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, Infrastructure Protection & Innovation

Cyber EO Implementation

May 17, 2022

Washington, D.C.

Chairwoman Clarke, Ranking Member Garbarino, and members of the Subcommittee, thank you for the invitation to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA). As we recently passed the one-year anniversary of President Biden's Executive Order on *Improving the Nation's Cybersecurity*, I appreciate the opportunity to highlight how CISA is driving improved cybersecurity across the 101 department and agencies of the federal civilian executive branch (FCEB) in order to protect the government services and sensitive information upon which the American people depend.

As the operational lead for federal civilian cybersecurity, CISA has served a central role in implementing the Executive Order and driving broad strategic change across the cybersecurity landscape. We have done so in close collaboration with my fellow witnesses from the Office of Management and Budget (OMB), Office of the National Cyber Director (ONCD), and the National Institute of Standards and Technology (NIST), in addition to our many public and private sector partners. I am proud to report that CISA met each of the requirements in the Order by the relevant deadlines. More importantly, CISA and our partners have catalyzed adoption of new approaches that should yield material benefits in securing the federal civilian enterprise going forward and driving systemic improvings in security and resilience of the broader technology ecosystem.

Partnership and collaboration are critical to our success and at the heart of CISA's mission. Our goal is simple: actively defend and strategically guide FCEB departments and agencies through best-in-class and cost-effective services, capabilities, and information as part of a deep partnership with OMB, ONCD, the National Security Council (NSC), and each agency's CIO and CISO. While we remain on a journey of improvement across the FCEB, the Executive Order and resources provided by Congress have dramatically accelerated progress over the past year.

The SolarWinds Compromise: A Call to Action

To understand the importance of the Executive Order, it's important to begin by reflecting on lessons leared from the SolarWinds intrusion campaign. In early December 2020, the Federal government became aware of a cyber intrusion campaign that included compromises of U.S. government agencies and private sector organizations. This highly sophisticated campaign, attributed to the Russian Foreign Intelligence Service (SVR), involved a compromise of trusted software updates to inject malicious code into thousands of victim organizations. After gaining entry, the SVR used advanced techniques and tradecraft to remain hidden for an extended period.

The SolarWinds supply chain compromise served as an important call to action for the government, and the Nation as a whole, demonstrating the capabilities of our most sophisticated adversaries and the potential implications of persistent intrusions on our national security, economic prosperity, and public health and safety. The campaign highlighted a delta between our adversaries' capabilities and our national cyber defense posture, and reflected the need for a new model. CISA led the U.S. government's response to the campaign, including by actively responding to intrusions, issuing an Emergency Directive requiring specific mitigation steps, and developing tools to help organizations drive remediation and eviction. As part of this role, CISA supported federal CIOs to gain reasonable confidence into the integrity of their networks and eviction of the adversary. Each significant line of effort in the Executive Order is based upon our lessons learned during the

SolarWinds campaign or other major intrusions.

First, the campaign reinforced that traditional architectures that rely upon perimeter defenses will often fail to protect networks against malicious attacks, and, in some cases, facilitate our adversaries' ability to move freely within networks. The Executive Order tackles this issue by driving urgent adoption of Zero Trust Architectures with heightened focus on securing data and services that assume no implicit trust can be granted based on physical or network location. Zero Trust Architectures will require significant changes to Federal Government information technology environments and cybersecurity capabilities. As part of this effort, CISA published a Zero Trust Maturity Model that guides agencies' adoption of Zero Trust principles and illustrates how CISA's services, like Continuous Diagnostics and Mitigation (CDM), will evolve to enable agencies' Zero Trust implementations. Recognizing that secure migration to cloud environments is inherently related to progress toward Zero Trust, we published a Cloud Security Technical Reference Architecture and continue efforts to help federal civilian agencies, and the broader community, utilize cloud resources with security as a priority. CISA published technical guidance outlining preferred approaches to enhancing the security of cloud business applications while enabling greater operational visibility of those environment.

Second, CISA and individual agencies must continue to pursue enhanced visibility into potential adversary activity targeting federal networks. The Executive Order has driven urgent steps to improve visibility into threats targeting the U.S. government, including deployment of Endpoint Detection and Response (EDR) capabilities across FCEB networks. CISA developed a FCEB-wide EDR initiative to support host-level visibility, persistent threat hunting, containment and remediation, and incident response. To this point, we have provided leading commercial EDR capabilities to more than 15 agencies, published an EDR Concept of Operations to define how CISA and agencies will proactively and persistently hunt for threats, which will dramatically reduce our time to detect intrusions. This has allowed us to directly engage and support all agencies impacted by the SolarWinds event. We have also made urgent improvements into our CDM program to understand the state of cyber risk across the FCEB, including deploying a new dashboard that now provides information on asset status, vulnerabilities, configuration flaws, and other risk conditions across 65 agencies, with more coming online each month.

Third, we gained an understanding of the deep criticality of managing supply chain risks. To this end, CISA and our partner agencies have developed new contract clauses that will impose strong security and information sharing requirements on federal contractors. We also worked with our partners at NIST to develop an inventory of critical software, which will ensure that providers of such software are held accountable to rigorous development and security controls. As an additional critical step, CISA supports the effort to drive adoption of Software Bills of Material (SBOM), the equivalent of "food labels", throughout the software supply chain, enumerating the specific packages and libraries used to construct the software. CISA will help refine, operationalize, and scale SBOM, building on the community work begun by NTIA, NIST, and a very diverse set of industry leaders and experts. Widespread adoption of SBOM will provide essential transparency in understanding security risks affecting our Nation's critical technology.

Fourth, we recognized that incident response, threat hunting, and security operations capabilities across the FCEB required further maturation. We developed and published cybersecurity incident response playbooks that will govern a standardized approach to incident response across the

civilian government and provide a benchmark for the broader cyber community. Being prepared and formalizing a standardized plan for how the U.S. Government responds to cyber incidents will improve the speed and efficiency with which we can respond to, recover from, and minimize impact from cyber intrusion campaigns. We also recognized an urgent need to remove barriers to sharing threat information between the Government and private sector. Industry is often uniquely positioned to detect a compromise first, which is why it is imperative for us to continue to deepen operational collaboration with key industry partners. The actions set out in the Executive Order ensure that IT service providers are able to share information with the government, and even requires them to share certain breach information. It is becoming increasingly clear that sophisticated actors don't care about the boundaries between individual agencies' networks and systems. We need to continue to focus on CISA being the recipient of threat, vulnerability, and incident information, even as we work to urgently and transparently implement requirements under the Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022, so we can enrich that information and broadly share it to protect other potential victims.

A Vision for the Future of Federal Civilian Cybersecurity

It is clear that status quo approaches to federal civilian cybersecurity have been unsuccessful. A new approach is needed that is grounded in the foundational precept that the federal enterprise must have unified visibility, capability, and trust of our partners to rapidly identify and drive mitigation of cybersecurity risks and accelerate progression toward secure technology environments. Our vision is an FCEB environment in which intrusions are swiftly detected and remediated, security weaknesses are identified and mitigated before intrusions occur, and outdated or insecure technologies are replaced by modern infrastructure leveraging Zero Trust principles.

To achieve this vision, we must continue four urgent efforts. First, we must continue to gain visibility across FCEB agencies, including by accelerating our EDR initiative and advancing our visibility into threats targeting agency cloud environments – and using this visibility to more quickly notify agencies of potential intrusions and drive remediation. Second, we must expand our provision of shared services to FCEB agencies to provide scalable, cost-effective capabilities that drive down known security risks. Third, we must provide agencies with actionable guidance and 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, CISA will continue to lead our national effort to drive adoption of modern security practices, including Zero Trust principles and secure cloud implementations, that will make measurable progress in reducing cybersecurity risk at scale.

Conclusion

Our Nation is at a turning point in cybersecurity. The Executive Order has provided us a roadmap to make that turn and take important steps toward this new direction. We must continue to work together, by deepening our operational collaboration and ensuring we have the plans and policies in place now, to defend against new and changing cyber threats going forward. Recent incidents and the ongoing threat of malicious Russian cyber activity provide a stark reminder about the vulnerability of our federal networks.

The Executive Order catalyzed extraordinary action – but it was just the start. In order to get to

where we need to be in terms of federal cybersecurity, we need sustained and coordinated investment in cybersecurity and IT Modernization over time. Our approach will require multiple layers of protection, integrated technology, and continued investment from Congress. There is no silver bullet or single technology that will secure our systems. At CISA, alongside OMB, ONCD, NSC, and our partners across the federal government, we stand ready for the challenge ahead. And we deeply appreciate Congress' and this Administration's commitment to achieving our shared end goal of safeguarding our most sensitive data and ensuring the availability of critical services on which our citizens depend.

****END****