

January 20, 2021

Melinda Rogers  
Deputy Assistant Attorney General/Chief Information Officer  
Department of Justice  
Justice Management Division  
950 Pennsylvania Avenue, NW  
Room 1111  
Washington, DC 20530

Joseph R. Peters, Jr.  
Associate Director  
Administrative Office of the U.S. Courts  
One Columbus Circle, NE  
Washington, DC 20544

Dear Ms. Rogers, Mr. Peters:

We write regarding recent disclosures that the Department of Justice and the Administrative Office of the U.S. Courts (AO) were compromised by backdoored versions of SolarWinds network-monitoring software. According to the Cybersecurity and Infrastructure Security Agency (CISA), this backdoor “poses a grave risk” to government agencies and private sector organizations and is “highly complex and challenging” to remove from networks. U.S. intelligence and law enforcement agencies have concluded that the hack was likely Russian in origin.<sup>1</sup> We are alarmed at the potential large-scale breach of sensitive and confident records and communications held by the DOJ and AO, and write to urgently request information about the impact and the steps being taken to mitigate the threat of this intrusion.

According to Microsoft, FireEye, and CISA, beginning in at least March 2020, a sophisticated campaign compromised software updates for SolarWinds Orion to install a backdoor on tens of thousands of customers’ networks. This backdoor provided the hackers a concerning toehold into federal networks, embedding them in sensitive network locations, 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, the National Security Agency (NSA) and private sector customers have identified further tools and techniques also

---

<sup>1</sup> <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2021/item/2176-joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-the-office-of-the-director-of-national-intelligence-odni-and-the-national-security-agency-nsa>.

used by the SolarWinds hackers to break into victims networks and retain access.<sup>2</sup> Unfortunately, shutting down SolarWinds products 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.

The DOJ and the AO have acknowledged that they were among the federal agencies breached by Russian hackers, providing troubling accounts of the breadth and depth of the compromise. According to the DOJ, the Office of Chief Information Officer found malicious activity related to the campaign and determined that “the number of potentially accessed O365 mailboxes appears limited to around 3-percent” —which, given that DOJ has over 115,000 positions, could amount to thousands of email accounts within an agency tasked with profoundly sensitive law enforcement and national security missions.<sup>3</sup> Similarly, in a January 6<sup>th</sup> memorandum, the AO advised judges of an “apparent compromise of the confidentiality of the [Case Management/Electronic Case Filing (CM/ECF)] system due to these discovered vulnerabilities.” As the AO explains in its memo, the CM/ECF system is its “most sensitive and critical computer application” that stores sealed filings that “contain sensitive non-public information that, if obtained without authorization and improperly released, could cause harm to the United States, the Federal Judiciary, litigants, and others.”<sup>4</sup>

Given the grave national security threat of this catastrophic compromise, we urgently request a briefing about the steps that DOJ and AO are taking to clean up the breach, account for the damage, mitigate the harm, and improve organizational cybersecurity. In the interim, please respond to the following questions no later than January 31<sup>st</sup>:

- 1.) For DOJ, what records, email accounts, and other information have you determined were potentially exposed through the SolarWinds breach? What offices, divisions, or systems of the DOJ were targeted within the intrusion?
- 2.) For the AO, what aspects of the CM/ECF system were targeted within the intrusion (e.g., were specific courts targeted over others)? How many dockets were potentially exposed?

---

<sup>2</sup> <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2451159/nsa-cybersecurity-advisory-malicious-actors-abuse-authentication-mechanisms-to/>; <https://www.nytimes.com/2021/01/06/us/politics/russia-cyber-hack.html>.

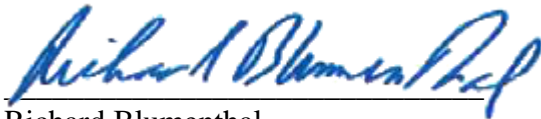
<sup>3</sup> <https://www.justice.gov/doj/page/file/1246841/download>;  
<https://www.justice.gov/opa/pr/departments-justice-statement-solarwinds-update>.

<sup>4</sup> <https://aboutblaw.com/UWL>.

United States Senate  
WASHINGTON, DC 20510

- 3.) Who at the DOJ and the AO are responsible for conducting incident response and forensics connected to this breach? Have the DOJ and AO been provided sufficient information to respond to the breach and do you have sufficient monitoring and logging to determine the extent of the compromise?
- 4.) What remedial actions have you taken to mitigate potential harms from the unauthorized access of sensitive information, particularly with respect to national security related information?
- 5.) What notice has been provided to investigators, prosecutors, and individuals whose personal information or records have been exposed in the course of the DOJ breach?
- 6.) What notice has been provided to judges and litigants whose sealed or non-public filings may have been exposed in the course of the CM/ECF breach?
- 7.) Has your organization identified any additional, non-SolarWinds methods where the adversary was able to access or compromise network authentication applications? If so, have you shared these with CISA?
- 8.) Please provide us with a specific timeline of significant events or actions taken by your organization in response to this incident.

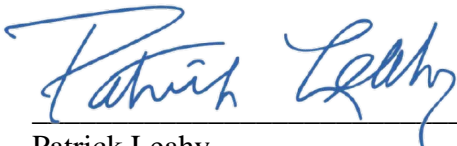
Sincerely,



Richard Blumenthal  
United States Senate



Dianne Feinstein  
United States Senate



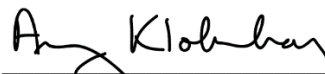
Patrick Leahy  
United States Senate



Richard J. Durbin  
United States Senate




Sheldon Whitehouse  
United States Senate



Amy Klobuchar  
United States Senate

United States Senate  
WASHINGTON, DC 20510



Chris Coons  
United States Senate



Mazie Hirono  
United States Senate



Cory A. Booker  
United States Senate