Testimony

Brandon Wales

Acting Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Prevention, Response, and Recovery: Improving Federal Cybersecurity Post-SolarWinds"

BEFORE THE UNITED STATES SENATE

Committee on Homeland Security & Governmental Affairs

May 11, 2021

Washington, D.C.

Chairman Peters, Ranking Member Portman, and members of the Committee, thank you for the opportunity to testify on the Cybersecurity and Infrastructure Security Agency's (CISA) role in cybersecurity incident response and recovery. Given recent cybersecurity incidents impacting the federal government, this hearing provides a timely opportunity to review how CISA works with federal agencies to manage cybersecurity incidents. I also look forward to discussing lessons learned from recent cybersecurity incidents, and sharing some perspective on how we can apply those lessons to improve our collective cybersecurity across the 102 federal civilian departments and agencies along with non-federal stakeholders.

While the purpose of this hearing is to discuss our collective response to the major software supply chain compromise generally referred to as the "SolarWinds" campaign, in the few months since this campaign, CISA has additionally led the national response to widespread exploitation of vulnerabilities in Pulse Connect Secure, a common Virtual Private Network technology used to connect remote workers to their organizational networks, and in Microsoft Exchange Servers. These latest compromises serve as urgent calls to modernize our cybersecurity and network infrastructure.

CISA leads the Nation's efforts to advance the cybersecurity, physical security, and resilience of our critical infrastructure. CISA serves as a focal point to share information and enable operational collaboration among the Federal Government, SLTT Governments, the private sector, international partners, law enforcement, intelligence, and defense communities. One of our primary missions is to enhance the security of federal networks. To accomplish this mission, CISA provides tools, services, training, guidance and direction that enables timely identification of, protection against, and response to cybersecurity risks. We *Defend Today* through collective defense against threats and vulnerabilities and *Secure Tomorrow* by ensuring effective long-term risk management and cyber resilience. Our vision is a secure and resilient cyber enterprise that enables the federal government to provide critical services to the American people under all conditions.

Federal civilian agencies are facing urgent cybersecurity risks, including from nation-state adversaries. To address these risks, CISA focuses on gaining visibility, analyzing risks, and driving remediation. In the first instance, CISA provides sensors and other capabilities, such as remote scanning and threat hunting to identify and detect potential malicious activity across federal civilian networks. Second, CISA analyzes data from multiple sources to understand unusual activity that may indicate a compromise. CISA maintains the unique capability to integrate information received from federal civilian networks with data from the intelligence community, private sector, SLTT, and other partners. Third, CISA drives remediation action via incident response support and binding directives to federal agencies.

CISA also works to address longer-term gaps in federal cybersecurity, such as identifying outdated systems, indefensible architectures, or inadequate focus on system maintenance, which are barriers to adopting modern cybersecurity technology and achieving consistent cyber hygiene. In order to raise the baseline for federal cybersecurity, CISA provides agencies with shared services and cybersecurity tools and training through the Quality Service Management Office and the Continuous Diagnostics and Mitigation (CDM) program. CISA further leads capacity building efforts to reasonably ensure that civilian agencies implement

strong governance programs and effectively manage their technology environments, in close coordination with the Office of Management and Budget.

Cyber attacks of significant consequences create serious risks for the United States, threatening our national security, economic prosperity, and public health and safety. Federal networks face large and diverse cyber threats ranging from unsophisticated hackers to nation-state intruders using state-of-the-art techniques that are challenging to defend against with even the best cybersecurity capabilities. The three recent cyber campaigns targeted federal networks and private sector entities using advanced cyber capabilities designed to undermine America's critical infrastructure, target our intellectual property, steal our national security secrets, and disrupt our democratic institutions.

SolarWinds Cyber Supply Chain Compromise

In early December the federal government became aware of a cyber intrusion campaign that included compromises of U.S. government agencies, critical infrastructure entities, and other private-sector organizations beginning in at least September 2019. This highly sophisticated operation, 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.

On December 13, 2020, the National Security Council stood up the Cyber Unified Coordination Group (UCG). Composed of CISA, the FBI, and ODNI—and with support from NSA—the UCG coordinated both investigation and remediation efforts for the federal government. As the lead agency for asset response in the federal civilian space, CISA provided technical assistance to affected entities who requested it as they identified and mitigated potential compromises.

CISA's work in response to this campaign falls under four primary lines of effort: scoping the campaign, sharing information and detection techniques, short term remediation, and long-term strategic recovery and rebuilding.

Scoping the Campaign

Under the first line of effort, CISA worked closely with private sector, government, and international partners to understand the full extent of the campaign. To date, we have confirmed that nine federal agencies experienced exfiltration of data or lateral movement by the adversary across their networks, along with a number of private sector entities, the majority in the IT sector.

Sharing Information and Detections

CISA began developing detection techniques and sharing information upon learning of the intrusion campaign. On December 13, 2020, we issued Emergency Directive 21- 01, requiring federal agencies to disconnect affected versions of SolarWinds Orion devices from

their network or take them off-line. We released the Directive publicly driving immediate mitigation steps and help both public and private sector entities determine whether their networks were exposed to the adversary. Within 72 hours of the directive's release, 100% of federal agencies that reported using an affected version of SolarWinds Orion had taken them off-line.

On December 17, CISA released a detailed alert describing the tactics of this actor and providing initial guidance and indicators to entities with suspected compromises. We have both supplemented our Emergency Directive and updated our Alert several times, and we will continue to do so as we uncover new information. We followed the release of our Directive and Alert with stakeholder calls, engaging thousands of public and private sector entities to provide information to guide their detection and response efforts. On Christmas Eve, CISA released a tool to help detect compromised accounts and applications in the Microsoft Office 365 cloud environment, which was widely targeted by the adversary as part of this campaign. And on March 18, 2021, we launched the CISA Hunt and Incident Response Program (CHIRP). CHIRP scans for signs of compromises within an on-premises environment to help network defenders find indicators of compromise (IOCs) associated with the SolarWinds and Active Directory/M365 Compromise.

Short Term Remediation

Under the third line of effort, CISA provided incident response support to compromised federal agencies. We also worked with private sector entities who observed suspected or confirmed activity associated with this campaign.

CISA released guidance to help federal agencies eradicate the adversary from compromised on-premises and cloud environments. This guidance addresses tactics, techniques, and procedures leveraged by the threat actor and provides short- and intermediate-term actions that agencies should take to mitigate this activity and prevent future threat activity. By taking steps to evict this adversary from compromised on-premises and cloud environments, agencies will reduce the likelihood of persistent threat activity across their networks.

Long-Term Strategic Recovery and Rebuilding

In parallel with its immediate response and remediation efforts, CISA undertook a fourth line of effort to analyze the attack to obtain a deeper understanding of the underlying causes. CISA has identified strategic priorities needed to build federal IT networks that have cybersecurity capabilities fully aligned with leading practices. These priorities include cybersecurity intrusions that are rapidly detected via deep visibility at all levels of the technology environment. The impact of intrusions needs to be limited through the adoption of zero trust principles. In the coming months, CISA will work with federal civilian agencies to provide guidance, shared services, and assistance to advance toward an end state in which even the most sophisticated adversaries will face significant barriers to perpetrating sustained and damaging intrusions.

Helping Federal Departments and Agencies Recover

Mitigating Future Attacks

The impact of the recent cyber compromises is far reaching and reflects an urgent need to strengthen our nation's cyber defenses, invest in new capabilities, and fundamentally change how we think about cybersecurity. CISA is focused on three urgent strategic improvements.

First, we must increase CISA's visibility into cybersecurity risks across federal agencies and, where feasible, across non-federal entities. Second, we must expand CISA's incident response capacity. Third, we must drive adoption of defensible and resilient network architectures, including by providing broadly available shared services and progressing toward zero-trust environments.

Operational Visibility. We must increase and improve our visibility into federal agency networks, including on-premise and cloud environments. Traditionally, CISA's monitoring capabilities have been limited to internet network traffic, with agencies responsible for monitoring and detection within their on-premise and cloud environments. The recent incidents underscore the need for both CISA and individual agencies to have granular visibility into potential threats across the environment, from the endpoint to the cloud. Many federal agencies have accelerated cloud migration, a trend that we expect will continue. Recent compromises of federal agencies show that cloud resources are an attractive target to our most sophisticated adversaries. Across different cloud environments, security standards differ based on contracting decisions, vendor-specific offerings, and risk decisions. Along with providing technical capabilities to gain necessary visibility, CISA will work with OMB to drive adoption of stronger security controls. At the same time, we are maturing our capability to analyze risk in order to more effectively prioritize cybersecurity actions within individual agencies and across federal agencies. This requires new analytical capabilities that can rapidly adapt to our operators' needs, automate as much as possible, and provide a common operating picture. Addressing our top cyber risk priorities also requires greater collaboration, sharing of cyber threat information, and synchronized action across agencies and between the federal government and non-federal stakeholders.

Incident Response Capacity. We must continue to build our capacity to hunt for threats on agency networks and respond to incidents. While we are effectively responding today, this most recent attack should serve as a warning that federal government incident response must be fortified now to ensure that we will not be overwhelmed in the future. Going forward, we must shift to a model of automated, persistent threat hunting, enabled by authorities in the Fiscal Year 2021 National Defense Authorization Act, to more rapidly identify potential intrusions into federal civilian networks. We continue to expand our expert personnel dedicated to hunting for adversary activity through funding provided by Congress in the American Rescue Plan Act.

Defensible and Resilient Network and System Architectures. We must drive adoption of more defensible and resilient architectures, including modernization of outdated technologies that constrain adoption of effective cybersecurity controls. This progression will

enable agencies to take advantage of more advanced cybersecurity capabilities to protect against threat activity, more quickly detect lateral movement, and more readily isolate and remediate impacts within affected environments and systems. We will make progress toward this goal through provision of shared services, including offering secure cloud environments to agencies, expanding identity management efforts and cloud security efforts under the CDM program, and catalyzing progress toward zero-trust architectures.

Conclusion

Our nation faces exigent cybersecurity risks from a variety of adversaries. While federal agencies have been targeted in recent campaigns, many other organizations across our country, including critical infrastructure, have been similarly targeted. The most recent campaigns highlight our adversaries' sophisticated capabilities, patience, and persistence.

CISA's charge is clear: protect and defend the Federal government's networks through collaborative risk management. At the same time, we must be candid in our recognition that the status quo is unsustainable. We must apply the lessons learned from these recent incidents to urgently improve our capabilities while simultaneously raising the bar for long-term cybersecurity. By enhancing our visibility, implementing persistent hunt capabilities, increasing provision of shared services, and moving toward a zero-trust model, we can help to ensure that the Federal Government remains able to provide critical services to the American people under all conditions.

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