May 17, 2022

Testimony of Christopher J. DeRusha

Deputy National Cyber Director for Federal Cybersecurity;

Federal Chief Information Security Officer

United States House of Representatives

Committee on Homeland Security

Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation

Hearing on

Securing the DotGov: Examining Efforts to Strengthen Federal Network Cybersecurity

Chairwoman Clarke, Ranking Member Garbarino, and Members of the Subcommittee, thank you for holding this important hearing to highlight the one-year anniversary of Executive Order (EO) 14028, Improving the Nation's Cybersecurity. I am pleased to testify before you today with Eric Goldstein, Dr. Charles Romine, and David Shive. I would like to use this opportunity to discuss why EO 14028 represents a paradigm shift for Federal cybersecurity, why I believe that shift is important, as well as the successes we have had implementing EO 14028 over the first year.

Foundationally, EO 14028 recognizes the 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." Each section of the EO aggressively challenges the Federal government to "identify, deter, protect against, detect, and respond to these actions and actors." Many of the goals within the order are ambitious, but we are never going to improve our shared security if we are not ambitious. As Chief Information Security Officer and Deputy National Cyber Director for Federal Cybersecurity, my goal is to focus on governmentwide outcomes, and ensure that the Federal enterprise is taking a holistic approach to confronting evolving cyber threats. I welcome the aggressive and ambitious goals of EO 14028.

The security of the nation will be vastly improved when the goals of the EO are met and the programs I talk about today are fully implemented. Instead of accepting the inherent vulnerabilities of the weakest part of the system architecture, we will have robust zero trust principles deployed. Rather than accepting *SolarWinds* as the new normal, we will directly protect critical software through enhanced security measures. Firewalls will be augmented by a government-wide, continuously monitored endpoint detection and response (EDR) system. No longer will we be forced to relearn the same lessons from every attack, but instead we will systematically store and keep system logs to learn from past vulnerabilities and train the next generation of system defenders.

The work towards building the secure future envisioned by the EO has begun, but it is far from done, and challenges remain. However, the agencies have made tangible security gains and will continue to do so as this Administration implements the EO. My comments today will focus on the EO's intent to aggressively evolve the security strategy and culture across the Federal enterprise.

The Paradigm Shift in the Cybersecurity Mindset

EO 14028 makes a significant contribution toward modernizing cybersecurity defenses by protecting Federal systems, improving information-sharing between the U.S. government and the private sector on cyber issues, and strengthening the United States' ability to respond to incidents when they occur. It was the first of many ambitious steps the Administration has taken to modernize national cyber defenses.

The intent of the EO is to aggressively change the security strategy and culture across the Federal enterprise to center around leading practices in the cybersecurity community. The first step is eliminating the outdated mindset and related focus on investing in digital walls around networks in an attempt to keep sophisticated actors out. We need to invest in secure solutions to make our

Federal systems defensible and then defend those systems such that we can change the decision calculus of the adversary. We will do this by applying multifactor authentication, building in segmentation, eliminating the use of passwords, performing routine patching, and training our workforce.

Key Successes This Past Year

In January 2022, we released *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (M-22-09) to direct agencies to invest in technology that is built and deployed with security foremost in mind and move towards a zero trust architecture that provides the vigilance to detect malicious behaviors and react quickly. Whether it is the next SolarWinds or supply chain compromise Log4j vulnerability, we need to be ready to rapidly identify malicious behavior and eliminate it before it can do harm. Our security will never be impermeable, but adopting a defensible approach will bring risks down to a level we can manage. Federal agencies have responded to this call to action and provided their zero trust implementation plans, thereby demonstrating a path to a new baseline for government security that will be iterated and improved upon over time.

The goal of the zero trust strategy and associated implementation plans is to demonstrate investment in secure solutions and people over time. The EO mandates encryption of data, and agencies have responded. They are implementing higher levels of encryption, using the best methods in the industry to verify legitimate users, and bringing in common toolsets that create constant vigilance within our networks. Additionally, the use of strong, industry-leading multi-factor authentication makes it harder for an adversary to move into and then laterally in a target environment.

The vital services the Federal government provides to the nation are reliant on critical software. Events like SolarWinds demonstrate the fragility of those services when critical software is not secured. The EO recognizes that software security must be one of our top concerns. The practice of developing software through opaque processes lacking sufficient controls only hinders security; and more often, introduces vulnerabilities throughout the application. We must ensure that products and application function not only in the manner intended but also in a manner that is secure by design. We will do so by partnering with the private sector to develop processes that enhance the software supply chain security.

The EO directed the National Institute of Standards and Technology (NIST) to develop guidance on core security measures to protect critical software and OMB to require agencies to comply with that guidance. Last July, NIST issued that guidance. The following month, OMB required agencies to adopt a phased approach to implement NIST's guidance. The memorandum on *Protecting Critical Software Through Enhanced Security Measures* (M-21-30) 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.

Given the magnitude of threats Federal agencies face, they must be prepared for a threat actor to compromise someone's account or device; this is why the EO mandated deployment of a

government-wide endpoint detection and response (EDR) system that is being continuously monitored. This will improve our ability to detect malicious cyber activity on Federal networks. To achieve this, OMB issued implementation guidance to agencies as they accelerate the adoption of EDR solutions and work to improve visibility into and detection of cybersecurity vulnerabilities and threats to the Federal Government. The memorandum, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (M-22-01) is intended to improve agency capabilities for early detection, response, and remediation of cybersecurity incidents on their networks through the use of advanced technologies and leading practices. At its core, cybersecurity is a risk reduction and management activity. We are countering our adversaries' tactics and improving the resiliency of our nation.

However, despite our best efforts to defend Federal systems, cybersecurity incidents may still occur. The EO recognized this and requires agencies to improve their investigative and remediation capabilities so they can be better prepared to respond. It is essential that agencies and their IT service providers collect and maintain information from networks and system logs on Federal information systems. Log information is crucial to diagnosing, investigating and responding to cyber incidents. Without this information it can be nearly impossible to know when and how a victim was compromised or regain confidence in the integrity of affected systems. Further, the maintenance of these logs affords the Federal Government the opportunity to learn from attempts to breach system security.

OMB issued *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (M-21-31) last August to establish requirements for logging, log retention, and log management across Federal civilian executive branch agencies. The requirements established in the memorandum will ultimately increase information sharing enabling both accelerated incident response and more effective information system defense.

We recognize there is much more work to be done and this first year has shined a light on the challenges and opportunities ahead. The framework created under the EO and subsequent OMB policies are nothing less than a paradigm shift for Federal agencies. Large scale change as envisioned here does not happen in a year; it requires continued investments, resources, and cultural change derived from the visibility and support of leaders both within the Executive Branch and here in Congress.

Strong security requires time and investment, but the cost of neglecting security is far higher, whether measured in dollars, lost data and PII, or impact to national security. The $1 billion investment in the Technology Modernization Fund in the American Rescue Plan Act of 2021 has already expanded our opportunities to address cybersecurity challenges. We encourage Congress to support the full FY 2023 Budget request for the Technology Modernization Fund at $300 million and continue to invest in the many other resources that support cybersecurity throughout the Federal enterprise.

Conclusion

This Administration made cybersecurity an immediate priority in Federal IT. Since January 2021, we have been extremely active in laying the strategic groundwork for the future of Federal cybersecurity. As we move forward, we will focus on helping agencies implement these priorities with the diligence this work requires and the speed the moment demands.

None of us can do it alone. It is a partnership where collaboration is key – collaboration with my colleagues here today and, most importantly, collaboration with all of the cybersecurity personnel who support the Federal government and work tirelessly to safeguard our nation. I appreciate this Committee's leadership, and I am confident that through partnership, mutual transparency, and frank discussions about where we need additional improvement, we will build a more secure and resilient Federal enterprise.

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