September 23, 2021

Testimony of the Federal Chief Information Security Officer

Christopher J. DeRusha

United States Senate

Homeland Security and Governmental Affairs

Hearing on

National Cybersecurity Strategy:
Protection of Federal and Critical Infrastructure Systems

Chairman Peters, Ranking Member Portman, and Members of the Committee, thank you for the invitation to testify about the Administration's cybersecurity priorities. I am pleased to be here today with Director Easterly and Director Inglis. The three of us work closely together, in partnership with the National Security Council (NSC), to leverage our unique authorities in the service of our common mission—to build a more secure federal enterprise. My goal as the Federal Chief Information Security Officer is to focus on enterprise-wide outcomes, and ensure that we are taking a holistic approach to addressing common challenges while taking advantage of shared opportunities.

This committee took decisive action earlier this year by supporting the allocation of $1 billion in emergency funding to the Technology Modernization Fund (TMF). To date, we have received more than one hundred project proposals from agencies, requesting more than $2 billion. Seventy-five percent of those proposals are focused on cybersecurity improvements. As the TMF Board prepares to release the first round of project approvals, there is a strong focus on learning what works well for one agency and translating those experiences and lessons into successful outcomes for many agencies.

These are challenging times to manage cybersecurity for any enterprise, even more so when the enterprise is as attractive a target as the federal government. This is not the time to maintain a steady course. We need to embrace bold new ideas, form enduring partnerships, and above all to act with a sense of urgency. I would like to highlight a few areas where this administration is taking decisive action.

Zero Trust Security

Earlier this month, we released for public comment a draft strategy to move the U.S. Government toward zero trust cybersecurity principles. The term "zero trust" refers to a security model where every person, device, and network inside of an organization is considered untrusted and even potentially compromised. This is a significant shift from the traditional model used by many enterprises throughout the public and private sectors. Our strategy calls for agencies to make this shift, and envisions a federal zero trust architecture that:

- Bolsters strong identity practices across federal agencies;
- Relies on encryption, authentication, and application testing instead of perimeter security;
- Recognizes every device and resource the government has;
- Supports intelligent automation of security actions; and
- Enables safe and robust use of cloud services.

This is an ambitious, multi-year strategy that establishes a new baseline for government security and requires us to iterate and improve over time. To start, our strategy requires agencies to adopt known, trusted technologies and practices that make it harder for even sophisticated actors to compromise an organization. We also recognize that some areas of zero trust are too complex to address through prescriptive technical requirements. In these areas, the federal government will continue to find flexible and innovative solutions to overcome practical and technical hurdles. Our strategy requires agencies to grapple directly with these challenges by developing long-term plans, demonstrating early, iterative progress, and working together to share information and develop best practices.

We also recognize that implementing zero trust principles is a paradigm shift for security, so we sought input and recommendations from experts by sharing the strategy for public comment. We are excited to see what can be strengthened and improved in this strategy before we release the final version.

Executive Order on Improving the Nation's Cybersecurity

In May, the President issued Executive Order 14028, with the intent of dramatically improving the nation's cybersecurity by requiring critical cybersecurity capabilities to be deployed government-wide, improving information-sharing between the U.S. government and the private sector, and strengthening the United States' ability to respond to incidents when they occur.

We recently passed the 120-day milestone since the Executive Order was issued. Over that time, OMB and NSC have been leading the execution across government. Key deliverables include:

- Over the summer, NIST, in consultation with OMB, CISA, ODNI, and NSA, provided a definition of critical software as well as accompanying security guidance. NIST also published minimum standards for vendors to test their software source code as part of a broader initiative to improve the security and integrity of the software supply chain, which will continue into FY 2022.
- OMB and DHS worked closely with key stakeholders to develop recommendations for new contract clauses that will enhance how the federal government and industry work together to address cyber threats. These clauses will streamline the sharing of threat intelligence and notification of incidents, and support a more rapid and coordinated response when security incidents occur.
- OMB released Memorandum M-21-30, *Protecting Critical Software through Enhanced Security Measures*, which builds upon NIST guidance by helping agencies identify their most critical software and prioritize security requirements for that software.
- OMB then released Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents.* This policy was developed in collaboration with DHS and establishes a comprehensive set of requirements for the logging of security-relevant data, centralization of access to those logs, and information sharing across agencies to support incident detection and response.
- NIST also recently held two days of workshops to get private sector input on criteria for consumer cybersecurity labeling programs for both internet of things devices and consumer software.

FISMA Reform

The Federal Information Security Modernization Act of 2014 describes the responsibilities and rules of the road for federal cybersecurity that underpin much of the policy and oversight work that our office does today. We appreciate the opportunity to work with Congress on reforming this flagship piece of legislation to improve the government's ability to manage risk. We share

Congress' view that federal cybersecurity management should be more clearly oriented towards security outcomes, and we are already updating our own FISMA oversight processes in service of this goal. What OMB asks agencies to measure and report should be the things that matter most and help determine whether agency cybersecurity investments are producing results.

We also need to emphasize the right roles for our current federal organization. For example, an updated FISMA should reflect CISA's heightened role in collecting and sharing risk information across the federal enterprise, providing cybersecurity operational support to agencies, and providing surge support capabilities when agencies respond to incidents. It should also maintain and strengthen the role of NIST in developing cybersecurity and privacy standards and guidelines, and clearly describe the responsibilities of the new National Cyber Director in regards to federal cybersecurity.

Conclusion

This administration is dedicated to making cybersecurity the immediate priority in federal IT. Since January, we have been extremely active in both responding to incidents and laying the strategic groundwork for the future of federal cybersecurity. As we move forward, we will be focused on helping agencies implement these priorities with the diligence this work requires and the speed the moment demands.

As I have said before, none of us can do it alone. This 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's digital assets. 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.