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.