United States Senate
WASHINGTON, DC 20510

June 22, 2015

The President
The White House
Washington, D.C. 20500

Dear Mr. President:

We write regarding the security of the information systems within the Executive Office of the President (EOP). Specifically, we are concerned that the EOP has not been meeting its obligation under law to report the status of its cybersecurity measures to Congress. Recently, we learned that the EOP has not submitted an annual information security review of its own systems to the Office of Management and Budget (OMB) or to the appropriate Congressional committees for at least the last three years. In addition, the last time OMB represented that it had received such a review was for fiscal year 2008.[1] Recent reports that the Office of Personnel Management suffered multiple significant intrusions,[2] resulting in the exposure of millions of employees' personal information, only underscore the importance for *every* federal agency, including the EOP, to take steps to improve its cybersecurity posture.

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), which you signed into law in December 2014, provides a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets."[3] As directed in the statute, all agencies, expressly including the EOP,[4] must implement a security program to take steps to secure their information and systems and comply with information security policies, procedures, standards, and guidelines, including those from OMB, the Department of Homeland Security, and the National Institute of Standards and Technology. All agencies, even agencies with sensitive

---

[1] Exec. Office of the President, Office of Management & Budget, *Fiscal Year 2008 Report to Congress on Implementation of The Federal Information Security Management Act of 2002* (Mar. 2009), at B2, *available at* https://www.whitehouse.gov/sites/default/files/omb/assets/reports/fy2008_fisma.pdf.
[2] Ellen Nakashima, *Chinese Breach Data of 4 Million Federal Workers*, WASH. POST, June 4, 2015, *available* at http://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html.
[3] *See* 44 U.S.C. § 3551 (amending 44 U.S.C. § 3541).
[4] "[T]he term 'agency' means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (***including the Executive Office of the President***), or any independent regulatory agency. . . ." *See* 44 U.S.C. § 3502 (emphasis added), which is applicable to the definitions under FISMA, 44 U.S.C. § 3552 (amending 44 U.S.C. § 3542).

information operating national security systems, must comply with the requirement to report on information security performance. Separate processes and proper protections can be employed for reporting on those systems.[5] As cybersecurity risks and threats to agencies grow and evolve, however, Congress and OMB must be able to assess the effectiveness of agencies' security efforts through required compliance reviews and reports.[6]

As Chairman Thune noted in his April 30, 2015, letter to you, for which a response is still outstanding, recent reports of a malicious cyber intrusion into the White House computer system underscore the importance of initiatives to protect federal information and networks. Moreover, improving cybersecurity in Executive Branch departments and agencies is a shared goal, and we look forward to working with you to ensure EOP's compliance with FISMA. To assure Congress and the American public that the EOP and its components are making every effort to prioritize the security of its systems, we ask that you provide responses to the following questions as soon as possible, but by no later than July 13, 2015.

1. Does the EOP comply with the security requirements and standards under FISMA for all information collected or maintained by or on behalf of the agency and all information systems used or operated by the agency or on behalf of the agency?

2. Why has the EOP failed to comply with the reporting requirements under FISMA?

3. Has the EOP undertaken the independent evaluations required under FISMA or any other similar information security reviews or audits?

Thank you for your cooperation and prompt attention to this matter.

Sincerely,

JOHN THUNE
Chairman
Committee on Commerce,
Science, and Transportation

RON JOHNSON
Chairman
Committee on Homeland
Security and Governmental Affairs

---

[5] *See* Memorandum from Sylvia M. Burwell, Director, Office of Management & Budget, M-14-04 (Nov. 18, 2013), at 4, *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf.

[6] Under FISMA, all agencies, including the EOP, must provide assessments annually to the OMB Director, the Senate Committees on Homeland Security and Government Affairs and Commerce, Science, and Transportation, and the House of Representatives Committees on Oversight and Government Reform and Science, Space, and Technology, the appropriate authorization and appropriations committees of Congress, and the Comptroller General. In December 2014, P.L. 113-282 added the Secretary of Homeland Security and the House Committee on Homeland Security to the list of report recipients. *See* 44 U.S.C. § 3554 (amending 44 U.S.C. § 3544).

cc: The Honorable Bill Nelson, Ranking Member
Committee on Commerce, Science, and Transportation

The Honorable Thomas R. Carper, Ranking Member
Committee on Homeland Security and Governmental Affairs