

United States Senate

WASHINGTON, DC 20510

December 15, 2020

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001

Mr. Brandon Wales
Acting Director
Cybersecurity and Infrastructure Security
Agency
Department of Homeland Security
Washington, DC 20528

Dear Director Wray and Acting Director Wales,

We write to you today regarding the alarming initial reports of a “highly sophisticated, manual supply chain attack” allegedly conducted by nation state threat actors targeting various U.S. federal agencies and non-federal entities over a significant, yet undetermined period of time.¹ Identified in the press as APT29 or Cozy Bear, the threat actors alleged to be behind the attacks are believed to be part of the Foreign Intelligence Service of the Russian Federation (or SVR RF). The National Security Council, Cybersecurity and Infrastructure Security Agency (CISA), and impacted federal agencies have already taken significant steps to mitigate the harms highlighted in recent reports. CISA has ordered all federal government departments to identify and shut down the software-based vulnerability by 12:00 PM Eastern Standard Time on December 14, 2020.² We are seeking all available information on the scope and details of the recently exposed vulnerability’s impacts on the U.S. federal government.

SolarWinds’ Orion software products, specifically versions 2019.4 through 2020.2.1 HF1 according to CISA’s *Emergency Directive 21-01*, are being exploited by malicious foreign actors that “permits an attacker to gain access to network traffic management systems.” While initial reports pointed to the Department of Commerce and the Department of the Treasury as specific federal agencies implicated by the vulnerability, SolarWinds’ website indicates that its federal customers also include the Departments of Justice, Veterans Affairs, and Defense, among other federal entities.³ The aforementioned directive is not optional and mandates federal agency networks to remove the affected software components for the foreseeable future. While this initial protective step was taken and SolarWinds similarly issued a security advisory,⁴ Congress needs to be informed of the size, scope, and details of the cyberattack campaign’s impact on the federal government to appropriately respond to this risk.

¹ Christopher Bing, “Suspected Russian hackers spied on U.S. Treasury emails – sources,” *Reuters*, December 13, 2020, <https://www.reuters.com/article/us-usa-cyber-treasury-exclusive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUSKBN28N0PG?source=email>.

² U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Emergency Directive 21-01 – Mitigate SolarWinds Orion Code Compromise*, December 13, 2020, <https://cyber.dhs.gov/ed/21-01/>.

³ “IT Management and Monitoring Solutions for Government,” SolarWinds Government, accessed December 15, 2020, <https://www.solarwinds.com/federal-government/it-management-solutions-for-government>.

⁴ “SolarWinds Security Advisory,” SolarWinds, last modified December 15, 2020, <https://www.solarwinds.com/securityadvisory>.

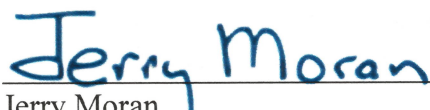
As members of the Senate Committee on Commerce, Science, and Transportation and the Senate Appropriations Subcommittee on Commerce, Justice, Science, and Related Agencies, our Committees oversee a wide number of federal agencies within our jurisdiction. We have oversight responsibilities to ensure that federal agencies within the Committees' respected jurisdictions uphold information security requirements established through the *Federal Information Security Modernization Act* and other relevant statutes. Under the *Federal Information Security Modernization Act*, the head of each federal agency is responsible for the security of its networks. The activities of the Department of Commerce, and one of its components that was impacted, the National Telecommunications and Information Administration, play a crucial role in the daily lives of all Americans, and compromising its efforts is of grave concern. However, the possible implications reach far beyond the specific federal agency jurisdiction of the Committees, including the private sector, and as such, we respectfully request complete and appropriately detailed answers to the following questions. We understand the investigations into this incident are preliminary and ongoing and so we expect that information will be shared as new details are learned.

1. Please list every federal agency that has identified in reporting to CISA that it is a customer of SolarWinds. Please identify the specific federal agencies that reported utilizing SolarWinds Orion software products, versions 2019.4 through 2020.2.1 HF1. Have agencies reported unauthorized access by a third party through the SolarWinds Orion products? If so, please identify the impacted agencies. Please describe the current status of each federal agency's compliance with *Emergency Directive 21-01*.
2. Of the federal agencies that have utilized SolarWinds Orion software products versions 2019.4 through 2020.2.1 HF1, please describe the specific categories and quantities of data, including classified information and sensitive personally identifiable information of taxpayers, and programs that were susceptible to unauthorized access as a result of the noted vulnerability. Please specifically note any confirmed cases of unauthorized access, retention, copying, using, transmitting, or otherwise processing of implicated categories of data.
3. How has CISA and the Federal Bureau of Investigation (FBI) organized their coordination efforts with the impacted federal agencies to support forensic analysis and investigative efforts related to unauthorized access? What role do the federal agencies or their Inspectors General play in the investigations?
4. Has the investigation of the impacted federal agencies identified any failures in implementation of the *Federal Information Security Modernization Act* or other relevant federal information security statutes? If so, please identify the pertinent statute or regulation. If not, will you commit to notifying Congress immediately if an implementation failure is later identified?
5. Please describe the assistance that SolarWinds has provided CISA, FBI, and its federal agency customers to address the information security concerns stemming from its Orion software products, specifically versions 2019.4 through 2020.2.1 HF1.

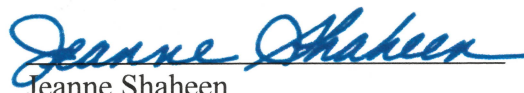
6. How will the investigative efforts of CISA and FBI assist the private sector customers of SolarWinds? Does the investigative scope include the impacted private sector entities? If not, does CISA and FBI plan to engage in specific information sharing efforts with the private sector customers to mitigate functional harms to their businesses and consumers? Please describe these efforts in as much detail as possible.

In addition to these questions, we ask that you arrange to brief our staff at the earliest possible opportunity. We understand under existing *Federal Information Security Modernization Act* guidance that our Committees will be briefed on this incident, and we thank you for your cooperation with us. Thank you for your attention to this matter. Please contact our staff with any questions or concerns.




Sincerely,



Jerry Moran
United States Senator



Jeanne Shaheen
United States Senator


John Thune
United States Senator
Richard Blumenthal
United States Senator
Roger F. Wicker
United States Senator
Maria Cantwell
United States Senator