

**Congress of the United States**  
**Washington, DC 20515**

December 17, 2020

The Honorable John Ratcliffe  
Director of National Intelligence  
Office of the Director of National Intelligence  
1500 Tysons McLean Drive  
McLean, V.A. 22102

The Honorable Christopher Wray  
Director  
Federal Bureau of Investigation  
935 Pennsylvania Avenue, N.W.  
Washington, D.C. 20535

Mr. Chad Wolf  
Department of Homeland Security  
245 Murray Lane, S.W.  
Washington, D.C. 20528

Dear Director Ratcliffe, Director Wray, and Mr. Wolf:

Our Committees are seeking information related to the apparent, widespread compromise of multiple federal government, critical infrastructure, and private sector information technology networks. While investigations and technical forensic analyses are still ongoing, based on preliminary reporting, it is evident that this latest cyber intrusion could have potentially devastating consequences for U.S. national security.

On December 13, *Reuters* reported that “Hackers believed to be working for Russia have been monitoring internal email traffic at the U.S. Treasury and Commerce departments.”<sup>1</sup> In response, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, which ordered federal agencies to “disconnect or power down SolarWinds Orion products ... from their network[s].”<sup>2</sup> By December 15, the Department of Homeland Security, the Department of State, and the National Institutes of Health had also reportedly been affected by the breach.<sup>3</sup>

During a call with Congressional staff on December 14, CISA warned that the perpetrator of this attack is highly sophisticated, and that it will take weeks, if not months, to determine the total number of agencies affected by the attack and the extent to which sensitive data and information may have been compromised.<sup>4</sup> However, according to one U.S. official, this

---

<sup>1</sup> *Suspected Russian Hackers Spied on U.S. Treasury Emails - Sources*, Reuters (Dec. 13, 2020) (online at [www.reuters.com/article/us-usa-cyber-treasury-exclusive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG](http://www.reuters.com/article/us-usa-cyber-treasury-exclusive/exclusive-u-s-treasury-breached-by-hackers-backed-by-foreign-government-sources-idUSKBN28N0PG)).

<sup>2</sup> Cybersecurity and Infrastructure Security Agency, *Mitigate SolarWinds Orion Code Compromise* (Dec. 13, 2020) (online at <https://cyber.dhs.gov/ed/21-01/>).

<sup>3</sup> *DHS, State and NIH Join List of Federal Agencies — Now Five — Hacked in Major Russian Cyberespionage Campaign*, Washington Post (Dec. 14, 2020) (online at [www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff\\_story.html](http://www.washingtonpost.com/national-security/dhs-is-third-federal-agency-hacked-in-major-russian-cyberespionage-campaign/2020/12/14/41f8fc98-3e3c-11eb-8bc0-ae155bee4aff_story.html)).

<sup>4</sup> Telephonic Briefing with Acting Director Brandon Wales, Cybersecurity and Infrastructure Security Agency, to Congressional Members and Staff (Dec. 14, 2020).

The Honorable John Ratcliffe  
The Honorable Christopher Wray  
Mr. Chad Wolf  
Page 2

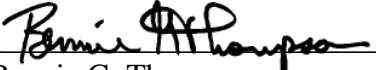
incident “is probably going to be one of the most consequential cyberattacks in U.S. history ... we’re dealing with something of a scale that I don’t think we’ve had to deal with before.”<sup>5</sup>

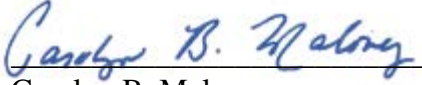
As the Committees of jurisdiction for U.S. cybersecurity preparedness and the defense of federal information technology systems, it is imperative that our Committees receive the latest information on the number of federal departments, agencies, and other entities affected by the breach, the extent to which sensitive information and data—including classified information—may have been compromised or exposed, the threat actor or actors responsible, and the Administration’s ongoing efforts to prevent further damage, secure its computer networks, and hold those responsible accountable.

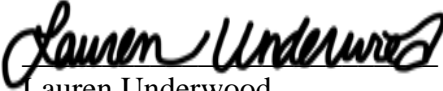
To that end, we ask that you provide our Committee Members with any damage assessments of this attack, including interim analyses, as soon as practicable. In addition, we look forward to a classified, interagency briefing on these matters on Friday, December 18, as previously discussed with your staffs beginning on Monday, December 14.

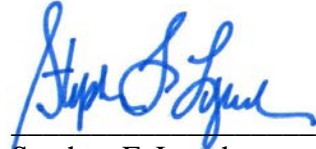
If you have any questions about this request, please contact Committee on Homeland Security staff at (202) 226-2616, or Committee on Oversight and Reform staff at (202) 225-5051.

Sincerely,

  
Bennie G. Thompson  
Chairman  
Committee on Homeland Security

  
Carolyn B. Maloney  
Chairwoman  
Committee on Oversight and Reform

  
Lauren Underwood  
Chairwoman  
Subcommittee on Cybersecurity,  
Infrastructure Protection, and Innovation  
Committee on Homeland Security

  
Stephen F. Lynch  
Chairman  
Subcommittee on National Security  
Committee on Oversight and Reform

---

<sup>5</sup> ‘Massively Disruptive’ Cyber Crisis Engulfs Multiple Agencies, Politico (Dec. 14, 2020) (online at [www.politico.com/news/2020/12/14/massively-disruptive-cyber-crisis-engulfs-multiple-agencies-445376](http://www.politico.com/news/2020/12/14/massively-disruptive-cyber-crisis-engulfs-multiple-agencies-445376)).

The Honorable John Ratcliffe  
The Honorable Christopher Wray  
Mr. Chad Wolf  
Page 3

cc: The Honorable Mike Rogers, Ranking Member  
Committee on Homeland Security

The Honorable James Comer, Ranking Member  
Committee on Oversight and Reform

The Honorable John Katko  
Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation  
Committee on Homeland Security

The Honorable Glenn Grothman, Ranking Member  
Subcommittee on National Security  
Committee on Oversight and Reform