STATEMENT OF

RYAN A. HIGGINS

CHIEF INFORMATION SECURITY OFFICER AND
DEPUTY CHIEF INFORMATION OFFICER
OFFICE OF THE CHIEF INFORMATION OFFICER
OFFICE OF THE SECRETARY
DEPARTMENT OF COMMERCE

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT THE HEARING ENTITLED
“PREVENTION, RESPONSE, AND RECOVERY: IMPROVING
FEDERAL CYBERSECURITY POST-SOLARWINDS”

PRESENTED
MAY 11, 2021

Good morning Chairman Peters, Ranking Member Portman, and members of the Committee. Thank you for the invitation to appear before you today to provide an update on the Department of Commerce's incident response activities.

I serve as the Department's Chief Information Security Officer (CISO) and Deputy Chief Information Officer (DCIO) within the Office of the Chief Information Officer (OCIO). I joined the Department in March 2020, and provide leadership for the Department's cybersecurity program, which includes establishing policies and procedures for the Department and its bureaus in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), implementing enterprise cybersecurity functions, and coordinating incident response activities on behalf of the Department.

As the Cybersecurity and Infrastructure Security Agency's (CISA) Acting Director Brandon Wales testified at the Committee's previous hearing on the Solar Winds attack, a cybersecurity campaign affecting multiple Federal agencies, critical infrastructure providers, and private sector organizations was identified in early December 2020. The National Telecommunications and Information Administration (NTIA) identified indications of a potential systemic compromise related to this campaign and immediately engaged with the Department's OCIO to initiate incident response activities. As a result of this engagement, the Department was one of the first Federal agencies to identify potential systemic compromise in response to SolarWinds, determined that this was a major incident, and immediately initiated coordination with CISA to assist.

FISMA directs the Office of Management and Budget (OMB) to define the term "major incident" and requires agencies to notify Congress in the event of a major incident. As defined by OMB, major incidents include those that are likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.[1]

Based on what the Department knew concerning the potential systemic compromise, an initial review showed that it met the definition of a major cybersecurity incident. Within an hour of making this determination, the Department notified CISA and OMB. Subsequently, the Department, in accordance with Presidential Policy Directive 41 (PPD-41) sent a notification of a significant cybersecurity incident to the Federal Bureau of Investigation (FBI), CISA, and the Office of the Director of National Intelligence (ODNI) to request coordinated support. And, as required by FISMA, the Department notified Congress within seven days and subsequently provided more detailed information.

[1] Per Office of Management and Budget, Memorandum M-21-02 Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (Nov. 9, 2020), a major incident is defined as:

> "Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. . . . Or, a breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people."

The Department actively participated in the Cyber Unified Coordination Group (UCG) stood up in response to the SolarWinds incident, which supported information sharing and coordination across the government for all affected agencies.

Along with the hands-on assistance with respect to the identified compromise, CISA also released Emergency Directive (ED) 21-01 (*Mitigate SolarWinds Orion Code Compromise*), which provided guidance for the Department to further investigate and determine the scope of exposure at the Department bureaus beyond NTIA. The Department completed all required activities for ED 21-01, including the three supplemental guidance actions published following the initial release. Department and bureau representatives also regularly participated in CISA-hosted calls, which provided updated information about developments related to the incident.

In addition to CISA, the Department received assistance from the FBI and the Microsoft Detection and Response Team to investigate, remediate and recover from the SolarWinds incident. We have concluded our initial engagements with each of these partners and received recommendations from CISA and Microsoft to inform our immediate recovery activities.

Along with the remediation efforts in process by the Department and NTIA, the longer term recovery plan includes: (1) adopting and implementing Zero Trust[2] for migrating to a modern security architecture; (2) conducting Trusted Internet Connection 3.0[3] pilots to accelerate adoption of cloud, mobile and other emerging technologies; (3) upgrading security features in existing solutions and services to maximize capabilities; and (4) transitioning to cloud-centric models and replacing legacy on-premise infrastructure.

In closing, I want to emphasize that we remain in close coordination with our Federal partners to ensure we are sharing relevant information through established channels and continuously identifying opportunities to strengthen our cybersecurity posture. As we have seen, sophisticated threat actors are always trying to find ways to compromise our networks, and importantly the service providers many of us rely upon to meet our mission are a prime target for threat actors. We must work together to more effectively prevent or limit the impact of these incidents, and when they occur, act swiftly and responsibly to remediate and recover. Given the interconnected world in which we all live, it is imperative that we also continue to build on our partnerships with the private sector to ensure that the appropriate threat information is shared and resources are available to respond to these incidents.

While the immediate activities related to SolarWinds have moved from incident response to longer-term recovery, we must remain vigilant as the threat environment continues to evolve and our adversaries learn from these incidents just as we do.

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

[2] National Institute of Standards and Technology Special Publication 800-207, Zero Trust Architecture (August 2020), https://csrc.nist.gov/publications/detail/sp/800-207/final

[3] OMB Memorandum M-19-26, Update to the Trusted Internet Connections (TIC) Initiative (Sep. 12, 2019), https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf