems" that, in addition to the EINSTEIN intrusion detection system, includes data analytics, information sharing, and core infrastructure capabilities.

Earlier this year, CISA announced plans to restructure NCPS and, over time, sunset the EINSTEIN intrusion prevention program.

EINSTEIN is designed to observe traffic going in and out of agency networks and relies on detecting known threats and, therefore, has limited effectiveness in modern network architectures or against novel attacks.

The remaining NCPS capabilities include data analytics, information sharing, and core infrastructure capabilities, which will be integrated into CADS.

CADS and the legacy EINSTEIN capabilities will be housed within the new Joint Collaboration Environment (JCE).

CISA boasts that the JCE will be a "best-in-class analytic environment that centralizes mission-relevant classified and unclassified data to enable more efficient analysis in large part due to increased automation."

Last year, Congress extended CISA's NCPS authorities until September 30, 2023, and they will expire at the end of the month unless Congress acts.

CISA intends for the new CADS program to support expanded capabilities that will improve the intake, integration, and automated analysis to facilitate the rapid identification, detection, mitigation, and prevention of malicious cyber activity.

According to CISA, CADS marks a significant expansion of NCPS's existing systems engineering, information technology infrastructure, and cyber operations tools and services.

The new JCE—and CADS, in particular—have the potential to dramatically improve how the Federal Government identifies and mitigates threats to Federal networks.

These new capabilities, however, rely on close collaboration with CISA's private-sector partners and vendors.

It is not clear that CISA has clearly articulated a complete vision for how it will implement its plans for JCE or CADS.

CISA also does not have a concrete plan for replacing or retaining EINSTEIN capabilities, even though "the visibility provided by existing EINSTEIN sensors remains a crucial enabler of CISA's mission to protect FCEB agencies."

In June, the General Services Administration issued a Request for Information on behalf of CISA seeking industry feedback on how to modernize the "legacy capabilities" of the EINSTEIN program.

I am interested in knowing if CISA has responded to the GSA or intends to respond to the question regarding EINSTEIN.

I thank today's witnesses and look forward to asking questions following the testimony of witnesses.

Thank you.

Chairman GARBARINO. I am pleased to have four witnesses before us today to discuss this very important topic. I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Chairman GARBARINO. Let the record reflect that the witnesses have answered in the affirmative. Thank you. Please be seated.

I would now like to formally introduce our witnesses. Brian Gumbel is the president of Armis, where he leads the company and its efforts to drive innovation in cybersecurity and emerging technology. Mr. Gumbel has spent 25 years in the tech industry, where he has worked for many companies, and is part of several advisory boards.

Steven Zakowicz is the vice president of CGI Federal, where he leads the DHS CISA account for the company. In this capacity, he leads a large team supporting 7 Federal agencies' participation in CISA's CDM program. In part of this role, Mr. Zakowicz oversaw a team providing environmental, health and safety, and regulatory compliance solutions and services to the chemical and energy companies. He also serves as a member of the American Council for Technology and Industry Advisory Council and the Washington Exec Cyber Council.

Joe Head is the chief technology officer and cofounder of Intrusion. He has held many roles with the company since its founding in 1983, and prior to that, he worked at Honeywell Optoelectronics. That was a tough one.

Finally, Robert Sheldon is the director of public policy and strategy at CrowdStrike. He leads corporate engagement on a variety of U.S. Federal, State, and local government policies, programs, and initiatives. He is the company's representative to CISA's Joint Cyber Defense Collaborative and the IT Sector Coordinating Council. In addition to his role at CrowdStrike, Mr. Sheldon serves as an adjunct professor lecturer on international cybersecurity policy at American University School of International Service.

Thank you all for being here today. Mr. Gumbel, I now recognize you for 5 minutes to summarize your opening statement.

STATEMENT OF BRIAN GUMBEL, PRESIDENT, ARMIS, INC.

Mr. GUMBEL. Chairman Garbarino, Ranking Member Menendez, and Members of the subcommittee, thank you for the opportunity to testify regarding our experience and perspectives on key programs designed to protect our Nation's most critical assets. As the leading asset intelligence security company, we share the mission and passion with all of you to ensure the protection and security of our Nation's critical assets. Many legacy programs tend to focus on what's commonly known as managed IT assets, but the growth beyond traditional managed assets is absolutely staggering. Our submitted testimony has a chart that highlights the explosion in what is referred to as unmanaged assets, or IOT, the internet of things, also operational technology, OT, and IOMT, which is medical technology.

When we discuss critical infrastructure, we must talk about and account for all unmanaged assets. We are encouraged by the focus and resources this committee and key agencies like CISA are putting toward building dynamic, resilient, and effective cybersecurity frameworks. A few of these programs that exist today, namely the CDM and EINSTEIN programs, have been in place for several years but need updating considering the expanding threat surface.

In the recent Executive Order on improving our Nation's cybersecurity, there are references made to the Federal Government partnering with private sector. This is a positive development, and

Armis looks forward to teaming with those agencies who are most responsible for protecting our Federal Government systems. The Executive Order states, incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. It mentions that the Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premise, or even hybrid. That the scope and protection of security must include systems that process data, such as information technology or IT, and that those that run the vital machinery that ensure our safety, operational technology, or OT.

The convergence of technologies and the discrepancies between devices offers a more complex and challenging task than the Federal Government has had to face just a few years ago. At Armis, our growing customer base consists of almost 50 percent of the Fortune 100, many large State and municipal governments, airports, ports, defense contractors, and key Federal agencies. These customers partner with us to achieve complete visibility and intelligence for all assets within their converged environments. Without such, we cannot be fully prepared for the growth of today and the uncertainties of tomorrow.

As stated in CISA's Binding Operational Directive, B.O.D. 23–01, continuous and comprehensive asset visibility is a basic precondition for any organization station to effectively manage cybersecurity risk. This directive focuses on asset discovery and vulnerability enumeration. To keep pace with technological change and rapidly-evolving threat landscape and deliver upon the letter and spirit of this Executive Order, bold change is needed now. CISA should align the CDM program updates to directives like B.O.D. 23–01 and should ensure that CDM dashboard is reflective and inclusive of existing and innovative technologies.

The Federal Government can no longer rely on legacy models, contracts, or solutions. What has worked in the past simply will not suffice now. Our adversaries are using automation to move at the speed of now, as should we. Armis is committed to working with CISA and other leading agencies to bring a holistic and inclusive approach where more complete and contextual cyber situational awareness and intelligence can lead to a resilient and responsive security posture.

I want to thank you all again for the opportunity to engage with the subcommittee. The resources of our entire organization stand ready to assist in the honorable mission of protecting our most critical national assets. I look forward to any questions that you may have.

[The prepared statement of Mr. Gumbel follows:]

PREPARED STATEMENT OF BRIAN GUMBEL

SEPTEMBER 19, 2023

Chairman Garbarino, Ranking Member Swalwell, and Members of the committee, thank you for the opportunity to testify and share our perspective on civilian agency cybersecurity programs. I applaud the committee's efforts in working to provide oversight and help improve impactful programs such as Continuous Diagnostics and

Mitigation (CDM) and Einstein. In accordance with a core function of the NIST Cybersecurity Framework that highlights the need to go beyond merely identifying devices but also understand the interdependence each asset has with each other and their relative importance to business objectives, we are honored to bring a contextual asset intelligence platform to our customers, partners, and Federal agencies.

Armis is THE leading asset intelligence cybersecurity company. We have been recognized by industry-leading analysts and publications as a platform provider who brings a level of insight, awareness, and actionable intelligence to our customers. Today it is important to not only know what exists in your network and cloud infrastructure, but the interdependencies and vulnerabilities within each asset. We are honored to be under consideration to become a member of CISAs JCDC, sharing the mission and passion with all of you in ensuring the protection and security of our Nation's critical assets.

We are encouraged by the focus and resources this committee and key agencies like CISA have put toward building dynamic, resilient, and an effective cybersecurity framework in protecting these assets. On May 12, 2021, the Executive Order on Improving our Nation's Cybersecurity states "Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life . . . ". It mentions that "The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid." And that "The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety and national sovereignty (operational technology (OT))."

In the Armis State of Cyberwarfare and Trends report 2022/2023 where 6,021 IT security professionals where surveyed we found that 73 percent of IT professionals in the United States say their company has experienced one or more cybersecurity breaches. Threat activity against the global Armis customer base increased by 15 percent from September to November 2022 with the largest threat activity coming from critical infrastructure organizations followed by health care organizations as compared with other industries.

Our job as the industry leader is to raise awareness and identify areas in need of attention and improvement. Our experience has shown that intrusions outside traditional IT "managed devices" have become more prevalent. Programs and frameworks that in the past have been primarily focused on these managed devices will be limited in their ability to address the larger growing attack surface.

At Armis our comprehensive contextual intelligence engine includes over 3 billion assets and growing and includes the entire spectrum of IT/OT/IoT/IoMT assets. We bring a level of contextual asset intelligence to our customers that introduces a holistic and responsive platform to assist in their mission. Our public-sector customers include several States, large city agencies, and cities and counties as well as the following highlighted below:

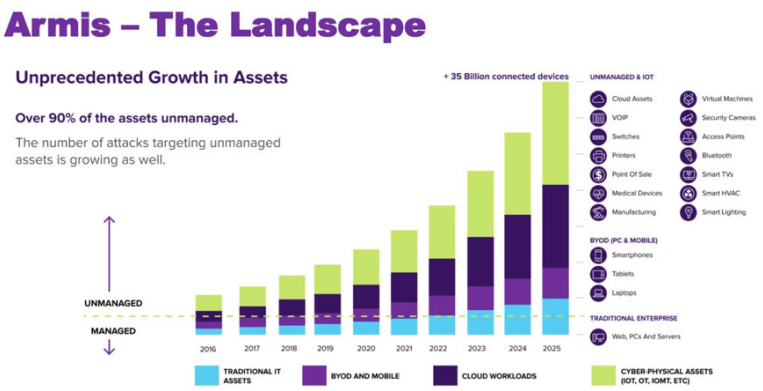
- An agency within HHS as well as numerous State agencies leverages Armis for Asset visibility and intelligence through integrations.
- A large defense contractor leverages the Armis platform for Asset Discovery, Intelligence, and Vulnerability Management
- A DOD agency leverages our platform for Asset Management and Security Workflow Remediation
- Department of Energy leverages Armis to increase automated identification and organization of the asset infrastructure across an entire lab.

Our enterprise and commercial customers include Drug and Manufacturing companies, Utility, Transportation, Aviation, and Healthcare organizations, and many others.

Our mission is to help organizations understand where and what exists in their environments and help put them in a position to identify and manage vulnerabilities to respond rather than react to a breach. You can't protect what you can't see and without addressing a visibility gap, organizations cannot be fully prepared for the growth of today and uncertainties of tomorrow.

We work with organizations throughout the globe to gain complete visibility into their managed and unmanaged assets. A "whole-of-nation" approach cannot be achieved without a complete view and deep level of intelligence of both managed and unmanaged assets.

As you can see in the chart below, the growth and in our opinion the growing attack surface introduce vulnerabilities heretofore unseen and even unknown. The convergence of technologies and the dependencies between devices has introduced a more complex and challenging task for those who are responsible for securing critical assets and operational environments.



As stated in CISA's Binding Operational Directive (B.O.D.) 23–01, "Continuous and comprehensive asset visibility is a basic pre-condition for any organization to effectively manage cybersecurity risk." This directive focuses on Asset Discovery and Vulnerability enumeration. Many agencies and enterprises are fortunate to have strong endpoint technologies in place (EDR) and solutions that help protect the perimeter, but the attack surface continues to grow and the cybersecurity perimeter which was well-defined just a few years ago is now dynamic and borderless. The introduction of unmanaged devices and operational technologies present challenges that cannot be addressed with legacy models and legacy technology. Present-day challenges and national security threats are now implementing AI and automated capabilities to identify the weakest link in the chain. Automated threats from U.S. adversaries requires automation and scalability delivering prioritization of cyber defense operators.

We applaud the activities toward the next-generation Einstein program, Cyber Analytics and Data System (or CADS). According to CISA's Eric Goldstein the system will integrate data from multiple sources, including "public and commercial data feeds; CISA's own sensors such as Endpoint Detection and Response, Protective [Domain Name System], and our Vulnerability Scanning service, which has thousands of enrolled organizations across the country; and data shared by both public and private partners,".

Creating next generation programs are crucial and as our customers would attest, knowing where every asset exists, what the profile of that asset is, and whether it is aged, vulnerable, or compromised in real-time will help to make the investment in next generation and existing solutions more effective.

We are committed to continuing to work with CISA and other leading agencies to bring a holistic and inclusive approach where more complete and contextual asset awareness, contextual intelligence, and attack surface definition can lead to increased resiliency and a responsive cybersecurity posture.

Some important and consistent feedback we hear from existing and former Federal CISOs, and CIOs includes the following:

"The focus should be on building modern security models, not perimeter-based, and should acknowledge and focus on cloud, zero trust, and IT/OT convergence.
"Many of the legacy models and contracts served us well in the past, but a new approach and model is needed."

These converged technologies deliver more efficiencies in the way we work but they introduce new vulnerabilities and complexities that legacy technologies are not built to identify, profile, or defend.

The "bold changes" highlighted in the E.O. call for a collaborative and inclusive programmatic and procurement directive that does not rely on legacy models, contracts, or solutions. What worked in years past will not suffice. Our adversaries are actively trying to exploit our visibility gaps, particularly in critical infrastructure. Our approach should be engaging with new and innovative 21st Century technologies. Lest we forget, bad actors are moving at the speed of now as should we!

RECOMMENDATIONS

- Design and implement a procurement path that allows for more expedient purchase and implementation of newer technologies built to align with the growing attack vectors and surface.
- Improve coordinating between programs like U.S. Digital Services, the Technology Modernization Fund, and CISA to create programs which enable agencies to quickly integrate and maintain newer technologies and services into their framework portfolios.
- Fund the Technology Modernization Fund so that return on investments can reliably cover both the simultaneous deployment of new technology and the retirement of legacy services.
- Align program updates to stated directives. For example, if Directives state cloud-first and all assets, agencies should have the ability to implement those solutions that are not limited to a subset of technologies. Currently the CDM program addresses only IT devices rather than the full spectrum of connected risk: IT/OT/IoT/IoMT. BOD 23–01 focuses on Asset Discovery and Vulnerability Enumeration. Requiring that the full spectrum of converged and connected technologies be inventoried and reported would give these programs more alignment to stated administration and agency objectives. Having only most of your roof covered in a storm won't prevent water from entering!
- The CDM program and dashboard should reflect all existing and upcoming technologies that need integration vs. a limited few to be effective.
- We encourage continued strong support of the CDM program with the appropriate measures taken to be more inclusive of technologies that may not be part of the existing program.

Thank you again for the opportunity to speak with this committee. The resources of our entire organization stand ready to assist in the honorable mission of protecting our Nation's most critical assets.

Chairman GARBARINO. Thank you, Mr. Gumbel. Mr. Zakowicz, I now recognize you for 5 minutes to summarize your opening statement.

STATEMENT OF STEPHEN ZAKOWICZ, VICE PRESIDENT, CGI FEDERAL, INC.

Mr. ZAKOWICZ. Chairman Garbarino, Ranking Member Menendez, and other distinguished Members of the Subcommittee on Cybersecurity and Infrastructure Protection, thank you for the opportunity to testify today. My name is Steve Zakowicz. I am a vice president at CGI Federal, and for the past 4 years, I have served as a project manager on CGI Federal's contract with the Continuous Diagnostics and Mitigation, or CDM, program. At the subcommittee's invitation, I'm here on behalf of CGI Federal today to provide perspective on the achievements of CDM and its path forward. Since 2016, CGI Federal has played an important role in the CDM program, providing capabilities to participating agencies through tailored solutions and a robust shared services platform.

Our company is currently the system integrator on two CDM Dynamic and Evolving Federal Enterprise Network Defense, or DEFEND, contracts. The first provides tailored CDM solutions to seven large Federal agencies: Departments of Commerce, Justice, Labor, State, FCC, TVA, and USAID. The second provides a state-of-the-art, cloud-based shared services platform currently supporting 65 smaller and independent Federal organizations leveraging those CDM capabilities.

CGI Federal has almost 300 skilled professionals and specialized subcontractors supporting the CDM program today. Given our experience in the CDM program, I would like to use my opening remarks to highlight four points regarding the program's success to date and suggestions to meet evolving objectives.

First, civilian agency partners must be appropriately resourced, funded, and committed for CDM to be successful. CISA cannot do this alone. Congress can help to ensure civilian agencies are approaching cyber preparedness with the appropriate level of attention and investment. Also, funding lapses or limitations stemming from uncertainties surrounding shutdowns and continuing resolutions do impact CDM's continuity and ability to carry forward new initiatives. Second, Executive Order 14028 called Improving the Nation's Cybersecurity enhanced CISA's ability to effectively perform its mission.

For example, authorizing CISA to engage in cyber hunt, detection, and response activities through endpoint detection and response, or EDR, solutions deployed via CDM. Congress could bring stability to CISA's authority to perform these critical activities by codifying appropriate authorities within the Executive Order into law. I understand this is currently under consideration by Congress in pending updates to the Federal Information Security Modernization Act of 2014, also known as FISMA.

Third, emerging opportunities exist to leverage CDM capabilities for State, local, Tribal, territorial, as well as critical infrastructure entities by using this existing shared service platforms and capabilities. The shared services approach can provide these target-rich but resource-poor stakeholders across the Nation the ability to leverage proven capabilities in a cost-efficient way to defend against threats they face, including nation-state actors and ransomware attacks.

Fourth, the evolution of the CDM dashboard ecosystem is an especially promising development. The dashboard has become the first venue of consultation for a wide variety of users within CISA's cybersecurity division, including threat hunt, vulnerability management, and directives and guidance organizations. The level of visibility across the Federal enterprise provided through the dashboard, combined with agency network visibility through EDR, has been a force multiplier and is a terrific case study in the innovation and power of combining data from multiple sources to accelerate progress.

In conclusion, I would like to affirm to the subcommittee CGI Federal's continued and unwavering commitment to our partnership with CISA on its core mission of strengthening America's cybersecurity. Thank you. I look forward to your questions.

[The prepared statement of Mr. Zakowicz follows:]

PREPARED STATEMENT OF STEPHEN ZAKOWICZ

SEPTEMBER 19, 2023

INTRODUCTION

Chairman Garbarino, Ranking Member Swalwell, and other distinguished Members of the Subcommittee on Cybersecurity and Infrastructure Protection, my name is Stephen Zakowicz. I am a vice president at CGI Federal Inc. ("CGI Federal"). As a wholly-owned U.S. operating subsidiary of CGI Inc. ("CGI"),[1] CGI Federal and its

[1] Founded in 1976, CGI is among the largest independent information technology ("IT") and business consulting services firms in the world. With 90,250 consultants and professionals across the globe, CGI delivers an end-to-end portfolio of capabilities from strategic IT and business consulting to systems integration, managed IT and business process services, and intellectual property solutions. CGI works with clients through a local relationship model com-

7,100 employees partner with Federal agencies to provide solutions for homeland security, defense, civilian, health care, justice, intelligence, and international affairs. During the last 4 years, I have served as the project manager on CGI Federal's contract with the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") for the Continuous Diagnostics and Mitigation ("CDM") Program. On behalf of CGI Federal and its employees, I am pleased to submit this written testimony to the subcommittee regarding the CDM Program.

CDM is a mission-critical Federal program that provides participating agencies with solutions and services to identify and combat cybersecurity risk. Since its original contract award in 2016, CGI Federal has provided this support to 100 participating agencies through tailored solutions and a robust shared services platform. CGI Federal is currently the prime contractor on two CDM Dynamic and Evolving Federal Enterprise Network Defense ("DEFEND") Task Orders—DEFEND C and DEFEND F. Under its DEFEND C Task Order, CGI Federal provides tailored CDM solutions to 7 large Federal agencies: Department of Commerce ("DOC"), Department of Justice ("DOJ"), Department of Labor ("DOL"), Department of State ("DOS"), Federal Communications Commission ("FCC"), Tennessee Valley Authority ("TVA"), and United States Agency for International Development ("USAID"). Under its DEFEND F Task Order, CGI Federal developed a state-of-the-art cloud-based Shared Services CDM platform, and currently operates and provides access to that platform to 65 non-Chief Financial Officer Act ("CFO Act") Federal agencies. Roughly 300 CGI Federal employees and subcontractors support the CDM program.

CDM: CURRENT PROGRAM STRUCTURE

As stated in the DHS fiscal year 2024 Congressional Budget Justification for CISA, "the CDM program provides the Department, along with other Federal agencies, with capabilities and tools to identify cybersecurity risks to agency networks on an ongoing basis. It prioritizes these risks based on potential impacts and enables cybersecurity personnel to mitigate the most significant problems first . . . Furthermore, CDM enables CISA and agencies to proactively respond to threats through the deployment of multiple different security capabilities, including data protection technologies, Endpoint Detection and Response (EDR), cloud security platforms, and network security controls, and enables CISA to continually evaluate the cybersecurity posture of [Federal Civilian and Executive branch ("FCEB")] systems and networks."

As CISA describes on their public website, the CDM program is structured to provide cybersecurity protections and capabilities in four key areas:

- The Asset Management (AM) capability is aimed at providing agencies with a centralized overview of their network devices and the risks associated with such devices. Asset Management enables an agency to maintain and improve its cyber hygiene through 5 capabilities: hardware asset management (HWAM), software asset management (SWAM), configuration settings management (CSM), vulnerability management (VUL), and enterprise mobility management (EMM).
- The Identity and Access Management (IDAM) capability is intended to manage the access and privileges of agency network users. Managing who is on the network requires the management and control of account and access privileges, trust determination for people granted access, credentials and authentication, and security-related behavioral training.
- The Network Settings Management (NSM) capability is designed to provide agencies with greater visibility into what is happening on their networks, which also gives them a better understanding of how the networks are being protected.
- The Data Protection Management (DPM) capability is intended to provide additional protections to the most critical mission data and systems on Federal civilian networks. While the other CDM capabilities provide broader protections across Federal networks, the DPM capability is focused on protecting sensitive (especially private) data within the agency.

These capabilities are centrally managed and reported through the CDM Dashboard Ecosystem, a cloud-based visualization and data analytics layer that allows agencies and CISA to obtain a top-level view of cybersecurity risk posture and access details regarding how individual systems and endpoints contribute to that risk posture. This allows agency personnel to quickly identify and address the highest risk cybersecurity vulnerabilities first.

---

plemented by a global delivery network that helps clients digitally transform their organizations and accelerate results.

The current CDM program consists of 7 individual Task Orders to provide consistent, prioritized CDM capabilities to FCEB agencies. Those Task Orders are:

- CDM DEFEND A: Providing CDM program requirements to DHS
- CDM DEFEND B: Providing CDM program requirements to DOE, DOI, DOT, OPM, USDA, and VA
- CDM DEFEND C: Providing CDM program requirements to DOC, DOJ, DOL, DOS, FCC, TVA, and USAID
- CDM DEFEND D: Providing CDM program requirements to GSA, HHS, NASA, SSA, and Treasury
- CDM DEFEND E: Providing CDM program requirements to DOED, EPA, FDIC, HUD, NRC, NSF, SBA, and SEC
- CDM DEFEND F: Providing CDM program requirements to up to 75 small and medium FCEB agencies through a Shared Services platform
- Dashboard Ecosystem: Developing and hosting a common CDM Dashboard platform on behalf of CISA to receive and consolidate information from participating CDM DEFEND agencies.

CDM PAST AND PRESENT

Since its inception in 2012, the CDM program has evolved to meet the priorities and relative maturity of the FCEB cybersecurity risk posture. When the CDM program began, it focused on implementing a standard set of commercial solutions to meet CDM-identified technical capabilities for enterprise visibility and protection. At that time, the program implemented cybersecurity risk management across the FCEB enterprise. Over time, however, the program recognized the need for flexibility to accommodate unique requirements and differing maturity levels from one agency to the next. Through CDM DEFEND, CISA addressed that need, and built a model focused on long-term, sustained engagement, delivering custom solutions tailored to each agency's unique environments and cybersecurity needs.

Within the DEFEND model, CISA has further refined its approach to delivering cybersecurity services. For example, CDM DEFEND activities initially focused on delivering a single capability (e.g. Asset Management or Identity and Access Management) to all participating agencies. After deploying these foundational capabilities, CISA evolved to deliver services based on agency readiness model. In advance of agency engagement, CISA works with the agency to identify where program priorities align with an agency's ability to implement and maintain a specific capability. Using this readiness model, CISA validates that both CISA and the agencies are adequately funded and have the resources necessary to successfully deploy, operate, and maintain the cybersecurity solutions.

The evolution of the CDM program is also driven by new regulations and executive guidance. For example, Executive Order 14028 "Improving the Nation's Cybersecurity" (the "EO"), issued on May 12, 2021, provides greater visibility to agency environments as it grants CISA access to object-level cybersecurity data collected through CDM (see Section 7(f)). The EO also authorizes CISA to engage in cyber hunt, detection, and response activities through Endpoint Detection and Response ("EDR") solutions deployed through CDM. These EO requirements grant CISA unprecedented visibility into agency network environments to proactively identify and remediate threats and apply observations in one agency environment across the FCEB enterprise.

Through the CDM program, CISA has gained critical visibility into the cybersecurity posture across the entire FCEB enterprise and is well-positioned to quickly identify, assess, and remediate potential threats to agency network environments and, by extension, U.S. national security. Specific accomplishments include the broad roll-out of EDR to FCEB agencies and the onboarding of roughly 250 CISA threat hunters to conduct analysis through EDR and CDM Dashboard Ecosystem solutions. That access coupled with the availability of object-level data through the Dashboard Ecosystem has been a "force multiplier" in providing CISA the ability to identify, assess, and remediate anomalies across the Federal enterprise network.

FUTURE OF CDM

CISA continues to evolve its CDM program to meet the needs of its stakeholders. Further, as CISA prepares for the next generation of CDM, it has actively engaged with industry and identified likely future priorities that include:

- Issuing Task Orders based on CDM capability to be applied across the entire FCEB community to promote consistency in solutions across agencies.
- Delivering CDM capabilities to State, local, Tribal, territorial (SLTT), and critical infrastructure (CI) stakeholders.
- Expanding access to Shared Services across CDM capabilities.

- Enhancing alignment and collaboration among CISA, FCEB agencies, and the cybersecurity tool vendor community.

CONCLUDING OBSERVATIONS

As a Federal contractor proudly supporting the CDM program, CGI Federal offers the following observations for consideration:

- Success of CDM's mission depends heavily on FCEB agencies applying the resources and funding to invest in cyber preparedness. Further, funding lapses or delays due to government shutdowns or Continuing Resolutions impact program continuity and ability to operate sustainably.
- Executive Order 14028 "Improving the Nation's Cybersecurity" enhanced CISA's ability to effectively perform its mission through, for example, authorizing CISA to engage in cyber hunt, detection, and response activities through EDR solutions deployed via CDM. Congress could ensure stability in CISA's authority to perform these critical activities by codifying these authorities into law.
- CISA could enable SLTT and CI stakeholders to leverage existing CDM shared service platforms and capabilities to defend against cyber threats such as ransomware attacks. These strategies would allow stakeholders to leverage valuable capabilities in a cost-efficient way to defend against threats such as ransomware attacks.
- The use of the Dashboard Ecosystem and EDR as a "first venue of consultation" for newly-identified critical vulnerabilities or anomalous network activity by CISA represents a force multiplier and a new era of centralized hunt and response capabilities within the FCEB. These foundational capabilities can be further leveraged in innovative ways to improve our national security risk posture.

CGI Federal appreciates the critical nature of the CDM program, as well as CISA's core mission. CGI Federal is proud to support CISA and the CDM program in working to secure the Federal Government's networks for citizens across the United States. CGI Federal also thanks the subcommittee for its continued oversight to ensure the continued success of the CDM program.

Chairman GARBARINO. Thank you, Mr. Zakowicz. Mr. Head, I now recognize you for 5 minutes to summarize your opening statement.

STATEMENT OF JOE HEAD, CHIEF TECHNOLOGY OFFICER, INTRUSION

Mr. HEAD. Thanks so much. Pleasure to be here with you guys today. We spent a lot of time, as do most I guess, on making the submittal perfect and word crafting, but I think me reading it is boring. So, what I'd like to do is just talk to a few things that aren't on there that I think are important.

You mentioned the CRs. We've got one critical breach we've been waiting on working for 4 years against the U.S. military, and they were first under a CR. Then when they were not under CR, they didn't have a budget. Then when they had a budget, they were back under a CR again, and we haven't spent dime one on anything yet.

So, when you start looking at major programs like you're discussing today, it is a layup that they will continue somehow. But when you have a reaction to a breach, God help you. There's nobody coming. You can't get budget. You can't get help. So, I would urge you guys, I've talked to Kay Granger about doing some sort of cutout where you say, this percent of your budget can be spent on a breach response. I would encourage you guys to think of a way in law to accommodate that.

If you look at the United States, all of us in the security business would like to say it's good. But I remember there was a comedian that says you go to a college and them bragging about their smarts is like going to an ER and everybody bragging about their health.

The United States is not secure. We suck at security. There's a new breach every 37 seconds. I went to a meeting one time with the STRATCOM chief, and they had all the chiefs of industry lined up at one end, and the rest of us with little companies lined around the outside, and basically said, we spend more on R&D every day than you guys in revenue every year. We got it covered. Well, they don't.

So, what I would urge you guys to think through is, how can you help the threat hunters do better? Then part of the thing that you guys could do with the CISA meetings is ask the simple question like a 4-year-old, if we do this, are we done? Are we finished yet? So, when they finish the program, can you truly say, every threat we have is fixed?

You know, if somebody decides they are going to roll up and sink an aircraft carrier, we're going to unleash holy hell on them. They don't think twice, they won't do it. But in cyber, sure. Take down this, take down that, steal these secrets, bankrupt the only supplier outside of China that can do a thing. They do it with impunity. So, we need to get to the point in cyber where people are scared to hit the enter button, and they are not scared.

So, I would suggest that, you know, I'm not here because I'm part of these programs. I'm here because I see how suck we are at security as a Nation and as a world. The offenders have asymmetry to their huge advantage. One guy in a room doing an all-nighter come up with zero day that ain't nobody going to see. I mean, I named my company Intrusion after intrusion detection systems. My joke was all IDS systems are this helpful system that hands you a Polaroid of the fist that just broke your nose. I don't need that. Can you just give me a system that stops the fist?

So, I think if we ask the questions better. We ought to be asking, if I do this, am I done? Is my COM system undownable? One big thing that I think we need to do in law and policy that you guys could help a lot with is it's—I'm sorry, I'm Texan, so, I don't know about PCness, but, you know, back when the cowboys and the Indians were fighting, the Indians didn't make guns, they didn't make bullets, and the outcome was certain. They were screwed. You can't fight if you don't make the stuff. Right now, there's no computer in any office here that wasn't assembled in China. Everything they wanted on it was on it when they shipped it.

So, when you start talking about being secure, gee, sanitation starts early, you know, and we need to have a cleaner environment to build things on. So, we don't make routers in America, we don't make servers, we don't make computers. We need to re-onshore some stuff.

I think there's room. If you read my testimony, I talked about doing a cyber Manhattan Project and I think we should. There's some of us here at the table, and we could name others that should be on the group. It's not just a contractor loop. There's some genius-level folks around the community that know what to do, but they haven't been tasked to fix it. So, I'd encourage you guys to stir that up a lot. So anyway, for the non-ad hoc stuff, feel free to read what we wrote. Thanks for letting us be here.

[The prepared statement of Mr. Head follows:]

PREPARED STATEMENT OF JOE HEAD

Good morning, and thank you Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the subcommittee. My name is Joe Head. I am the cofounder and chief technology officer of Intrusion—proudly headquartered in Plano, Texas.

It is both a privilege and an honor for me to be here today, sharing my technical expertise and insights, which I have accumulated over four decades of immersion in the cutting-edge realms of the cybersecurity industry. I wholeheartedly commend the dedicated individuals on this subcommittee and their staff for their tireless efforts. They understand the need to enhance the Federal Government's cybersecurity capabilities but are also channeling their energies toward advancing the mission of agencies like CISA, with a strong focus on developing next-generation software and technologies that are critical in the forthcoming cyber conflicts.

I began designing and providing secure networks and other security solutions for the U.S. Government when Ronald Reagan was President. We built equipment for the hotline from the White House to the Kremlin during his second term. I co-founded my company Intrusion in 1983, just 3 years out of college and we've been a public company since the '90's.

I've had more fun designing and securing things than you should get paid for. My goal today is to help the committee spur innovation in security. The United States is not secure. There are some secure networks, but very, very few. Complacency with the state of our security is a serious risk. A relaxed defender is the most naive one. Cyber offense is winning everywhere. A great challenge of our time is to make defenders better able to defend. I have an old friend who liked to say that he'd rather be lucky than smart. A network or system not breached is not a matter of the defender being lucky or smart, it is sadly that an attacker just isn't interested enough to focus on breaching it.

As you read my opening remarks, keep in mind that an outline of the Manhattan Project was not put in the *Congressional Record* before Los Alamos was built. Our Government needs people with technical depth and a winning mindset. My job is not to inform our enemies what we plan to do to win the cyber war but to methodically ensure we take this domain. We do know what to do. There are core experts both in Government and industry that understand what winning would require and how to get there. This path also includes how not to get there by spending billions unwisely.

Today I too often see security plans and programs looking a lot like children's soccer—a bunch of kids clustered around the ball. In cyber, the kids are always automating the hottest buzzwords without a grand plan to produce an absolute win. The challenge is to wisely architect a plan, put the right people in charge of defining the requirements, manage a design production, and reliably deploy a cyber get-well plan.

We must have a get-well plan in cyber which gets silently built and deployed, representing a master stroke in reversing the reality of our current predicament. Adversaries all over the world are killing it in cyber with massive asymmetry, winning and penetrating millions of systems that we need to be trustworthy. Many are capable hackers working inside adversary cyber operations or just as individuals on their own.

It was in the 1990's while identifying a threat at an automotive manufacturer that I realized we needed a better way to find the needle in the haystack. I built a database to understand what the internet looks like, who owns what, which areas were unsafe to visit. This analytic engine has evolved into a mainstay of defense-in-depth cybersecurity. By the early 2000's we built a tool to inspect and audit internet travels. Today, we know what traffic is coming and going from monitored systems, but more importantly how to stop threats from impacting operations.

Now is a critical time for the U.S. Government, U.S. critical infrastructure, and critical parts of U.S. industry. If the world was awesome at cybersecurity, there wouldn't be a breach every 37 seconds. The more you know, the worse it looks. Is it hopeless? No. Is there reason to believe that the USG will naturally solve the problem? No. But the entirety of the Nation faces continuous and advancing attacks precisely because of U.S. commercial and Governmental successes, so the USG must strategically cultivate protections.

As a student of history, we have seen dramatic examples of innovation in the face of new threats. There were dramatic examples in WW2 when foreign threats and war drove U.S. innovation to new heights. Sadly, few programs in the cyber field are constructed to be game-changers. Mostly they scale up and automate a few elements of a good security approach but are not master strokes of a comprehensive solution. In other words, when the projects are done you won't be truly secure. Well-

automated partial solutions don't make you secure, they just delay risk and make companies poorer from the expenses. While we must improve our baseline defensive posture to exponentially increase the cost of attack, profit-motivated hackers, criminals, and adversaries have already doubled-down on their attack investments with extensive resourcing.

We already know that signature-based defenses fall in the face of zero-days and basic offensive threats. Most defenses ignore attacks via trusted sources like supply chains and security tools. The adversary is operating faster than the decision cycle of defenders, hidden in the vast noise of network traffic. Similarly, most budget requests and coding projects are to scale up defenses that cannot see novel compromises that have never been seen before, much less stop these threats completely. We have the capability now to tell if the crown jewels leave on a path headed for the shadows. With the advent of machine learning, network tools have identified and blocked untrustworthy sites, automatically guiding both people and devices to avoid the untamed internet, or offering them a picture of the monster rather than letting them directly reach out and touch it. But the unknowns must also be stopped, which requires knowing what good looks like.

Enemies are already exacting heavy costs on the United States with cyber. Threats have been quietly planted into our infrastructure. Today—our country is still too reliant on foreign factories and vulnerable supply chains. The United States does not make the computers, routers, switches, process controllers, dock cranes, pumps for gasoline, car parts, cameras, medicines, chemicals, and many other electronic things. But in cyber, it is much worse if your adversary made all the computers used in critical infrastructure or weapons systems. If your enemy left a back door or a designed-in a kill switch—they might use it. True security requires covering the supply chain threat as well as all other classes of threats like hackers and the insider threat.

SOLUTIONS

Why was I interested in testifying on this topic today? I believe that there is a chance that the United States can re-achieve the needed sense of urgency these threats require. Investments in critical infrastructure, strengthening supply chains, and reshoring critical manufacturing are all necessary investments for our security. We must continue to be proactive in our approach to cybersecurity.

The allocation of over $400 million in funding for the transition from Einstein to CADS is a significant level of funding. It is imperative, however, that the CADS program design and implementation are meticulously executed to deliver not only enterprise-wide system monitoring and control but also the seamless handling of vast volumes of data and information. Intelligent and actionable outputs must be quickly and proficiently delivered to a broad audience. History has shown that well-intentioned technological advancements can be hindered by overly complex and convoluted designs, drowning users in a sea of tools and unnecessary complexity. We must keep in mind that offensive cyber operations can be cheap and flexible. Just like water can find any hole in a ship, building, or computer system and cause massive damage—a cyber attacker needs only to be creative enough to find or create one hole to get in and defeat you with cyber. We must remove those attacks from the shadows of the internet, cut through that barrage of noise, and enable network defenders and analysts to discover the anomalies in the trusted high ground, where the maturing U.S. cyber workforce can collaborate to investigate without having resources overwhelmed. We can start by identifying what good looks like. How should safe software and devices behave? Knowing these profiles drives proficient identification of threats.

Concurrently, we must remain vigilant against the pitfalls of comprehensive coverage leading to comprehensive failure. Adversaries will monitor our progress and respond. In the realms of design, application, and deployment, we must consistently ask ourselves how to intelligently and efficiently innovate new capabilities and approaches into a far more effective solution. This ensures that our legacy solutions, designed to address legacy problems on a massive scale, are agile enough to perform effectively in real-world scenarios.

To achieve success, systems like CADS must work quickly, easily, and reliably. That is difficult. Solutions need to respond immediately to a threat, preventing outbound communications and impact to system operations. The response should be simple and as automated as possible—and not labor-intensive—overwhelming our already-taxed defenders. Plans need to account for integration and sustainment at the outset. And be agile enough to know that new things will need to be included over time. Our systems need to be real-time, 24/7 without a nagging string of alerts. A system that is both powered by quality and comprehensive data.

Beyond the outside threats, the CADS system should support zero-trust principles to mitigate and uncover compromises of accounts and systems. Digitally this means understanding the following about a system and its users:

- Who are the users?
- How do they behave?
- What is their reputation?
- Who have they been associating with?
- What does normal activity look like for mission need?
- What are the indicators of malicious intent?
- What are common traits of targets for a particular attack?
- How can targets reduce their exposure before being targeted?

Moreover, it's essential to examine how a relatively modest investment in pioneering technologies and capabilities could potentially revolutionize our cybersecurity approach. By allocating funding to these "moonshot" endeavors, even in the order of a few million dollars, we may uncover the next major breakthrough in cyber defense, at a cost that pales in comparison to the budget required for comprehensive systems like CADS.

We strongly recommend these flagship programs and agencies acknowledge that without specific and targeted funding for strategic research and development, we run the risk of neglecting the cyber defenses necessary for the latter half of the 21st Century. DOD does this with DARPA and other programs. That's one model, but any substantial investment in major cyber defense programs, without accompanying funding for innovative and transformative technologies, could render these programs vulnerable. Much like the Maginot Line, an unforeseen breach in an inadequately defended area could undermine the entire defense system, rendering it futile and ineffective.

As I conclude my opening remarks, I would like to emphasize to the committee that while the introduction of the CADS system seems to represent a significant stride in the right direction, we must not let complacency take root. We should actively seek ways to complement the capabilities of CADS with innovative functions and useable systems that align with our overarching mission of fortifying the U.S. cyber defense posture. By doing so, we can ensure that our Nation remains at the forefront of cybersecurity, prepared to confront the evolving challenges of the digital age.

Just like the Manhattan Project would not have worked without a core team of geniuses backed up with a massive support and implementation program—now is as good a time as any to take charge. Congress can wisely pass laws and fund efforts that guide the course of this cyber conflict. We don't need to wait for our communications, power, logistics, and critical infrastructure to be taken offline in the lead-up to a conflict.

Spending tens of billions on the latest partial buzzwords isn't a winning strategy, let's implement a winning cyber strategy on a tight time line at an achievable budget. This path doesn't stop the kids' soccer teams from doing what kids do with massive pieces of Federal budgets, so let's carve out 5 percent for a cyber Manhattan Project that surprises the world with a defensive cyber solution that came out of nowhere and reversed the asymmetry of this conflict which we are losing. Winning is better.

Thank you again Mr. Chairman and Mr. Ranking Member for inviting me into this subcommittee's discussion today. I would be happy to answer your questions.

Chairman GARBARINO. Thank you, Mr. Head. Mr. Sheldon, I now recognize you for 5 minutes to summarize your opening statement.

STATEMENT OF ROB SHELDON, SENIOR DIRECTOR, CROWDSTRIKE

Mr. SHELDON. Chairman Garbarino, Congressman Menendez, Members of the subcommittee, thank you for the opportunity to testify today. Government functions are predicated on operable information technology systems. Because these functions underpin national security and other key services, Federal cybersecurity is a topic of paramount importance.

CrowdStrike is a U.S. cybersecurity company with employees in the United States and abroad. We are a provider of endpoint security technologies, cyber threat intelligence, and cybersecurity services to CISA and a host of other Federal agencies. We are proud

to be an alliance member of CISA's Joint Cyber Defense Collaborative, JCDC. We also have unique perspectives from being a leading commercial provider serving major technology companies, 15 of the top 20 largest U.S. banks, and thousands of small and medium-sized businesses.

Over the past several decades, the Federal IT landscape has changed drastically. Beyond desktops and servers, we must now defend cloud environments, mobile devices, internet of things devices, and even specialized operation technologies. In parallel, the volume and severity of cyber threats to Federal systems is increasing.

Over the past few years, adversaries like China and Russia have successfully breached the U.S. Government on multiple occasions. In July, Chinese threat actors once again exploited authentication flaws in a major software vendor's email and office productivity platform, this time resulting in threat actors' unauthorized access to the email of two Cabinet Secretaries.

The Federal Government approach to cybersecurity is now evolving. An initial major cybersecurity program launched in 2008, the National Cybersecurity Protection System, NCPS, and its EINSTEIN capability focused on perimeter defense. But this strategy has fallen out of favor as most enterprises no longer even have a perimeter to defend. A complementary program, Continuous Diagnostics and Mitigation, or CDM, was created in 2012. This program offered a flexible portfolio of technologies to defend Federal networks. While CDM had a slow start, it has accelerated meaningfully over the past year, thanks in part to the addition of key endpoint detection and response, or DAR, efforts.

This year, CISA officials announced the creation of two associated programs, the Joint Collaborative Environment, JCE, and the Cyber Analytics and Data System, CADS. CADS, in particular, will be central for supporting a variety of new data-intensive operational requirements. Among other things, this includes implementation of the Cybersecurity Incident Reporting for Critical Infrastructure Law, CIRCIA, passed last year.

Beyond programs, Federal cyber policy has changed in recent years to better address threats. Congress provided CISA the authority to threat hunt across Government networks in the fiscal year 2021 National Defense Authorization Act. The White House issued Executive Order 14028 in May 2021. This initiated key efforts for endpoint security, log retention, cloud adoption, and incident response standardization. In 2022, the Office of Management and Budget, pursuant to Executive Order 14028, issued a Federal Zero Trust Strategy that clarifies and aligns Government efforts on implementing zero trust principles. This year, the Office of the National Cyber Director issued a new National Cybersecurity Strategy and an associated implementation plan that provides a roadmap and dates for several important cybersecurity initiatives.

I'd like to offer a few recommendations for Federal cybersecurity going forward. New programs such as CADS must be designed to enable flexibility and be built for scale. The expanded use of cloud workloads, growing log retention needs, and the use of artificial intelligence, or AI, each entail extensive data processing requirements. As noted above, the recent addition of EDR capabilities has strengthened CDM, but when the time comes to modernize that

program itself, stakeholders should consider clear terms for long-term cost-sharing and additional shared services approaches. The Federal Information Security Modernization Act of 2014, FISMA, is of a similar vintage as CDM and could benefit from reform. A bill that aligns disparate Federal IT policies accrued over the past 10 years would improve cybersecurity outcomes.

Looking ahead there are a number of emerging technologies that would further strengthen the Federal cybersecurity posture. These include Extended Detection and Response, or XDR, which enables integrated EDR like visibility and control to cybersecurity products beyond the endpoint, identity threat detection and response, which supports zero trust adoption objectives, and expanded use of AI, which can enhance a broader range of cybersecurity solutions, and managed security services, which can enable high-fidelity commercial support to distributed Federal security operations. Each of these is described in more detail in my written statement. Thank you again for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Sheldon follows:]

PREPARED STATEMENT OF ROBERT SHELDON

SEPTEMBER 19, 2023

Chairman Garbarino, Congressman Menendez, Members of the subcommittee, thank you for the opportunity to testify today. Materially all Federal Government functions are predicated on operable information technology (IT) systems. Given that these functions include the provision of key services that underpin national security and our way of life, Federal cybersecurity is a topic of paramount importance.

CrowdStrike is a U.S. cybersecurity company, with employees across the country and globally. We bring a unique perspective on Federal cybersecurity issues. We are a provider of endpoint security technologies, cyber threat intelligence, and cybersecurity services to the Cybersecurity and Infrastructure Security Agency (CISA) and other Federal agencies. We are proud to be an original plank holder of CISA's Joint Cyber Defense Collaborative (JCDC). We also have unique perspectives from being a leading commercial provider serving major technology companies, 15 of the top 20 largest U.S. banks, and thousands of small and medium-sized businesses.

Over the past two decades, the Federal IT enterprise has swelled in size and scope. No longer basic networks of desktops and servers, Federal IT today includes cloud workloads, mobile devices, internet of things (IoT) devices—and even specialized operational technology (OT).

In parallel, the volume and severity of cyber threats to Federal systems has increased. Nation-state threat actors regularly seek—and too often, succeed—in breaching Federal enterprises. Over the past few years, major incidents have enabled adversaries like China and Russia to collect sensitive intelligence. In July, Chinese threat actors once again exploited authentication flaws in a major Federal vendor's office productivity and email platform—this time resulting in threat actors' unauthorized access to the email of two Cabinet Secretaries.[1] Under slightly different geopolitical conditions or adversarial objectives, these incidents could have enabled scaled destructive attacks.

The evolution in the IT environment and worsening of the threat landscape mean it's important to regularly review and assess the efficacy of Federal cybersecurity measures—which include policies, programs, and strategies.

---

[1] See Nakashima, Ellen. Menn, Joseph. Harris, Shane. *Chinese hackers breach email of Commerce Secretary Raimondo and State Department officials.* The Washington Post, July 14, 2023. *https://www.washingtonpost.com/national-security/2023/07/12/microsoft-hack-china/;* and *Results of Major Technical Investigations for Storm–0558 Key Acquisition,* Microsoft, September 6, 2023. *https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/.*

A BRIEF BACKGROUND ON CISA'S PRIMARY FEDERAL CYBERSECURITY PROGRAMS [2]

By the early 2000's, Federal IT infrastructure had grown significantly. Cybersecurity protections were still fairly organic, with different agencies adopting different approaches, dedicating disparate resources, and achieving uneven outcomes. A significant uptick in cyber attacks targeting national laboratories, major defense industrial base entities, and the Federal Government agencies themselves highlighted the need for greater investment and more standardization.

National Cybersecurity Protection System (NCPS).[3] Established in 2008, NCPS's goal was to protect Federal networks through a suite of perimeter defense technologies called "EINSTEIN," as well as an associated analytic capability. Leveraging intrusion detection and later intrusion prevention capabilities, EINSTEIN would attempt to defeat threats prior to threat actors accessing sensitive systems, like endpoints, or sensitive data. While the program clearly improved Federal cybersecurity posture from the status quo ante, and the associated analytic capabilities supported broader initiatives, EINSTEIN itself was not ultimately well-suited to meet the full scope of cyber threats to the ".gov."

Perimeter defenses are only one small part of cybersecurity. Two concepts help explain why. The first is the assumption of breach. Elite defenders have come to assume that threat actors can—and indeed, already have—breached perimeter defenses. Whether through a supply chain attack, malicious or unwitting insider, compromised identity, or any number of other methods, attacks often sidestep perimeter security measures and other defensive controls. Within this worldview, defenders must operate accordingly.[4] The second concept is defense in depth. This practice essentially layers defensive technologies to provide defenders multiple opportunities to detect and respond to threats. If a threat actor is able to breach the perimeter, defenses at the network, endpoint, and identity layers provide additional chances to stop them before they can achieve their objectives.

However useful EINSTEIN was at inception or at its peak efficacy, its value has eroded over time. Mobile devices, remote work, cloud applications, and other changes in the IT landscape have dissolved the perimeter, even as the increased use of encryption has complicated detection of malicious traffic at the perimeter layer. Further, threat actors have become more adept in recent years at targeting endpoints, users, and identities directly. As a result, the security community—including Government agencies and the White House [5]—have embraced concepts like Zero Trust, which essentially disavows the defensibility of the perimeter. While it's reasonable to maintain perimeter defenses as part of a layered security architecture for the ".gov," it's also reasonable to consider EINSTEIN a legacy technology and to focus investments elsewhere.

Continuing Diagnostics and Mitigation (CDM). By 2012, DHS had established a complementary, broader program called CDM. Rather than applying a uniform suite of protections across the ".gov," CDM would offer a flexible portfolio of technologies to defend Federal networks. The program would deliver new capabilities in four phases: Asset Management; Identity and Access Management; Network Security Management; and Data Protection Management.[6] A unifying requirement for tools acquired under the program is the ability to offer visibility through an integrated agency-level dashboard, as well as an aggregated Federal-level dashboard.

Despite modest progress in early years, CISA officials report rapidly-accelerating progress over the past few years. According to a recent CISA blog, "CDM is no longer a static effort to standardize agency capabilities and collect cybersecurity information, but rather the U.S. government's cornerstone for proactive, coordinated, and agile cyber defense of the Federal enterprise."[7] The post further credits Execu-

---

[2] For brevity, I have not described broader Federal cybersecurity initiatives like Trusted Internet Connection program (2007), the Comprehensive National Cybersecurity Initiative (2009), FedRAMP (2011), the Federal Information Security Modernization Act (2014), or the Federal Information Technology Acquisition Reform Act (2014), but I would like to acknowledge their contributions to the Federal cybersecurity infrastructure that exists today.

[3] See *National Cybersecurity Protection System,* CISA. *https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system.*

[4] This assumption leads to the imperative to hunt, described below.

[5] See Executive Order 14028, Improving the Nation's Cybersecurity, The White House. *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.*

[6] See CDM Program Overview, CISA. *https://www.cisa.gov/sites/default/files/publications/2020%252009%252003__CDM%2520Program%2520Overview__Fact%2520Sheet.pdf.*

[7] See *Evolving CDM to Transform Government Cybersecurity Operations and Enable CISA's Approach to Interactive Cyber Defense,* CISA. July 23, 2023. *https://www.cisa.gov/news-events/news/evolving-cdm-transform-government-cybersecurity-operations-and-enable-cisas-approach-interactive.*

tive Order 14028 with strengthening the program's operational visibility, which highlights the addition of the Endpoint Detection and Response (EDR) program to CDM (explained in more detail, below). Further progress is possible with the extension of EDR to cloud workloads and mobile devices.

RECENT POLICY DEVELOPMENTS

While the current major Federal cybersecurity programs administered by CISA are now 10–15 years old, Federal IT policy has accelerated. Stakeholders have made significant progress in the past few years, best illustrated by three key developments.

Threat-Hunting Authorities. A central insight from the influential, bipartisan Cyberspace Solarium Commission Report of March 2020 was recommendation 1.4, which highlighted the need for CISA to perform continuous threat hunting across the ".gov."[8] Pub. L. 116–283, the fiscal year 2021 National Defense Authorization Act (NDAA) Section 1705 granted CISA this authority, which positions the agency to act as the operational defender of the Federal Government.[9]

Executive Order (E.O. 14028). The May 2021 Executive Order on Improving the Nation's Cybersecurity advanced a suite of measures to further bolster security of the ".gov." Key among them were requirements to:

- Deploy Endpoint Detection and Response (EDR) capabilities, which among other things serve as the foundational enterprise cybersecurity technology for threat hunting;
- Implement Zero Trust Architectures, as well as generally accelerate cloud and Software-as-a-Service (SaaS) utilization;
- Standardize incident response practices; and
- Maintain more robust and consistent logging, which supports investigations and remediations.[10]

Federal Zero Trust Strategy. In January 2022, fulfilling a requirement from E.O. 14028, the White House Office of Management and Budget (OMB) issued a strategy for implementing Zero Trust across the ".gov." The memorandum identified specific outcomes and objectives that agencies must achieve over the coming years. This strategy serves a key roadmap that aligns industry and agency efforts over what will be a complex, multi-year process.[11]

FORTHCOMING PROGRAMMATIC DEVELOPMENTS

Budget request documents released over the past year foreshadow perhaps the most significant shift in the Federal cybersecurity program space since the advent of CDM. Specifically, CISA is in the midst of creating two new, closely-linked programs which will absorb elements of NCPS.[12] First, according to these documents, CISA will create a program called the Joint Collaborative Environment (JCE). At a high-level, JCE would split the NCPS program into two components. The first is EINSTEIN capabilities (i.e., perimeter defense), which would be maintained as legacy technology under JCE.

The second component of JCE is much broader—and is itself a meaningful new program—called Cyber Analytics and Data System (CADS). A summary document for the fiscal year 2024 President's Budget Request describes CADS as "a system of systems[] that will provide a robust and scalable analytic environment capable of integrating mission visibility data sets and providing visualization tools and ad-

---

[8] See *Cyberspace Solarium Commission Report,* March 2020. *https://www.solarium.gov/report,* p. 41.

[9] See *NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission,* Sen. Angus King, January 2, 2021. *https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-solarium-commission;* and *The National Defense Authorization Act for Fiscal Year 2021, https://www.Congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf,* p. 695.

[10] See *Executive Order on Improving the Nation's Cybersecurity,* The White House, May 12, 2021. *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*.

[11] See Memorandum 22–09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,* Executive Office of the President, January 26, 2022. *https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.*

[12] This narrative draws on program descriptions within *CISA Budget Overview for Fiscal Year 2024 Congressional Justification. https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20SECURITY%20AGENCY.pdf.* See also *CISA Strategic Plan fiscal year 2024–2026. https://www.cisa.gov/sites/default/files/2023-08/FY2024-2026_Cybersecurity_Strategic_Plan.pdf.* For consistency, I have focused on characterizations from the President's Budget Request rather than from more recent but yet-to-be-finalized House and Senate Appropriations documents.

vanced analytic capabilities to CISA's cyber operators."[13] CADS would absorb the remaining analytic capabilities from the NCPS program, serve as the hub for Cyber Incident Reporting for the Critical Infrastructure Act of 2022 (CIRCIA) analytics, and support a number of other data-intensive operational activities.

NEXT STEPS IN FEDERAL CYBERSECURITY

A core principle in cybersecurity is that the defender must have visibility into security-relevant events of the systems they defend. Today, this includes the endpoint, cloud, and identity planes in addition to the traditional network. Although stakeholders have made significant progress on Federal cybersecurity over the past few years in enhancing this visibility and control, several points stand out as next steps to further strengthen the security posture of the ".gov."

JCE and CADS implementation. Clearly, the JCE and CADS efforts described above will require a significant investment of time and resources. Federal cybersecurity programs historically have a long "shelf-life," and strengths and weaknesses can both compound over time. This underscores two key, future-oriented considerations:

- It's important to design these programs to enable flexibility. Changes in the IT or threat environment over time may precipitate the need to reallocate resources between program areas or initiatives.
- CADS in particular should be built for scale. The processing of data for cybersecurity purposes increased exponentially during the transition from the legacy antivirus age to the current EDR age. This trend could continue for some time, particularly as cloud workloads swell, log retention expectations increase, and adversaries and defenders alike seek to leverage Artificial Intelligence (AI). CISA must build CADS data processing capabilities that can perhaps double (or more) year over year for the foreseeable future.

CDM modernization and sustainment. With the realignment in NCPS described above, CDM will in a sense become the "mature" Government cybersecurity program. This raises the question: at what point might CDM itself need to be modernized? From an operational standpoint, the EDR program has clearly breathed new life into CDM, so perhaps this is a question that can be resolved in the future. Nevertheless, when the time comes, stakeholders should consider two questions:

- While some EDR technologies were available through CDM prior to E.O. 14028, it ultimately required a mandate from the White House to deploy this essential technology across the ".gov." Cybersecurity professionals within CISA understood the importance of EDR, and it was clear that EDR would support CISA's hunting mandate. But CDM still works on the model of a catalog. In the future, is there scope for CISA to more proactively enforce the use of CDM technologies to fulfill its mission?
- Although, as noted above, EINSTEIN's operational capabilities have aged poorly, the NCPS program's architecture has aged like a fine wine. Specifically, it worked on a shared services model, meaning agencies got the benefit of EINSTEIN protections without complex budgeting or cost-sharing processes. With respect to the CDM program and associated funding, Federal CISOs still sometimes hesitate to acquire new technologies, given a real or perceived uncertainty about cost-sharing with CISA over time. In the future, is there scope to adapt CDM, or elements thereof (e.g., EDR), to operate more directly as a shared service, where CISA funds the program for users directly?

Emerging cybersecurity capabilities. The cybersecurity industry is evolving at an uncharacteristically rapid rate. So over the next few years, the conversation within the Federal cybersecurity community will shift to new priorities. A few emerging areas to monitor, and further integrate into Federal defenses as appropriate, include:

- *Extended Detection and Response (XDR).* Mature security programs within the private sector are already augmenting EDR to attain detection and response capabilities at other layers of the enterprise security stack. XDR enables visibility and control over network and identity (described below) data; the aggregation of logs; and the integration of threat intelligence within a unified workflow.
- *Identity Threat Detection and Response.* As security practitioners increasingly confront risks from IT ecosystem monoculture specifically, and identity-based attacks generally, there's greater interest in defending enterprises at the identity layer. This emphasis comports nicely with broader Federal Zero Trust adoption efforts.

---

[13] See *Department of Homeland Security Fiscal Year 2024 Budget in Brief. https://www.dhs.gov/sites/default/files/2023__03/DHS%20FY%202024%20BUDGET%20IN%20-BRIEF%20%28BIB%29__Remediated.pdf,* p. 4.

- *Artificial Intelligence (AI).* While the application of AI to cybersecurity is not new, it is advancing. Although already resident within leading endpoint security tools, multiple other cybersecurity technologies will integrate AI and new AI-based capabilities will emerge over the coming years. This will drive speed, efficiency, and even make some tools more accessible through the integration of a natural language interface.[14] To the extent possible, Federal cybersecurity executives should view this opportunity holistically, consult broadly with industry and academia, and engage in long-term planning.
- *Managed Security Services.* Enterprises—even very large ones—increasingly leverage commercial managed security solutions. Defenders should be prepared to respond to and remediate cyber threats 24x7x365, and not all entities are able to build programs that can match the agility of dedicated commercial offerings. On the other hand, internal IT and security staff, by virtue of their trust and familiarity with the organization's mission space and constraints, are uniquely positioned to develop processes, address risks, and otherwise strengthen security maturity. So unburdening these internal operators from tactical demands on their time pays enormous dividends. This opportunity clearly applies in aspects of the Federal IT ecosystem.

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

Chairman GARBARINO. Thank you, Mr. Sheldon. Members will be recognized by order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized. I really do appreciate the participation, though, of my colleagues for being here today. This is a dense topic, but it is a very important one. So, I do appreciate you all being here, especially considering CISA right now is under attack from some of our colleagues, ranging from proposed defunding of salaries to up to a 25 percent cut of their budget, something that I think after today's testimony from our witnesses, people will understand how important CISA is and that the focus needs to be on defense, especially when it comes to cybersecurity.

So, I now recognize myself for 5 minutes of opening questions. Mr. Gumbel, for a long time, agencies have been required to maintain asset inventories. The base layer of CDM was meant to help this. You can't defend what you can't see. But even with a requirement in FISMA and tools in CDM meant to help identify and manage assets, agencies consistently struggle to accurately and continuously maintain asset inventories. CISA even put out a binding operational directive at the beginning of this fiscal year, again directing agencies to better manage their assets. What more can the CDM program do to help agencies get this right?

Mr. GUMBEL. Sure. Mr. Chairman, thank you for this question. I think there's a lot that they can do to help get this right. I think some of our recommendations are we need to create a more transparent and collaborative technology assessment process. We also need to, and I think we all can be aware of this, that the procurement process within Federal Government is not the easiest to get through, and it also excludes some of the newer technology, cloud-based technologies, and it's more leaning toward and geared toward legacy technologies. So, I think improvements there within procurement can absolutely help out.

There's also a lot that can be learned from the private sector. The private sector has done incredible advancements around cloud-based technologies, around end-to-end solutions that offer full visi-

[14] See, for example, *Charlotte AI: Accelerate Cybersecurity with Generative AI Workflows CrowdStrike. https://www.crowdstrike.com/products/charlotte-ai/.*

bility into unmanaged devices. I submitted in my written testimony a bar chart that showed the explosion of unmanaged devices. Those devices, meaning the ones that you can't see traditionally, IP cameras, HVAC systems, building management systems, and printers, those things need to be looked at when we are looking at securing the American public.

Chairman GARBARINO. Thank you very much. I have heard from many companies that some of our best technologies are being kept out because of the procurement process right now.

So, something we should work on. Mr. Zakowicz, NCPS has traditionally structured as a true shared service with CISA providing and covering the cost of operation. Whereas CISA provides funding and tools for CDM for the first 2 years, with agencies expected to carry on funding after that. Are there changes that would help improve agency adoption of CDM tools? What role does centralized funding play in that?

Mr. ZAKOWICZ. Thank you for the question. As I mentioned in my opening remarks, the funding associated with progress on CDM is not just in the hands of CISA. It's also in the hands of the agencies who have their own mission priorities and focus that they need to balance against the priorities that CISA provides and their own security. I think that one case study under the CDM program that we've seen under the shared services model is that unlike the 2-year funding model that you referenced, that shared services model does provide those services in perpetuity to those smaller agencies and organizations as long as they're using that standardized set of capabilities that are provided to those agencies.

That model is not going to work for the largest, most complex federated agencies out there. They are going to have their unique requirements that won't necessarily allow them to take on a shared services approach. But there are a lot of agencies that currently don't qualify for the shared services program that could take advantage of those and that would allow centralized funding. It would allow reduction in total operating costs due to the purchasing power of that shared services platform, and could ultimately provide some additional benefit.

Chairman GARBARINO. Are there risks introduced by moving toward a true shared services model that increases interdependencies and thus increases the potential for cascading vulnerabilities across agencies?

Mr. ZAKOWICZ. So, I think the risks associated with moving to a shared services model generally, you know, come from an agency perspective around the lack of control in the solution, which can be a risk and a benefit depending on what your IT resources look like. The current shared service model under CDM provides multiple options of any given tool or capability, at least two, so that agencies can pick which one is best suited to their needs. Then it also provides additional watch capabilities so that there's a central organization within CISA keeping an eye on what alerts, what monitoring activities are occurring under those tools, and provides a, you know, checks-and-balances process to then notify those agencies when issues are identified.

Chairman GARBARINO. Thank you. Mr. Head, as the head of your company, both CDM and NCPS—he made me do that, by the

way—both CDM and NCPS are critical parts of Federal civilian cyber defense. It seems to me that these two programs, which ultimately are about visibility and continuous monitoring, should work better together. How should CISA be thinking about getting these programs to work better together?

Mr. HEAD. I think if we start with the basics of the roles when we consider the options, you know, what data do I need to see what I need to see? One of the panel members makes a product that says here's your inventory all that stuff on your network. I think we also need to look at role. One of the things I like to look at is, you know, is your printer a bank teller? Is your printer an engineer? If not, why is it accessing customer records? So, when you start looking at things that shouldn't happen the way they are happening, you've got to answer the question, if I have a tool and I choose to make it proactive and to block and, I mean, do we want to spend our whole time analyzing or reporting on how we got eaten? Or do we want to flip the tables and say, no, we stopped this cold and they won't come after us again?

I think a piece of that is you got to do to them what they just did to you. So, you know, we need to have some law changes in terms of punitive damages as well as unleash the military guys to have fun. So, whatever they do to us, we need to do them 10 times until they quit. This is terrible.

Chairman GARBARINO. Thank you very much. I now recognize Ranking Member Menendez for 5 minutes for any questions he may have.

Mr. MENENDEZ. Thank you, Chairman. Government funding is set to expire in just 11 days, creating a dangerous risk of a Government shutdown. Even in a best-case scenario where we keep the Government open, we will have a continuing resolution with no sign of a bipartisan full year appropriations bill in sight. This question is for all of you. What do you see as the main impacts a Government shutdown could have on the ability of CISA to defend networks? We will start with you, Mr. Gumbel.

Mr. GUMBEL. I think the shutdown will obviously cause delays and some cyber projects will come to a halt. The longer we delay, the longer the adversaries will have the chance to get in front of us. So, delays are just terrible for this Nation and it is going to cause some major impact.

Mr. MENENDEZ. Thank you.

Mr. ZAKOWICZ. Thanks. So, having done this for 4 years, I've lived through a couple of, you know, Government shutdowns and the impacts, I think really day-to-day operationally are ones of continuity and ones of resource availability. So, what are we able to do, what are we able to make progress on? Ultimately, what tradeoffs are each one of those agencies making as they're, you know, facing the questions of what, you know, resources are they going to have left, how are they going to keep the doors open? That does have an impact, not just on, you know, that shutdown in the moment, but also continuity, planning, and forward progress in some of these initiatives.

Mr. MENENDEZ. Thank you. Mr. Head.

Mr. HEAD. As I mentioned before, the big programs under a CR continue at the previous funding levels, or 80 percent. The thing

that just hits you the hardest is the new initiatives just get stopped completely and we need a lot of innovation in the cybers. So, I think you all need a way to fund during a CR, especially new programs and reactive breach responses. That's sadly lacking across the table and it is sort-of disheartening to the guys that are burning 20-hour days to do the work across all the agencies.

Mr. MENENDEZ. Just to quickly follow up on that, you mentioned the new initiatives. New initiatives are to match the evolving threat environment, correct?

Mr. HEAD. Correct.

Mr. MENENDEZ. So when we are not implementing that, we are not only not keeping up, but we are falling behind in a relatively quick fashion.

Mr. HEAD. Yes.

Mr. MENENDEZ. Thank you. Mr. Sheldon.

Mr. HEAD. You can't start a new effort under a CR, but you can continue an old one. This is all new. It's new every day with a new breach, new zero day, new attack.

Mr. MENENDEZ. I appreciate that. Mr. Sheldon.

Mr. SHELDON. Thank you. You don't get to have good cybersecurity outcomes if you don't have continuity in your cybersecurity programs. The absence of funding could disrupt that.

Mr. MENENDEZ. Thank you. Mr. Gumbel, just to come back to you to sort-of follow up on the point Mr. Head just made. How would a year-long continuing resolution that locks in last year's budget impact the ability of CISA to innovate to match the current threat environment?

Mr. GUMBEL. I'm sorry. Could you repeat that?

Mr. MENENDEZ. Sure. How would a year-long continuing resolution that locks in last year's budget impact the ability of CISA to innovate to match the current threat environment?

Mr. GUMBEL. My view is that we need to obviously match what CISA is doing in order to progress some of the changes in the systems that we're looking to put forth. So, I think it is a big concern.

Mr. MENENDEZ. Thank you. The current CDM program monitors traditional IT assets across Federal agencies. However, the attack surface is growing to include internet of things, devices, and threats to operational technology. As CDM continues to modernize, including all assets will be an important part of the program's maturation. Mr. Gumbel, can you elaborate on why you think including internet of things and operational technology assets in the CDM program is so important?

Mr. GUMBEL. The reason why it's so important is that only 10 percent of networks have managed devices on them. The other 90 percent are unmanaged devices. As you mentioned, Mr. Chairman, you can't protect what you can't see. All of these other devices are out there and they are invisible unless there's modern technology, there's cloud-based technologies, and there's ways in which you can view these assets. Without being able to view these assets, these are vectors for the adversaries to be able to get in and to be able to compromise our environments.

Mr. MENENDEZ. Great.

Mr. GUMBEL. So, it's a real big threat.

Mr. MENENDEZ. A quick follow-up to that you mentioned you can't protect what you can't see. How should CISA go about expanding its visibility into those devices?

Mr. GUMBEL. I think how they go about it is to allow modern companies to be able to bid when there's new contracts that come out. I think they have to evolve from legacy companies that have on premise solutions, allow cloud-based technologies to come in and provide a holistic view. I think the other thing that they can do is start looking at commonality between different leadership groups within organizations. Right now, you have some groups that you have just visibility into OT or IT. You have some that are focused just on IOT. There needs to be a conversion to leadership across all Federal agencies so that there's a holistic view of what's being managed and what's being unmanaged.

Mr. MENENDEZ. I appreciate that. Probably all of us on this subcommittee have had local governments in our district hit by ransomware attacks and other cyber incidents that have denied constituents access to vital Government services. One way to help State and local governments is to provide them expanded access to CDM services. We will ask you to keep this brief because I am over. Mr. Zakowicz and Mr. Sheldon, how should CISA enable expanded CDM shared services to State and local governments?

Mr. ZAKOWICZ. I think they've got a good blueprint to follow in the shared services capability they've already offered to the Federal entities. As you can imagine, the cyber maturity of agencies across our FCEB can, in a lot of ways, mirror the relative maturity of State and local critical infrastructure stakeholders where some are very well-resourced and others are not. So, I think there's a lot of learnings from that rollout of shared services that could be directly applied to State, local, Tribal, territorial, and critical infrastructure.

Mr. SHELDON. Thank you. There are some lessons for sure that State and local entities can take from Federal Government programs like CDM. There are also, frankly, some lessons that the Federal Government can take from State and local entities that kind of more organically operate on shared services models in some instances.

Mr. MENENDEZ. Thank you.

Chairman GARBARINO. I now recognize the gentleman from Florida, Mr. Gimenez, for 5 minutes.

Mr. GIMENEZ. Thank you, Mr. Chairman. Mr. Head, I was listening to your testimony, and it struck me, were you saying basically that the United States' cybersecurity efforts are mainly, if not exclusively, defensive in nature?

Mr. HEAD. I would say that we are reactive defensive in that we are not taking actions to stop it before it happens. You know, and I think, there's, obviously, there's a difference between the offensive side and the defensive side. So, the military guys have offensive capabilities that they hold in reserve and that'll work independent. But my comment was more on the side of don't just wait until something happens and develop a process to know about it and report it sooner. Work on the technologies that stop the attack in the first place.

Mr. GIMENEZ. But I think you also said that our cybersecurity threats, they kind-of operate with impunity. They know that nothing's ever going to happen to them.

Mr. HEAD. Correct.

Mr. GIMENEZ. Which means that they are not afraid of any offensive capability that their target may possess.

Mr. HEAD. That's correct.

Mr. GIMENEZ. Is that because is it illegal for us or a company to conduct offensive——

Mr. HEAD. I think there's——

Mr. GIMENEZ [continuing]. Or retaliatory operations against somebody who just attacked their network, et cetera, or what is that?

Mr. HEAD. I think there's many levels to that. I've been asked several times about, should we take off the gloves and let people that are hit, hit back? I'm not a big fan of that approach because you could end up starting a nuclear war just by, you know, doing something crazy. So, I don't think we want to go vigilante, but I do think we need better clarity.

When I first started looking at this a decade ago, we had a guy that had a bunch of documents stolen, and he put scripts in his documents so that when they got to wherever they were going to, they would call him and let him know where they ended up. They arrested him for operating shell scripts on a computer without permission. That's crazy. So, being able to trace. We need to clarify——

Mr. GIMENEZ. Was that illegal?

Mr. HEAD. Yes.

Mr. GIMENEZ. It was illegal.

Mr. HEAD. He didn't have permission from the guy that attacked him to run scripts on the attacker's computer. So, he included executable files in what was stolen, and he was arrested for that. So, there's a little bit of crack-smoking that goes on in the legal world that we need to fix.

Mr. GIMENEZ. All right. So, somebody attacked him.

Mr. HEAD. Yes.

Mr. GIMENEZ. And he put something in there to make sure that he could find out who it was that attacked him?

Mr. HEAD. Correct. They arrested him.

Mr. GIMENEZ. Then the person that attacked him said, hey, you couldn't do that to me even though I attacked you first, and therefore, the guy that was attacked was the one ultimately jailed?

Mr. HEAD. Yes.

Mr. GIMENEZ. That sounds logical.

Mr. HEAD. You don't have to look far for comedy in the cyber space. But I'm just saying, you know, you guys are really good about—a lot of us that have been in the defensive world forever we try to figure out how to operate within the laws and make it better. The reason I'm here is it suddenly dawned on me, a year or so, just change the law. Let's get rid of the crazy. It helps.

Mr. GIMENEZ. I guess that is what I was trying to get to, that there may be laws that are actually hindering our ability to defend ourselves and maybe, look, I have no problem hitting back every once in a while, OK?

Mr. HEAD. Absolutely.

Mr. GIMENEZ. All right. Because then you should have as an attacker, you need to be fearful of what could happen to you, depending on who you attacked. I mean, can you imagine if we had after Pearl Harbor, we just said, well, I guess we will just wait for the next attack, OK. We are not going to take any offensive capabilities. Or in Europe, well, you know, we are just going to stay here in England, and we were not going to do D-Day because, you know, we are just going to defend ourselves. I don't think you could win too many wars that way. So, I find that very interesting.

I don't know who can answer this, but artificial intelligence. If somebody can put out a crystal, you know, get a crystal ball and say, OK, what will artificial intelligence do in this realm, offensively and defensively? What do you all see?

Mr. SHELDON. I could take a stab at that. Thank you, sir. So, artificial intelligence has made a lot of news recently because there's greater access to some consumer products that make LLMs, especially large language models, available for experimentation. But really, artificial intelligence and cybersecurity is not all that new.

My company, for example, has had artificial intelligence and machine learning embedded in it at scale, deployed out across tens of millions of endpoints for the better part of 10 years. That really drives some of our ability to identify and stop even very novel threats, attacks that haven't been seen before. So, there's a lot of ways in which defenders already are using AI and that is poised to continue as AI gets integrated into other product areas. So, it is a very exciting time from the standpoint of what the defenders are able to do.

On the other hand, it's also the case that adversaries and different threat actors are experimenting with large language models and other forms of AI. It's something that us in the defense community need to look out for. It may be the case that there's some more developments in that over the next coming months because there are broader access to some of these tools now than there have been over some time. So, it's something that merits watching.

Mr. GIMENEZ. Thank you. I guess my time is up. I yield back.

Chairman GARBARINO. The gentleman yields back. I now recognize the gentleman from Louisiana, Mr. Carter, for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman. Thank you all for being here. In 2021, President Biden issued Executive Order 14028, which imposed a host of new mandates on agencies to strengthen the Federal Government's cybersecurity. One positive result of this order was a deployment of endpoint detection and response technologies across Federal agencies as a part of the CDM program. With that Executive Order now already 2 years old, the technological environment continues to evolve with advances that constantly test our defenses. For all of the witnesses, as we seek to constantly evolve the CDM program to stay ahead of our adversaries, what technologies and cyber defense practices do you think are most urgently needed to be deployed at Federal agencies based on today's ever-moving threat?

Mr. GUMBEL. Thank you, Congressman. For Armis, we view the only way for pure protection across all agencies is ubiquity and that view to have 100 percent visibility into all assets. Whether

those assets be IT OT, IOT, or IOMT, it is critical that you have visibility into the unmanaged devices within an environment in order to provide that holistic view. Otherwise, you're at risk of adversaries getting one step ahead of the game and being able to infiltrate a network.

Mr. CARTER. Thank you.

Mr. ZAKOWICZ. I agree with the answer. I would say at least with my experience on the CDM program, that yes, historically the focus has been on IT-managed assets. They have done some work associated with operational technology, mobile assets, cloud assets, and I think that needs to be prioritized and accelerated to be able to get that complete view that my colleague's referencing.

Mr. HEAD. I think one aspect that is worth saying is when you look at endpoint protection, there's some really good stuff. We use theirs and love it. But what you want to do is instrument a network in such a way that how do you know when you've been blindsided. So, I think, you know, if you look at IOT devices, there's not going to be endpoint software, you know, on a watch, or on a firmware device, or a lot of IOT things, door alarms, so on. So, you're going to have to have network-based things that look to see if those are acting in ways they shouldn't.

So, you want a layered defense. People talk about that all the time, but when it comes to implementing it, we do sort-of light beer when you're ready for full-bodied. So, we need to really look at a more defense-in-depth with a lot more visibility.

Mr. SHELDON. Thank you. I'd say there's still some progress that can be made within the EDR program itself by way of deploying it out to cloud environments, mobile devices, and the like, just to make sure that you have the same level of visibility control on those types of assets. Then beyond that, really thinking about a concept that the industry calls extended detection and response, which is the same idea of bringing that visibility and control out to other parts of the network security stack. So, making sure that you can get integrated workflows with data not just from the endpoint but also from the network, or from the perimeter, or being able to integrate logs, being able to integrate threat intelligence and similar things then giving people more coherent set of a control plain for being able to do the work that they do from a defensive standpoint.

Mr. CARTER. Mr. Sheldon, in your earlier testimony you discussed the need for CISA's proposed cyber analytics and data systems to be built to scale. I agree on the need to ensure that CADS has the capacity to process significant increases in data we can expect CISA to receive in the upcoming years. How can CISA ensure that it deploys the new program in a way that is flexible enough to handle future demands?

Mr. SHELDON. Thank you, Congressman. This, I think, is probably one of the more interesting questions that CISA has to grapple with today. I think an interesting stress test for whatever plans they've developed for the CADS program is to think about, you know, would this work if we needed to—whatever our sort-of best guess is, or our assumption about how much data we need to be able to process in that environment, would it be able to handle twice that, and then would it be able to handle twice that again?

Doing some of those sort-of stress tests would, I think, position them well to understand whether they're developing architectures that can scale to the level that they will need to if they are doing more types of data-intensive programs across the Federal Government.

For our case, we have 2 trillion events per day or more that we stream up to our cloud. So that's the type of big data that——

Mr. CARTER. I got 3 seconds. Let me just cut you off a second. I want to ask Mr. Gumbel, given where we are and the threat as they evolve, and the pace at which technology is moving, if you had a silver bullet that you can use with this committee or with Federal Government, what would that be to make sure that we are staying abreast and ahead of the bad actors?

Mr. GUMBEL. I want to repeat this again, but I do believe the silver bullet is to have end-to-end security for visibility for all of your assets. That's the only way to get full visibility and protection across your enterprise. To take a step further, is once you can identify those assets, understand where those vulnerabilities lie, and then take action upon those vulnerabilities to protect your environment holistically.

Mr. CARTER. How complex is it to do that and how long does it take?

Mr. GUMBEL. It is not that complex at all. We have organizations that, at scale, have rolled out tens of millions of endpoints in weeks. This is something that we can partner with the Federal Government to achieve.

Mr. CARTER. Thank you, Mr. Chairman. I yield back.

Chairman GARBARINO. The gentleman yields back. I now recognize the gentlelady from Florida, Ms. Lee, for 5 minutes.

Ms. LEE. Thank you, Mr. Chairman. Mr. Gumbel, I would like to pick up right where we left off there. You have given us some very useful information today about our general status at this point that we have done a lot of work on endpoint detection, but as the attack surface continues to grow, so do our defenses and our preparation need to evolve. I am interested in what capabilities we need to be integrating into CADS to improve analytics and increase visibility, as you have been testifying about. Specifically, do we need to pay particular attention to the concept of encrypted communication? Are we capturing that now? Is there anything we need to be doing in that space?

Mr. GUMBEL. Sure. So, that was a lot to unpack. But I believe that, Congresswoman, the thing that we still need to do once you have the holistic view of an entire environment, you have to look at other vectors too. You bring up encryption, encryption is definitely of utmost importance and making sure that the encryption standards that the Federal Government holds across all agencies are kept up to date.

You also have to make sure that you're looking at legacy providers and technologies that have been built 10, 20 years ago. Are they really up-to-date? Are they really current today if they are not modern in their approach? Because the adversaries are going to come forth with something new and they are going to bypass and get past those networks that are being defended today by legacy

contracts. So, I think all of that needs to be taken into consideration.

Ms. LEE. OK. Mr. Zakowicz, you indicated earlier on the subject of hunt and incident response through CDM that you thought we might need to look at changes in Congressional authority in order to be really utilizing that as part of our approach. Would you tell us a little bit more about that?

Mr. ZAKOWICZ. Sure. Thank you. So, there were two authorities granted within the Executive Order that I think were directly relevant to the CDM program's ability to gain insight and access into agency network environments like they hadn't been able to before. The first was associated with endpoint detection and response, or EDR, hunt and response activities. It's being done through an initiative granting threat hunters access to agency EDR tooling through what's called persistent access or pack capabilities. So, that's given them an opportunity to be able to look in those agency environments real time, directly using tools like CrowdStrike and others to understand what's happening in that space.

Then the second is access to what's called object-level data. So, within the agencies, the detailed information on every endpoint that's being collected and rolled up and aggregated into this CDM dashboard having direct access to that object-level data allows them to within minutes search across the Federal enterprise for the presence of, let's say, zero-day vulnerability or known exploitative vulnerability. Identify the potentially vulnerable assets within an agency environment across the FCEB, and then use EDR in partnership with the agency to go further, interrogate that asset and understand what the risk profile really looks like. I think CISA's seen some success with that combination of capabilities with even recent breaches, being able to identify in minutes what may have taken hours or days or longer through data calls.

Ms. LEE. Mr. Head, I would like to hear from you on what capabilities you think CISA should be including in the CADS program to help improve analytics and visibility.

Mr. HEAD. If you look at the detail that I've seen, you know, publicly, they had things like DNS and signatures in there, but they didn't have flow. I think it is really important to be able to see flow in terms of oversight guidance. There's also the notion of how do you know who somebody is? So, on a network, a lot of the privacy concerns have led manufacturers into anonymizing the Mac addresses so that you don't know what the device is anymore. So certainly on Federal Government agency networks, you need to know what things are and they shouldn't be able to do anonymization and hide their activities.

The other piece I would also mention is you get into the details of things like you ask about encryption. The purpose of encryption is to keep somebody from stealing your stuff. But if you're in the business of stealing stuff, encryption is hiding what you're stealing. So, the answer isn't to give everybody the keys, the answer is encompass in your logging what file moved from his machine to my machine. You shouldn't have your audit system be more prone to invasion and privacy concerns than your original network was. So, we can do things like MD5, all of the files as they flow, and say this file was the unreleased this and you sent it to him, why? So,

I think it's possible to build an audit system without breaking the world, but it doesn't do just to start let's opine about things that are impossible. Let's write down methodically things that are easy and very effective.

Ms. LEE. Thank you, Mr. Head. Mr. Chairman, I yield back.

Chairman GARBARINO. Thank you. The gentlelady yields back. I think since everyone is here, I am going to start my second round of questions. I want to start with Mr. Zakowicz. Amidst an increasingly complex threat landscape, technology innovations of the last decade and recommendations for improvements from the GAO and industry stakeholders, the CDM program must evolve to keep pace with the threat and improve Federal cyber defense. Do you envision any gaps in authorities needed to allow CISA to continue to strengthen the Federal Government's information infrastructure?

Mr. ZAKOWICZ. Thank you for the question. I think we've already covered a couple of specific authorities that I think would be beneficial to be codified in order for CISA to continue the mission that they have. I think we've also touched a little bit on I think there was reference in one of the opening statements to CISA's authority to actually conduct testing and verification in agency environments, to run, you know, penetration testing or network testing activities within the individual agency environments. While I'd say personally, I think that, you know, with the responsibility resting with the agencies themselves, that's something that would need careful consideration. I do think continuing to take a look at how actively they are able to engage with agency networks, agency environments, would be worthwhile to understand if that gives them the authorities they need.

Chairman GARBARINO. Thank you very much for that answer. EDR has been rolled out through the CDM program after it was acquired in the May 2021 Cyber EO. A few years ago, CISA was given an authority to proactively hunt for threats on agency networks. Mr. Sheldon, in your testimony you discussed the opportunities for EDR to inform CISA's threat hunting capabilities. How can CISA better leverage EDR data to improve threat hunt efforts?

Mr. SHELDON. Thank you, Mr. Chairman. So, I think CISA is really far ahead of where they were a couple of years ago by virtue of the authorities that I mentioned that were given to them in Section 1705 of the fiscal year 2021 NDAA and then by virtue of having this now-very powerful EDR capability deployed out across many, many Federal agencies. I think the core task now is to ensure that, is it the case that every endpoint that can be protected with that type of capability is. It may be possible for them to think about extending it more over cloud environments and mobile devices, as I mentioned before. Then to think through the next set of problems, which is again, thinking about bringing that same type of control to other parts of the network and then really creating a unified workflow for their analysts to be able to do something productive with that very quickly when there's a threat.

Chairman GARBARINO. Thank you very much. Mr. Head, following up on your response to Ms. Lee before, how can AI be more incorporated into these programs, particularly, as CISA looks to evolve NCPS?

Mr. HEAD. I think in lots of ways. Whenever you're drowning in a sea of big data, like you mentioned, trillions, all of us deal with, you know, tens of trillions of events, you know, on a periodic basis and just slugging through all that with humans just doesn't scale well. So, we all see that as our salvation for doing a thorough job across broad spectrum of assets that need protecting.

I think zooming up a little bit, there's also big data that needs to come to bear outside the—remember the old game where you had to draw lines, three rows of three dots, and you drew your lines? I think a lot of times we are focusing in the box instead of outside. So inside, we are not spending much time to do surveys of what isn't covered and in that you can drive a sinking country through. So, I think we need to kind-of look at what are we missing as a paid research project for somebody.

Chairman GARBARINO. I am not sure how often we think outside the box when it comes to the Government. I only have a little time left. But I said at the beginning of this hearing, we are doing this to talk about the two programs, NCPS and CDM. And we are going to have Government witnesses, one from CISA, someone from somewhere else. This is for all of you and feel free to jump in. What should we be asking them at the next hearing when we have them in front of us specifically about these programs? We can start with Mr. Gumbel, and we can move down the aisle if you want.

Mr. GUMBEL. I think one of the biggest questions, Mr. Chairman, is ask them have they looked at modern technologies or are they only focusing on the contracts that they have with legacy providers that have built technologies 20 years ago? Those technologies that are either on premise, they're not cloud first, there are older ways in their thinking in the way that they protect networks and connect infrastructures. So, I'd say that would be the first thing that I would ask.

Chairman GARBARINO. Mr. Zakowicz.

Mr. ZAKOWICZ. Thank you. So, I would suggest focusing on, you know, across our national security, our economic security, where are the threats? Because I think they certainly exist within the Federal Executive branch, but they also exist outside of the Federal Executive branch. I think as CISA looks at applying their resources, their time, their focus, you know, is it internal to Federal? Is it external to State, local, Tribal, critical infrastructure? Where do we get the most benefit in our improving our security's posture?

Chairman GARBARINO. Thanks. Mr. Head.

Mr. HEAD. I'd ask about how will they map what they're doing to the threat landscape? So, how are you going to stop these things with what you're doing? That gets down to the next level into what are you logging? What are you keeping? What can you see? What can you not see? When do you plan on doing that? You know, I've joked that, you know, there used to be a cartoon with the cat and the mouse, and the mouse would run through the garden hose and there'd be a big lump that was mouse size running through the hose. We don't see our secrets leaving out our ethernet cables like watermelons flowing. So, I think just the simple visibility of have they stolen us blind? Do we have any national secrets left? You know, the cables don't get hot and glow and melt, you know, as they're stealing our stuff. So, I'd look at CISA's programs and say,

what are you doing that'll let us see an OPM breach instantly instead of finding it a year later? I found that one myself, you know, looking at data. So, the question is, how is what you're doing going to help that?

Chairman GARBARINO. Mr. Sheldon.

Mr. SHELDON. Thank you. I think it's worth asking CISA if they've seen incidents or other issues on Federal networks that would be protected by technologies that exist within the CDM portfolio and the agency in question hadn't used those technologies than to just try and interrogate where was the disconnect? So, I think some of us have spoken about this today. It may be the case that there's an opportunity to clarify some of the longer-term funding for some of the CDM projects and to make that more consistent and then to really shift that program so it's operating more on that shared service type of basis that you had with NCPS and EINSTEIN. That may resolve some of the issues. There could be others, but it'd be interesting to hear about it.

Chairman GARBARINO. Thank you very much. I now recognize Mr. Menendez for 5 minutes for any questions he may have.

Mr. MENENDEZ. Thank you, Chairman. Thanks to progress made by the Biden administration and support from Congress, CDM has made important strides in recent years and has helped CISA more quickly respond to cyber incidents. Mr. Sheldon and Mr. Gumbel, are there recent examples you are aware of where CDM has helped CISA with incident response or the mitigation of vulnerabilities? What aspects of CDM have been most helpful with strengthening Federal cybersecurity? We will start with you, Mr. Gumbel.

Mr. GUMBEL. I'd actually really like to take this one for the record and get back to you with a thorough answer because I'm currently not aware of anything that's been that beneficial that I could speak to.

Mr. MENENDEZ. I respect that.

Mr. GUMBEL. OK.

[The information follows:]

In response to Ranking Member Menendez's question about examples of where the CDM program has been most beneficial and helped response and mitigation of cyber incidents, we submit the following:

CDM has brought value to small and micro agencies and driven the implementation of new technologies into Federal IT programs. Agencies are better equipped to manage privileged accounts because of the identity efforts leading to more resilient and secure critical citizen services. EDR deployments likewise have been largely successful.

However, our overall assessment of the core CDM efforts is not positive. Many of the original goals of CDM have been achieved and much of the deployment is secondary rather than integrated to agency operations.

The CDM program however relies on a legacy model and approach, and it is our hope that a more open, full-industry approach can help CISA achieve its original CDM mission of: Reducing agency threat surface, increasing visibility into the Federal cybersecurity posture, improving Federal cybersecurity response capabilities, and Streamlining Federal Information Security Modernization Act (FISMA) reporting.

Mr. MENENDEZ. Mr. Sheldon.

Mr. SHELDON. I'll just say briefly that it's sometimes the case that, you know, even we as vendors don't get perfect visibility on how, you know, how particular investigations have unfolded. There may be some good reasons for that from an operational security standpoint, just, you know, people in CISA who are working on dif-

ferent projects, issues, responding to incidents, they'll be in touch from time to time.

The part about this that I do think is helpful and is clarifying is reporting that we will ultimately get from the CSRB, the Cyber Safety Review Board, and they've announced an investigation recently where they were going to look at the July breach of the Microsoft 365 platform that led to the ability of Chinese threat actors to read the email of two Cabinet Secretaries. It'll be interesting to get ultimately a reconciled view from different vendors, from Government agencies that have responded, and from other people out in the security research community about what precisely happened. That's a very useful thing for people to know so that we can learn and integrate lessons as appropriate.

Mr. MENENDEZ. I appreciate it. I just want to give you both a chance on the second part. What aspects of CDM have been most helpful with strengthening Federal cybersecurity? If you'd like to respond.

Mr. SHELDON. I'm sorry, could you say that again?

Mr. MENENDEZ. Sure. What aspects of CDM have been most helpful with strengthening Federal cybersecurity?

Mr. SHELDON. I think we've all mentioned EDR and highlighted that. So, at the risk of beating a dead horse, obviously it's a powerful capability. I think the design of CDM was to make available a portfolio of technologies so that if particular Government agencies had very specific needs, there might be something there that would be able to meet that need. So, it may well differ from agency to agency about what, on top of something like EDR, drives the most value.

Mr. MENENDEZ. I appreciate it. One challenge for Federal agencies is that many rely on outdated technology that is harder to secure. In recent years, Congress has tried to address this challenge by funding the Technology Modernization Fund, which supports efforts to update agency technology. This year, the Appropriations Committee has advanced legislation that would eliminate funding for the program. Mr. Gumbel, why is funding for the Technology Modernization Fund important for strengthening Federal cybersecurity?

Mr. GUMBEL. I think it's very important to be able to fund those projects so it enhances and continues the progress of securing the Nation. Without this continuous funding, there might not be the opportunity to look at modern technologies in ways that could protect the Federal Government. Any type of funding slowdown will halt any progress and the adversaries have the opportunity to just speed up time and be able to come after any of the exposures or links into networks that aren't protected.

Mr. MENENDEZ. You said any slowdown, correct?

Mr. GUMBEL. Any slowdown.

Mr. MENENDEZ. Yes. Following up on that, what kind of investment should be prioritized when looking to upgrade Federal agencies technology? Do you have any specific examples of more investments?

Mr. GUMBEL. Yes, I think the biggest message is don't always look at Government examples to upgrade your technology, look to private sector. Private sector has done in a lot of areas, has done

very well in keeping their technologies modern. There's a lot of great use cases that the private sector is using to protect their products, to protect their customers, and to protect their IP. I think the Federal Government can learn a lot from that.

Mr. MENENDEZ. Within private sector, are there any industries that you feel are leading or ahead of the curve that we should potentially pay extra care to?

Mr. GUMBEL. Sure, sure. I think, you know, manufacturing is one, the financial services is another. Some industries that have a lot of operational technology machinery, oil, and gas, I think those are areas to look at as well.

Mr. MENENDEZ. I appreciate that. Thank you, Mr. Chairman. I yield back.

Chairman GARBARINO. The gentleman yields back. I now recognize the gentleman from Mississippi, Mr. Ezell, for 5 minutes of questioning.

Mr. EZELL. Thank you, Mr. Chairman. Guys, about 40-plus years ago, I went to work at the police department in my hometown. What I remember the chief and the administrators at the time talking about was bad communication. Mr. Head, when you were talking there a few minutes ago, it just reminded me of my early life in police service. People don't normally want to call the police unless they got a problem or something's going on. We show up, we respond. When you talked about the aircraft carrier come under attack and what we would do in response to that. I would like to know, and each of you jump in there, what we can do as a Congress to better hold some of these folks accountable for not getting the communication to the proper place so that we can say, why is this happening? Why can we not do something about it? Who can we hold accountable for these things? Anybody?

Mr. GUMBEL. Sure. I'll start off. I believe that there's an opportunity for Congress to look at some of these contracts to bridge some of the gaps of disparity. I will point to something for an example, B.O.D. 23–01 requires agencies to report on all assets connected to their networks. But however, CDM, this program explicitly excludes IOT, OT, and other managed technology. So, you have two different programs with two different views. This is just an example of areas or contracts that have this disparity. I think Congress can really help bridge the gap to make sure that everything's on the same playing field.

Mr. EZELL. Thank you. Mr. Head, could you talk just a little bit more about some of your concerns that you were speaking about in your opening statement?

Mr. HEAD. Sure. Reflecting on what you just asked about, one thing I've tried to understand a little bit is when someone reports a breach, FAA for a long time—I'm a pilot just for fun—and for a while there, if you had a near-miss, you report the near-miss and you're excused from losing your license over your participation in that. In the cyber space, it is not usually apparent when you report a thing whether they're going to get you for allowing it to happen or give you a Ferrari for finding it and stopping it. So, we haven't really got the risk/reward down for how do you elicit insightful cooperation and insightful response within and without the organiza-

tions? I think there's a large jurisdictional—I can't say that—contest between who's supposed to help you.

Mr. EZELL. Yes.

Mr. HEAD. So that would certainly be helpful.

Mr. EZELL. It is kind-of like in police world, if you have a problem and you don't know who to call, what do you do, you're stuck. So, I think that, you know, we as committee Members and you as very concerned folks, we have got to do a better job on our end. We have got to be able to have some very frank conversations because this is not going to stop. There are these bad actors in the world and they want our stuff. Like you were saying, you know, what have we got left that they don't have? So anyway, I want to thank you all for being here today. Mr. Chairman, I yield back.

Chairman GARBARINO. The gentleman yields back. I now recognize the gentlelady from Florida, Ms. Lee, for her second round of questions.

Ms. LEE. Thank you, Mr. Chairman. Mr. Head, I would like to come back to you. You mentioned something in your opening statement and in your written testimony that you refer to as our Cyber Manhattan Project. Would you please share with us a little bit more about your vision there and how you think that would look?

Mr. HEAD. Sure. That was the hardest part about writing it because when they started the real Manhattan Project, they didn't put it on public record and put it on C–Span, hey, we're just looking to build a bomb and nuke you. You know, shoot these guys because they are our lead scientists. So, I think what we should do is think about some percentage of our budget. In Texas, I think it was Lady Bird Johnson forever ago that put in the thing for 2 percent of all highway funds will be spent on plants and trees and beautification. We spend a lot of money. I describe it in the testimony that a lot of the cyber efforts remind me of your kids playing 5-year-old soccer. They are all just huddled around the ball chasing the latest buzzwords. At the end of the day, they are not a team and they didn't accomplish anything. That's kind-of prefaced by the we suck at cyber as a country.

Although there's some really good folks in the industry and I think all of us put together in a quiet time would say, let's just fix it. Like the two buzzards' patience, hell, let's kill something. You know, so I think there's room in the oversight process to say to DISA, to DARPA, to somebody, gee, you're in charge of making this suck less every month.

You know, and then there's been some rapid progress made in a lot of fronts, particularly after go back to World War II. But I think, you know, the measure of pissed-offness ought to be higher than it is for us getting attacked every day and doing nothing.

So, I think I would challenge that back to you guys. This is like I told today coming and testifying with you guys, nothing against it, but on my list of top 10 things to do, it's 3,742nd.

But I think now the time is right for doing something and I think that the brains are right for doing something. So, I'd just love to see let's do something that's not ordinary. At the end of the day, we can say, that was bad, we fixed it.

Ms. LEE. On that point, you also just referenced the concept of risk/reward.

Mr. HEAD. Yes.

Ms. LEE. Who is working with us? What are they reporting? When and how are they reporting it? I know I previously worked at an agency that implemented a bug bounty program——

Mr. HEAD. Right.

Ms. LEE [continuing]. To that end, so that in hopes that some of the good guys might help us identify issues that we had prior to the bad guys finding them. What are your thoughts on that type of solution or any other ideas you have to help us properly incentivize risk/reward?

Mr. HEAD. Plenty. I would start, though, with removing the stupid. So, I was looking at one a few years ago that Congress funded and the Pentagon implemented, and it was basically free service for defense contractors. So, you could basically rent this dog that will come in and bite you and your children. So, anything they find, you're on the hook for paying the full cost of remediation, which could bankrupt you.

So, the rightful answer would be don't ask, don't invite, don't participate, because you're renting a dog that could hurt you. Does that make sense?

Ms. LEE. It does.

Mr. HEAD. Because we're going against formidable adversaries and most people don't have the staff to play that game. Like I say, comedy abounds when you look at the rules that we put in place. But I think a reason to pass through all of those to say let's remove the worst first.

Ms. LEE. All right. Mr. Sheldon, and I will ask each of you this preparing to come here today and the things that you think we need to have top of mind and we need to be working on, is there anything you haven't had the chance to tell us about today that you think we should know?

Mr. SHELDON. Thank you for the opportunity. Really, just to drive more focus in the Federal space. So many of the attacks that we see, they don't involve malware, they don't involve classic indicators of compromise that we can block through existing solutions. It is really a compromised credential or something to that effect that might cause the breach.

So, there are some solutions in place and some architectures that try to address that. Zero trust is one of them. That's something that I would encourage all of us as a community to think more about. How do we promote the adoption of that type of solution in the Federal space?

Ms. LEE. Mr. Head.

Mr. HEAD. I think I've talked too much and told you most of my ideas, so.

Ms. LEE. Pass.

Mr. HEAD. Thank you.

Ms. LEE. Mr. Zakowicz.

Mr. ZAKOWICZ. Thank you. I was going to echo my colleague from CrowdStrike, and I'm impressed we went this long before saying zero trust for the hearing. But I think identity is an area we haven't spent much time talking about in this forum but is critically important to understand who is actually on the network.

What are they doing? How do we make sure that people only have access to the things they need to get their job done?

Ms. LEE. Fundamentally zero trust type of thinking?

Mr. ZAKOWICZ. Correct, yes. One of the fundamental pillars of zero trust is identity, and I think that is one that needs the most focus first.

Ms. LEE. Access control.

Mr. ZAKOWICZ. Yes.

Ms. LEE. OK. Mr. Gumbel, what about you?

Mr. GUMBEL. Yes. I'd say last because I've said a lot today, but I think ensure that procurements and programs are aligned to stated administrative, Executive Orders, and agency BODs. I think that's super important.

Ms. LEE. All right. Thank you, Mr. Chairman. I yield back.

Chairman GARBARINO. Thank you very much. I really want to thank the valuable testimony from our witnesses today. Mr. Head, I am glad that the 3,741 other things on your list weren't available to you today. I want to thank the Members for their questions.

The Members of the subcommittee may have some additional questions for all of you, and we would ask the witnesses to respond in writing. Pursuant to committee rule VII(D), the hearing record will be held open for 10 days. Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:25 a.m., the subcommittee was adjourned.]