United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 6, 2016

The Honorable Shaun Donovan
Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Director Donovan:

The Government Accountability Office ("GAO") recently released a report examining cybersecurity threats and information security practices of federal agencies responsible for high-impact systems.[1] GAO found that the eighteen agencies with high-impact systems reported that foreign nations[2] were "the most serious and most frequently-occurring threat to the security of their systems."[3]

In all, the agencies reported 2,267 incidents involving high-impact systems including 500 cases where malicious code was installed.[4] The persistent threat from nation-state actors and other cyber adversaries highlights the importance of securing all federal information systems and particularly those that have been identified as high-impact—particularly given the serious implications for federal government operations and affected individuals.[5]

Pursuant to the Federal Information Security Modernization Act of 2014 ("FISMA"),[6] the Office of Management and Budget ("OMB") is responsible for overseeing agency information security policies and practices. In its audit report, GAO recommended that OMB issue the updated Appendix III of Circular A-130, which was required to be completed by December 18, 2015 pursuant to FISMA[7] to streamline federal agency reporting of cybersecurity monitoring and audits, and to issue "the plan and practices specified in the *Cybersecurity Strategy and Implementation Plan*."[8]

---

[1] GOVERNMENT ACCOUNTABILITY OFFICE, GAO-16-501, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE CONTROLS OVER SELECTED HIGH-IMPACT SYSTEMS (May 2016), *available at: http://www.gao.gov/products/GAO-16-501*.

[2] *Id.* GAO described nations as: "including nation-state, state-sponsored, and state-sanctioned programs" which "use cyber tools as part of their information-gathering and espionage activities." *Id.* at 10

[3] *Id.* at 10.

[4] *Id.*

[5] *Id.* GAO describes high-impact systems as those "where the loss of confidentiality, integrity, or availability can have a severe or catastrophic adverse effect on organizational operations, assets, or individuals," and that "such an impact can result in loss or degradation of mission capability, severe harm to individuals or major financial loss."

[6] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3087.

[7] *Id.*

[8] GOVERNMENT ACCOUNTABILITY OFFICE, GAO-16-501, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE CONTROLS OVER SELECTED HIGH-IMPACT SYSTEMS (May 2016), *available at: http://www.gao.gov/products/GAO-16-501*.

We previously wrote to you about this issue on April 26, 2016.[9] We now are writing to learn the status of the required update to Circular A-130, reiterate our request for quarterly briefings, and understand your response to the findings of the GAO report. Accordingly, please provide the following information:

1. On what date will OMB issue final revisions to Circular A-130?

2. When does OMB plan to issue the plan and practices in the Cybersecurity Strategy and Implementation Plan, including plans for federal security operations center best practices as well as for shared services?[10]

3. Please describe other actions that OMB is taking to address the findings of this GAO report and to direct federal agencies to take actions to improve security of high-impact systems.

Please provide this information as soon as possible, but we request that you provide a response by no later than July 21, 2016.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[11] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes…."[12] For purposes of this request, please refer to the definitions and instructions in the enclosure.

If you have any questions about this request, please have your staff contact Dan Lips or Matt Grote at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

Thomas R. Carper
Ranking Member

---

[9] Letter from Hon. Ron Johnson, Chairman, and Hon. Thomas Carper, Ranking Member, S. Homeland Sec. & Governmental Affairs Comm., to Hon. Shaun Donovan, Dir., Office of Mgmt. & Budget (Apr. 26, 2016).

[10] GOVERNMENT ACCOUNTABILITY OFFICE, GAO-16-501, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE CONTROLS OVER SELECTED HIGH-IMPACT SYSTEMS (May 2016), *available at: http://www.gao.gov/products/GAO-16-501.*

[11] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).

[12] S. Res. 73 § 12, 114th Cong. (2015).