RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS

United States Senate
WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, SUITE 304
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

http://blumenthal.senate.gov

Dec 23, 2020

The Honorable Robert Wilkie
Secretary of Veterans Affairs
810 Vermont Ave NW
Washington, DC 20420

Dear Secretary Wilkie,

I write regarding the troubling threat posed to the Department of Veterans Affairs (VA) by the backdoored version of SolarWinds network-monitoring software. According to the Cybersecurity and Infrastructure Security Agency (CISA), this backdoor, believed to be connected to Russian hackers, "poses a grave risk" to government agencies and private sector organizations and is "highly complex and challenging" to remove from networks. I am alarmed by the potential threat to the VA and write to urgently request information about the impact of this incident and what steps are being taken to ensure the resilience and confidentiality of the VA mission.

According to Microsoft, FireEye, and CISA, beginning in at least March 2020, sophisticated foreign actors compromised software updates for SolarWinds Orion to install a backdoor on thousands of customers' networks. This backdoor allowed the hackers a concerning toehold into federal networks, embedding them in sensitive resources, which could then be used to spy on communications and access data. While CISA issued an Emergency Directive on December 13, 2020 to shut down all SolarWinds products, this initial response is only a small step in the long road ahead to assess the damage of this catastrophic breach and to ensure that the hackers are fully kicked out of federal networks.

Alarmingly, the VA has been described as "the biggest spender on [SolarWinds Orion products] in recent years," raising deep concerns about the extent of its exposure and the impact on the sensitive data it holds on millions of veterans.[1] SolarWinds has repeatedly held out its work with VA as a model customer, in one press release stating it "helped the VA consolidate to a single enterprise-wide platform, implementing ten regional instances, putting everyone on the same page and giving consolidated visibility."[2] In effect, SolarWinds' statements raises the

[1] Thomas Brewster, "DHS, DOJ And DOD Are All Customers Of SolarWinds Orion, The Source Of The Huge US Government Hack," Forbes (New York City, New York), December. 14, 2020, https://www.forbes.com/sites/thomasbrewster/2020/12/14/dhs-doj-and-dod-are-all-customers-of-solarwinds-orion-the-source-of-the-huge-us-government-hack/?sh=4e3442725e68.

[2] Brandon Shopp, "One Platform to Rule Them All": How SolarWinds provided IT visibility across the VA's enterprise," Federal News Network (Washington, D.C.), October 30, 2019, https://federalnewsnetwork.com/innovation-in-government-success-stories/2019/10/one-platform-to-rule-them-all-how-solarwinds-provided-it-visibility-across-the-vas-enterprise/.

troubling prospect that the maliciously backdoored software was sitting at the heart of the VA, with unparalleled access to sensitive information.

I am disappointed that the VA has not been forthcoming about its exposure and investigation into the potential breach. VA initially agreed to brief Senate and House Veterans Affairs Committee staff this week, but canceled that briefing for unknown reasons. Therefore, Congressional oversight committees have no information as to what systems or data was compromised, including veterans' personal health information. As you are aware, the veteran community is particularly vulnerable to identity theft given the necessary reliance on the DD214– which contains a social security number and other sensitive information – to prove veteran status. This hack threatens to exacerbate existing privacy concerns and enable hackers to share and sell veterans' personal information.

I request VA answer the questions below immediately and also provide a staff-level briefing as soon as possible regarding the SolarWinds hack and its effects on VA and any other related, relevant issues.

1.) What VA components used SolarWinds Orion and how were those components potentially exposed to breach or unauthorized access by the backdoor versions of the product?

2.) Who at VA is responsible for doing incident response and forensics of VA assets believed to be exposed to the Orion backdoor? Is that forensic investigation underway, and what is the status?

3.) What precautions, such as network segmentation and other countermeasures, exist that would have isolated sensitive VA information, including health records, from breached VA assets?

4.) What monitoring does VA have in place to determine whether the Orion backdoor was activated, such as the EINSTEIN program or other log keeping systems?

5.) Does VA have any indications or evidence of an intrusion based on the Orion backdoor?

6.) Has VA conducted forensic investigations in response to additional recent advisories regarding related attacks on cloud resources, provided by the National Security Agency and CISA?

7.) Has VA encountered any suspicious cybersecurity activities and incidents since March 2020, including, but not limited to unauthorized access to email accounts or stored information?

    a. Have any of these cybersecurity incidents involved or affected VA activities in responding to the COVID-19 pandemic?

    b. Have any of these cybersecurity incidents affected or had the potential to affect direct patient care?

8.) If VA finds evidence of a breach involving veterans' personal information, how does it plan to identify and notify those affected?

Veterans must have confidence that VA can protect their sensitive health data, and VA must address what information was involved in the recent hack. I appreciate your immediate attention to this critical matter.

Sincerely,

RICHARD BLUMENTHAL
United States Senate