



Testimony

Eric Goldstein

Executive Assistant Director for Cybersecurity

**Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security**

**FOR A HEARING
BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES**

**Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection**

“Evaluating Federal Cybersecurity Governance”

October 25, 2023

Washington, D.C.

Chairman Garbarino, Ranking Member Swalwell, and members of the Subcommittee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA) regarding our federal cybersecurity mission.

In January 2021, as the U.S. government responded to a widespread intrusion campaign exploiting a malicious software supply chain compromise of SolarWinds software to gain access Microsoft cloud environments in 2020, CISA and our partners noted material gaps in federal cybersecurity: a lack of resources, direction, centralization, and prioritization. With the support of Congress over nearly three years, we have made remarkable progress. We have used our Directive authorities to drive widespread measurable risk reduction across Federal Civilian Executive Branch (FCEB) agencies. We have gained unprecedented visibility into threats and vulnerabilities targeting FCEB networks, including through our Continuous Diagnostics and Mitigation (CDM) federal dashboard and widespread deployment of Endpoint Detection and Response (EDR) tools. We have provided effective, centralized shared services that save taxpayer resources and enable coordinated management of significant risks. We have partnered closely with the Office of Management and Budget (OMB) to increasingly manage the FCEB as a single enterprise and drive toward quantifiable performance measurement to show that our collective efforts are keeping FCEB agencies, and Americans' sensitive information, safe. Most notably:

- For the first time, we have real-time visibility into vulnerabilities and misconfigurations across 102 agencies, allowing timely remediation before intrusions occur – including directing the remediation of over 12 million Known Exploited Vulnerabilities (KEV) over the past two years.
- We have deployed EDR tools across 52 agencies, allowing our analysts to actively hunt for intrusions and enable eviction before adversaries are able to cause harm.
- We have provided new shared services that measurably reduce risks, including by blocking millions of communications with malicious websites and enabling researchers to find over 1,000 vulnerabilities in federal websites *before* they are exploited by adversaries.
- We have issued directives that have fundamentally transformed how federal agencies prioritize and fix vulnerabilities, continuously monitor for security risks, and harden frequently exploited technology assets.
- We have taken proactive steps to transform vulnerability management by publishing our Industrial Control Systems (ICS), Operational Technology (OT), and Medical Device vulnerability disclosure information in the Common Security Advisory Framework (CSAF), a machine-readable format that enables greater automation and better tooling across the vulnerability management ecosystem.
- We launched a Federal Zero Trust Management Community of Practice (CoP), which now has over 130 members and 31 unique agencies including the 23 civilian CFO Act agencies and eight critical small agencies. The CoP has advanced interagency Zero Trust collaboration, increased agency expertise and readiness, and built a community of value

for our federal partners.

Even as we reflect on our accomplishments, we recognize that we are at a midpoint on our journey. Recent intrusions into cloud-based email environments demonstrate our continued need to drive strong accountability across federal vendors, further advance our visibility into cloud and mobile environments, and advance adoption of zero-trust principles for agency environments and secure-by-design practices for all technology providers.

CISA's Mission and Role in Federal Cybersecurity

CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure on which Americans rely every hour of every day. One of CISA's core missions is to serve as the *operational lead for federal cybersecurity*, charged with protecting and defending FCEB networks, in close partnership with OMB, the Office of the National Cyber Director (ONCD), and agency Chief Information Officers and Chief Information Security Officers. In this role, we provide a common baseline of security across the FCEB and defend and secure the federal enterprise through proactive, collaborative cyber defense and risk management. While agencies remain ultimately accountable for their own risk, CISA is responsible for ensuring that the most significant cyber risks to the federal enterprise – the network of all federal systems – are being addressed effectively and driving progress based upon accurate and timely data.

As part of this mission, we serve as the *lead for federal cybersecurity shared services*. We have learned that many cybersecurity capabilities can be provided more effectively, affordably, and in a scalable manner through a centralized model rather than having over 100 individual FCEB agencies manage cybersecurity risk independently. Through our Cybersecurity Shared Services Office (CSSO), we provide high-quality services to advance and centralize cybersecurity capabilities across the FCEB and help agencies manage cyber risk. For example, our Protective Domain Name System service has blocked over 300 million communications with malicious websites and our Vulnerability Disclosure Platform service has enabled remediation of over 1,000 vulnerabilities in federal websites over the past year alone. We continue to explore investments in modern shared services, whether provided by CISA or by contracted third parties, that will further make the best use of federal cybersecurity resources and show clear return on investment.

Hardening the Terrain: Driving Risk Reduction Before Harm Occurs

Our work begins by making it harder for adversaries to exploit FCEB networks. Core to this priority is the CDM program, which is our foundational effort to enable real-time, continuous visibility into risks affecting federal agencies to drive timely risk reduction.

Within the last three years, the CDM program's scope, scale, and impact on federal cybersecurity has grown significantly. Previously, FCEB operators and CISA counterparts lacked sufficient operational visibility – insight into what devices, software, and users were operating within the environment – to effectively mitigate risks prior to a breach. Operators had no automated way to share valuable intelligence with other federal agencies; it was all manual data calls. Now, because of the CDM program, agencies and CISA can respond to cyber threats in a coordinated and expedited fashion by sharing data between dedicated CDM Agency Dashboards and CISA's CDM Federal Dashboard. The frequency, precision, and level of detail of this information sharing has

been a key enabler of CISA's operational visibility throughout the FCEB. CISA's cyber defense operators are increasingly turning to the Federal Dashboard to aid in incident response while agency cyber leaders and practitioners alike are shaping operational and strategic activities based on the evolving "current state" data provided by CDM. As a result, our relationships across the FCEB have progressed to much more effective, valued, and collaborative partnerships that promote identifying, understanding, and reducing risks across the federal enterprise.

As an example, in early summer 2023, CISA leveraged CDM capabilities as part of a broader response to two concerning cyber events. CISA operators analyzed near real-time agency dashboard reports to coordinate targeted notifications for the MOVEit Transfer vulnerability and understand prevalence within minutes. Additionally, in response to the recent widespread email security gateway exploit, CISA threat hunters utilized the CDM EDR platform in collaboration with the impacted agency to directly access the agency's environment to search for instances of threat activity working shoulder-to-shoulder with agency staff. This demonstrates what the federal enterprise gains by evolving our collective, interactive cyber defense posture.

The expansion of CDM's operational visibility capabilities, enabled through enhanced authorities in Executive Order (EO) 14028 and the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2021, have greatly increased the value of the CDM investment through newly accessible use cases that enhance threat hunting and vulnerability management. CISA now utilizes the CDM Federal Dashboard, a tool of operational first resort, to assess and coordinate effective response to cyber threats. We're proud of the progress we've made over the last decade and are looking forward to continuing to advance CDM's capabilities in the future.

As we look to evolve the CDM program, we will extend the portfolio of deployable cyber defense capabilities while updating our operating model to protect the critical investments made to date. Over the next several years, CDM will incorporate mobile devices, cloud services, and the Internet of Things (IoT) into CISA's operational visibility. We will deploy new protections for federal agency data repositories; provide rich, host-based insight into High Value Assets (HVAs); and integrate modern network sensor capabilities. Additionally, we will ensure operationalization of our CDM investments to drive risk-based decisions, respond to threats, and contribute to agencies' efforts to implement zero trust architecture principles.

While CDM is a foundation of FCEB cybersecurity, it is not our only mechanism to drive change. Through our Automated Testing program (formerly known as Cyber Hygiene), we assess internet-facing assets across every FCEB agency. This program provides near-continuous vulnerability scanning across all types of internet-facing assets as well as bi-weekly, deep-dive scanning for internet-facing web applications.

We also conduct penetration tests, red team assessments, and vulnerability assessments to identify exploitable conditions internal to federal agencies. The Federal Attack Surface Testing (FAST) program leverages new legal authorities granted by the FY21 NDAA to conduct "no notice" continuous penetration testing, including across seven FCEB agencies in the past fiscal year. This led us to successfully identify critical and high findings on several agencies' internet-facing web applications. In collaboration with the agencies, CISA re-tested the findings to validate agency remediation actions to ensure proper fixes were deployed. The SILENTSHIELD program also exercises FY21 NDAA authorities. The long-term, no-notice approach afforded by these authorities

enabled CISA to get an accurate depiction of an agency's true security posture. Within its first program year, SILENTSHIELD successfully targeted, compromised, escalated, and maintained access to an agencies network and is enabling long term FCEB cybersecurity and architecture investments.

Recognizing that every agency must prioritize their finite cybersecurity resources, we maintain the KEV catalog as the authoritative source of vulnerabilities that have been exploited in the wild, sending a clear message to all organizations to prioritize remediation efforts on the subset of vulnerabilities that are causing immediate harm based on adversary activity. CISA's efforts are enabling FCEB agencies to deny threat actors opportunities to gain access to federal networks and reduce risk of compromise due to internet accessible KEVs that frequently compromise public and private entities. These activities are yielding clear results:

- Since the creation of the KEV catalog in November 2021, FCEB agencies have remediated more than 12 million KEV findings including over 7 million this calendar year alone.
- FCEB agencies have demonstrated a 72% decrease in the percentage of KEVs exposed for 45 or more days.
- The mean-time-to-remediate KEVs is an average of nine days faster than for non-KEVs, and 36 days faster for internet-facing KEVs.
- From FY22 to FY23, CISA observed a 79% reduction in the FCEB's attack surface due to internet-accessible KEVs, based on analysis of Automated Testing capability data, despite an increase in KEV catalogue entries during this timeframe.

Leveraging Our Directive Authority

Effectively securing the FCEB requires a coordinated action to address urgent risks. While our Directive authorities have proven highly beneficial in emergency situations, we have derived even greater value in mandating common steps to mature key cybersecurity capabilities that yield enduring benefit. CISA works in consultation with NIST and in conjunction with OMB and FCEB agencies to develop these Directives, and this collaboration has proven invaluable to managing cyber incidents and driving collective action.

For example, in FY22 CISA issued two Emergency Directives (EDs) requiring agencies to enumerate and remediate all instances of VMWare and Log4J, critical vulnerabilities that pose grave risk to the federal enterprise and report all findings to CISA. Through issuance of these Directives, agencies remediated 56,400 Log4J findings and nearly 2,000 vulnerable VMWare instances. CISA's efforts significantly reduced the risk that threat actors could exploit these existing vulnerabilities, protecting federal information and enhanced enterprise network security. In FY23 CISA issued two Binding Operational Directives (BOD). *BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks* drove significant visibility improvements for agencies and CISA and vastly improved federal cyber defense. *BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces* directed agencies to better secure Networked Management Interfaces in response to threat activity targeting network devices supporting underlying network infrastructure. CISA has been identifying these interfaces across

federal agencies and working with them to reduce their attack surface in compliance with the Directive requirements.

CISA is prioritizing development of additional directives to address operational risk and drive action to reduce overall attack surface and ensure better coordination across the federal enterprise. In FY24, CISA is focused on directive requirements to improve threat detection, incident response, and secure cloud management. Furthermore, CISA plans to address gaps and redundancies in legacy directives as a part of a broader strategic approach. Going forward, CISA will remain committed to analyzing ways to leverage its Directive Authority to address foundational cybersecurity challenges and ultimately reduce the likelihood of a future cybersecurity incident.

Expanding Our Operational Collaboration Model: Increased Participation and Value for Partners

Our Joint Cyber Defense Collaborative (JCDC) continues to cultivate multi-directional information sharing, operational collaboration, and strong working relationships with members of the FCEB to counter persistent, emerging cyber threats and comprehensively strengthen the evolving federal cyber domain.

In FY23, JCDC established a portfolio-based approach to FCEB engagements, enabling more focused operational engagements with individual FCEB agencies and improving ongoing collaboration and multi-directional information exchange across the FCEB. This approach organizes our FCEB engagements into seven portfolios, each with dedicated CISA portfolio managers and cyber experts. The seven portfolios are Energy and Science, Financial and Business, Interior Services, Security and Foreign Affairs, Medicine and Agriculture, Infrastructure and Government Administration, and Education and Labor. Each portfolio includes CFO Act Agencies as well as smaller and micro agencies. In FY23, CISA held 68 kickoff meetings (including meetings with 21 CFO Act agencies).

To further drive focused and impactful information exchange and joint collaborative action, CISA also established critically important communications pathways through Slack, including channels built around FCEB cybersecurity news, FCEB indicators of interest, cybersecurity vulnerabilities impacting the FCEB, a channel specific to agency CISOs, and a dedicated channel for micro agencies.

Achieving Persistent Visibility: Real-Time Analysis of FCEB Networks

The authorities granted to CISA to enable persistent access and proactive hunting have fundamentally changed the way we work with agencies to identify, assess, and remediate malicious activity on federal networks. Since 2021, CISA has procured over 1.2 million EDR licenses to assist agencies in deploying advanced, host-based protections that provide advanced monitoring, detection and remediation capabilities on government laptops, workstations, and servers. EDR supports threat hunting and deep visibility in behaviors and activity on covered endpoints, making it one of the most effective cyber defense technologies available. Each of these EDR tools includes the ability for CISA threat hunters to have direct and persistent access to agencies' EDR platforms. With this access, our threat hunters can easily conduct hunt operations across federal agency

organizational boundaries, greatly enhancing CISA's ability to rapidly identify and correlate malicious behavior in accordance with FY21 NDAA authorities and EO 14028 requirements.

This translates to a paradigm shift in CISA's Threat Hunting services. Coupled with the operational visibility afforded through the CDM Federal Dashboard, CISA acts as a force multiplier to assist agency cyber operators in the investigation and remediation of cyber threats. In the past, providing this level of support to agencies required CISA to send fly-away teams with their own equipment to embed with agencies onsite, often in a process that took days or weeks to complete. Now, CISA can provide this support in near real time. Throughout FY24, CISA will be executing proactive hunts of agencies continually targeted by malicious actors and baselining the FCEB enterprise to inform strategic initiatives, modernization, and optimization.

Creating a Modern Cyber Defense Agency: Toward Integrated Data Analysis

Through years of managing the National Cybersecurity Protection System (NCPS), CISA gained a firsthand view of evolving adversary techniques and changes in the technology environment, including previously unseen tactics, tools, and techniques, increased sophistication, and persistence with highly advanced evasion capabilities. As our adversaries and technology change, we are adapting accordingly.

The legacy NCPS program, to include the EINSTEIN sensor suite, was built to provide intrusion detection and prevention capabilities, advanced analytics, and information sharing capabilities to mitigate cyber threats to federal civilian networks. Looking ahead, CISA has proposed several program and activity changes reflected in the President's FY24 budget, focused particularly on the transition of certain legacy NCPS systems into the proposed Cyber Analytics and Data System (CADS) program.

To understand the transition to CADS, one must begin by understanding a fundamental transition within CISA. For much of CISA's history, including as our precursor organization, we had minimal access to relevant and actionable cybersecurity information. The past two years have seen a fundamental shift: as described throughout this testimony, our analysts now have unprecedented access to ever-increasing amounts of operational data from our sensors and EDR tools deployed across agency networks, from our shared services, and from our partners. To make best use of this data, we need an operating environment that is highly interoperable with many systems and their highly diverse input and output requirements, capable of consuming massive data amounts, including multiple sources of threat intelligence and information and rapidly growing data volumes, and is reliable, adaptable, and includes the most robust security measures to protect all systems, data, and users. CADS will ingest data from myriad sources, apply robust automation and analytics, and provide CISA's full suite of cybersecurity teams with access to analytical results, threat insights, and detailed visualization with capabilities to share results and mitigations in real time.

NCPS intrusion detection capabilities, specifically EINSTEIN 1 and EINSTEIN 2, will continue to be sustained under the legacy NCPS program and will undergo sensor suite upgrades and modernization. EINSTEIN 3A (E3A) Domain Name Service (DNS) intrusion prevention services will be sunset after FY24. To protect the federal enterprise against the latest threats and support emerging technologies, CISA is actively working on upgrading these intrusion detection and

prevention capabilities. The latest example is the Protective DNS resolver, a state-of-the-art recursive DNS resolver service that replaces the sunset E3A DNS services and prevents government Internet traffic from reaching known malicious destinations.

CADS is designed to provide a critical capability as CISA continues to evolve: a modern, scalable, unclassified analytic infrastructure for CISA's cyber operators. CADS will serve as the cornerstone of CISA's Joint Collaborative Environment (JCE), the central technology ecosystem by which CISA and its partners will integrate, analyze, collaborate, and act on cybersecurity information to conduct cyber defense operations. A key recommendation of the 2020 U.S. Cyberspace Solarium Commission Report, the JCE will support real-time data and information sharing and operational collaboration by integrating internal and external information sources, including CADS, threat intelligence platform feeds, and various-source inputs.

The Future of CISA's Federal Cybersecurity Role

A strong operational lead agency is essential for the rapid identification and mitigation of near-term urgent threats and vulnerabilities as well as ensuring a consistent baseline for long-term capability investments and risk management decisions. To achieve this vision, CISA is focused on growing in several key areas.

First, we will further define and strengthen CISA's role as the operational lead for FCEB cybersecurity. Specifically, we are taking steps to strengthen CISA's ability to lead operational collaboration across the FCEB, including by providing collaboration tools, facilitating information exchange, and planning for operational risk reduction. Going forward, we will continue to evolve governance processes and capabilities for communications mechanisms such as Slack to enable joint action, foster transparency, and increase visibility across the FCEB. CISA is also exploring potential technology solutions for a threat intelligence platform that allows us to onboard partners into trusted enclaves to openly exchange threat information, as well as building out a cyber playbook to enhance mutually supportive FCEB response and coordination during cyber events.

Second, to further ensure unity-of-effort, shared visibility, and consistently effective security capabilities – and in line with the National Cybersecurity Strategy and its Implementation Plan – we will strengthen CISA's role as the shared service provider where there are clear gaps or requirements to do so. This includes assessing the expansion of our shared services to FCEB agencies to provide scalable, cost-effective capabilities that drive down known security risks, while growing into our role as the lead for providing and setting benchmarks for cybersecurity shared services.

Third, we will strengthen our ability to gain operational visibility across FCEB agencies, through capabilities such as our CDM program, and using this visibility to more quickly address potential intrusions and drive remediation. CISA looks forward to working with Congress, OMB, and ONCD to optimize CISA's ability to build and sustain the operational visibility required to achieve this vision, such as through the development of a plan for centralized services as outlined in the National Cybersecurity Strategy Implementation Plan.

Fourth, we will further drive and support adoption of modern security practices, such as Zero Trust principles and secure cloud implementations. We will partner closely with OMB and ONCD to

ensure agencies' long-term plans will align with and enable our operational needs like defensible networks, operational visibility, and expedited response. We will further build on newly-proposed procurement clauses to help agencies incorporate cybersecurity and transparency requirements into each of their contract relationships.

Fifth, we will bolster our ability and capacity to provide agencies with hands-on support, including through our Federal Enterprise Improvement Teams, to help agencies accelerate progress toward implementing Zero Trust architectures and implement our directives.

Finally, at a strategic level, we will continue working to defend the FCEB enterprise as a cohesive, interdependent organization, where agencies maintain their responsibility and authority to manage their own systems while centralized investments effectively address cross-agency risks.

Conclusion

As described in our Cybersecurity Strategic Plan, “we must be clear-eyed about the future we seek, one in which damaging cyber intrusions are a shocking anomaly, in which organizations are secure and resilient, in which technology products are safe and secure by design and default.” We must first build this future within and across our own federal agencies – the American people expect and deserve nothing less.

We will continue to take swift action to make the FCEB a hard target for our adversaries. This work will continue to take investment – in technology, in people, in partnerships. The past several years have shown the progress we can make with the support of Congress and our inter-agency partners, while leveraging insights and expertise from industry. Now is the time for us to take the next steps forward – and we must take them together.

Thank you again for the opportunity to be to appear before the Subcommittee. I look forward to your questions.

October 25, 2023

Testimony of Christopher J. DeRusha

Deputy National Cyber Director for Federal Cybersecurity;

Federal Chief Information Security Officer

2:00 P.M. EDT

United States House of Representatives

Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

Hearing on

“Evaluating Federal Cybersecurity Governance”

Chairman Garbarino, Ranking Member Swalwell, and Members of the Subcommittee, thank you for holding this important hearing to highlight Federal cybersecurity governance efforts. I am pleased to testify before you today with the Cybersecurity and Infrastructure Security Agency's (CISA) Executive Assistant Director for Cybersecurity Eric Goldstein, a key partner in this effort.

I will use this opportunity to update you on progress the Federal government has made in implementing the President's Executive Order on Improving the Nation's Cybersecurity (E.O. 14028), the Office of Management and Budget's (OMB) Zero Trust Strategy, and the President's National Cybersecurity Strategy (NCS). These efforts, and many others, have shifted the Federal enterprise toward achieving greater collective defense.

As I stated in my testimony before this Subcommittee last year, E.O. 14028 recognizes a hard truth: "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." The E.O. outlines a bold cybersecurity modernization agenda and serves as our roadmap for securing the Federal enterprise. Following publication of the E.O., OMB released the Federal Zero Trust Strategy (M-22-09) in January 2022 and six additional implementation memos to guide agencies in meeting the goals of E.O. 14028.

Released in March of this year, the President's NCS builds on these foundational initiatives and provides an affirmative vision for cyberspace. The NCS calls for changes to the underlying dynamics of the digital ecosystem, to shift the advantage to its defenders, and persistently frustrate the forces that threaten it. The President's vision is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them; where sensitive or private information is secure and protected; and where neither incidents nor errors cascade into catastrophic, systemic consequences. In creating these conditions, we can and must seize the opportunity to take full advantage of technological advances while instilling America's values.

A key objective of the NCS is achieving public-private collaboration at scale to reduce cyber risk at a systemic level. I appreciate the Subcommittee's approach to tackling hard cybersecurity problems and was encouraged to see the Subcommittee seeking feedback from our private sector partners last month. The private sector owns and operates the majority of our critical infrastructure and develops the leading digital technologies we use in our own environments, so their feedback and participation in incident response exercises, roundtable discussions, and other forums like this are critical to strengthening the entire ecosystem.

As Federal Chief Information Security Officer and Deputy National Cyber Director for Federal Cybersecurity, I am focused on government-wide improvement and ensuring the Federal enterprise is taking a holistic approach to confronting evolving cyber threats. My role encompasses the oversight, governance, and accountability of Federal cybersecurity efforts, as well as aligning budgetary resources to policy guidance through our annual priorities memo and working with our resource management colleagues in OMB to assess agency funding needs. CISA plays many critical roles as the operational lead for Federal cybersecurity, most importantly as Federal agencies' security coordinator. A model where hundreds of Federal agencies are left on their own to defend themselves is not sustainable. CISA programs and

services provide an enterprise-view of risk across Federal agencies, enabling a collective approach to defense, and often free up agencies' scarce dollars and resources to be allocated elsewhere.

My testimony here today alongside CISA's Executive Assistant Director for Cybersecurity, Eric Goldstein, illustrates the constant coordination occurring between the Office of the National Cyber Director (ONCD), OMB, and CISA. This collaboration is essential as it enables us to align the NCS published by ONCD on behalf of the President with the policy guidance issued by OMB and the operational cybersecurity assistance and programs CISA offers to departments and agencies.

Setting the Strategic Direction

The President's NCS calls for two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyberspace.

First, the most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem. Today, end users, like your constituents, bear too great a burden for mitigating cybersecurity risks. Individuals, small businesses, local governments, and many critical infrastructure operators have limited cyber expertise and resources. Yet, these users' choices – even when well-intentioned – can have a significant impact on our national cybersecurity. Across both the public and private sectors, we must expect more of the most capable and best-positioned actors – including the Federal government – to make our digital ecosystem secure and resilient. In a free and interconnected society, protecting data and assuring the reliability of critical systems must be the responsibility not only of the owners and operators of the systems holding our data and enabling our daily lives, but also of the technology providers building and servicing these systems.

Second, our economy and society must incentivize activity that makes cyberspace more reliable over the long term. Protecting the systems we have now, while investing in and building toward a future digital ecosystem that is more inherently defensible and resilient are both priorities. The strategy outlines how the Federal government will use all available tools to reshape incentives and achieve unity of effort in a collaborative, equitable, and mutually beneficial manner. We must ensure that market forces and public programs alike reward security and resilience, build a robust cyber workforce that draws from all parts of our society, embrace security and resilience by design, strategically coordinate research and development investments in cybersecurity, and promote the collaborative stewardship of our digital ecosystem with our allies and partners.

Our approach to Federal cybersecurity governance embodies these two major shifts. The Federal government can better support the defense of critical infrastructure by making its own systems more defensible and resilient. This Administration is committed to improving Federal cybersecurity through near-term efforts like multi-factor authentication, endpoint detection and response, encryption, logging, and establishing skilled security teams. We are also committed to longer-term efforts to implement zero trust architectures and modernize both information technology and operational technology infrastructure. This includes the annual release of a cybersecurity budget priorities memorandum to Federal departments and agencies. This annual

guidance, issued jointly by ONCD and OMB, outlines the Administration's cross-agency cyber investment priorities and directs agencies to prioritize cybersecurity efforts that will bolster key initiatives laid out by the NCS. By aligning our budget requests with our priorities, we will ensure that agencies are investing in durable, long-term solutions that are secure by design.

Implementation and Outcomes

The strategic objectives outlined in the NCS require a strong focus on implementation. The Federal government is taking a data-driven approach and will measure investments and progress towards meeting the goals of the strategy. The Federal government is leading by example, ensuring its own networks and systems are adopting best-in-class security measures.

Additionally, over the last two and a half years, we have seen departments and agencies across the Executive Branch drive forward in implementing E.O. 14028 and the Federal Zero Trust Strategy (M-22-09). Across the Federal enterprise, agencies submitted zero trust plans that align to the vision and goals laid out in M-22-09 (*Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*). Agencies have made meaningful progress paying down technical debt and modernizing security practices and tooling. Agencies are implementing higher levels of encryption, using proven methods, and leveraging common toolsets that establish constant vigilance within our Federal systems. Additionally, the deployment of strong, industry-leading phishing-resistant multi-factor authentication makes it harder for an adversary to gain a foothold in any system.

In furtherance of E.O. 14028's goals, OMB has issued several guidance documents to better protect Federal networks and minimize the government's risk exposure. M-21-30 (*Protecting Critical Software Through Enhanced Security Measures*) is intended to: 1) protect critical software and critical software platforms from unauthorized access and usage; 2) protect the confidentiality, integrity, and availability of data used by these software and software platforms; and 3) allow agencies to quickly detect, respond to, and recover from threats and incidents involving critical software and critical software platforms. Additionally, M-21-31 (*Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*) established requirements for logging, log retention, and log management across Federal Civilian Executive Branch agencies. This will ultimately increase information sharing, empowering both accelerated incident response and more effective information system defense. Work continues on implementation of Section 4, *Enhancing Software Supply Chain Security*, of E.O. 14028. M-22-18 (*Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*) and M-23-16 (*Update to Memorandum M-22-18*) seek to minimize the risks associated with running unvetted technologies on agency networks. OMB and CISA have worked in partnership to release the Self-Attestation Common Form, which directs software producers to provide government users with assurances that they have taken specific measures to secure the development of their software products.

Implementing the bold changes within E.O. 14028 requires partnership with the private sector. On October 3, the Federal Acquisition Regulation Council published two proposed rules for public comment that implement Section 2, *Removing Barriers to Sharing Threat Information*, of E.O. 14028: 1) Cyber Threat and Incident Reporting and Information Sharing and

2) Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems. These proposed rules would require establishing minimum, consistent cybersecurity standards that apply to contracts for Federal information systems; incident reporting and CISA and Federal Bureau of Investigation access to contractor facilities and systems for forensic analysis; and implements IPv6 capability requirements, among others. In addition to implementing the requirements of Section 2 of E.O. 14028, these rules also propose changes necessary to implement the Internet of Things Cybersecurity Improvement Act of 2020. These proposed rules open the dialogue with the public and our industry partners on the steps necessary to remove barriers to information sharing, provide consistent processes for threat reporting, and implement consistent cybersecurity standards. We will continue to work with our industry partners to ensure the vision of E.O. 14028 is fully realized.

The Federal government is also leading the way in transitioning to Post-Quantum Cryptography (PQC). Per National Security Memorandum-10, “the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035.” Federal agencies were asked to conduct an initial inventory of their cryptographic systems vulnerable to a Cryptanalytically Relevant Quantum Computer (CRQC) and the initial cost estimates to transition those systems. Agencies delivered on this request this summer. This is the first time an inventory such as this has been collected, and as such there is continued work that will be needed with agencies to refine the inventories and cost estimates. Agencies will be updating this inventory annually and initial analysis indicates agencies are already thinking through the costs of the upgrades and transition to PQC. Next year, OMB will be delivering a more in-depth report to Congress on the status of agency transition to PQC, to include a risk analysis and initial cost estimates.

Long-term and large-scale change requires continued and consistent investment, complemented by innovative funding mechanisms, such as the Technology Modernization Fund (TMF). The TMF has played a critical role in supporting agencies on their journey to more modern cybersecurity practices, serving as a catalyst to show what’s possible across government and scale lessons learned while maintaining rigorous project vetting and sustained oversight. With the \$1 billion investment from Congress through the American Rescue Plan Act, the TMF Board has invested over \$600 million in 29 projects across 23 agencies to help address immediate security gaps and elevate the foundational security of Federal agencies, with an emphasis on zero trust, multi-factor authentication, and standardizing secure data and information sharing.

Conclusion

This Administration, both through Executive action and by working with Congress, has made cybersecurity an immediate priority. Together, we have been extremely active in laying the strategic groundwork for the future of Federal cybersecurity to enable the U.S. government to deliver the services on which the American public depends. Building upon the work that has been accomplished through E.O. 14028 and the Federal Zero Trust Strategy, we will continue to help departments and agencies implement the priorities laid out in the NCS with the diligence this work requires and the urgency the moment demands.

Realizing our vision of a defensible and resilient digital economy requires both whole-of-nation collaboration to rebalance the responsibility of securing cyberspace and realigning our incentive structure to favor long-term investments. I appreciate this Subcommittee's interest and support and I am confident that through partnership and frank discussions about where we need additional improvement, we will build a more defensible Federal enterprise.

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