

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<http://oversight.house.gov>

March 28, 2017

The Honorable Mick Mulvaney
Director
Office of Management and Budget
1800 G Street, 9th Floor
Washington, D.C. 20503

Dear Director Mulvaney:

We are writing to request information on the status of guidance that the Office of Management and Budget (OMB) had been developing to assist agencies in their efforts to improve cybersecurity protections in federal acquisitions.

As the Committee's 2015 to 2016 investigation into the data breaches at the Office of Personnel Management (OPM) made clear, an important component in improving the government's information security includes strengthening the cybersecurity protections in the contracts it enters into with contractors. Indeed, the Majority staff report and Minority staff memorandum on the investigation expressly recognized the urgent need for OMB to strengthen and improve cybersecurity requirements for federal contractors.¹

In January 2014, the General Services Administration and the Department of Defense delivered a report, entitled *Improving Cybersecurity and Reliance through Acquisition* that made recommendations aimed at incorporating cybersecurity requirements into the federal acquisition process.² For example, this report recommended instituting baseline cybersecurity requirements as a condition of award for certain acquisitions and developing common cybersecurity definitions for federal acquisitions. This report provided general recommendations for incorporating cybersecurity into the federal acquisition process.

¹ Majority Staff, House Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, at 24-25 (Sept. 2016) (online at <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>); Memorandum from Democratic Staff to Democratic Members of the House Committee on Oversight and Government Reform, Committee Investigation into the OPM Data Breach, at 11-17 (Sept. 6, 2016) (online at <https://democrats-oversight.house.gov/news/press-releases/cummings-releases-staff-memo-on-cyber-attacks-against-opm>).

² Gen. Serv. Admin. & Dep't of Defense, *Improving Cybersecurity and Resilience Through Acquisition* (Nov. 2013) (online at http://www.gsa.gov/portal/mediaId/185367/fileName/improving_cybersecurity_and_resilience_through_acquisition.action).

Subsequent to this report, OMB released proposed guidance on cybersecurity for federal contractors for public comment in August 2015, and requested feedback on the guidance by September 10, 2015.³ The goal of this proposed OMB guidance was “to take major steps toward implementing strengthened cybersecurity protections in [f]ederal acquisitions and therefore mitigating the risk of potential incidents in the future.”⁴ The guidance proposed to achieve this goal by “strengthen[ing] government agencies’ clauses regarding the type of security controls that apply, notification requirements for when an incident occurs, and the requirements around assessments and monitoring of systems.”⁵ At the time, OMB announced final guidance would be issued after the closing of the public feedback period.⁶ To date, however, OMB has not finalized this guidance.⁷

Given the critical need for implementing strengthened cybersecurity protections in the federal acquisition process and the current lack of clear guidance for agencies on this topic, we request that you provide the Committee with an update on any such guidance under development. Further, if there is no specific guidance under development at this time, we ask that you provide a strategy or plan for developing guidance for agencies to improve and update cybersecurity requirements for federal acquisition. The strategy or plan should include milestones and stakeholder outreach information.

Please provide a response to this request by April 10, 2017, and have your staff contact Julie Dunne of the Majority staff at (202) 225-5074, or Tim Lynch of the Minority staff at (202) 225-5051, with any questions about this request. Thank you for your prompt attention to this matter.

Sincerely,



Will Hurd
Chairman
Subcommittee on Information Technology



Robin L. Kelly
Ranking Member
Subcommittee on Information Technology

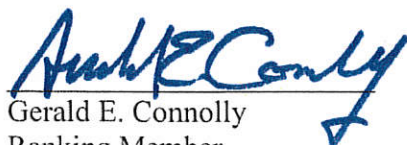
³ Office of Management and Budget, Office of the Federal Chief Information Officer, *Draft Federal Technology Policies, Improving Cybersecurity Protections in Federal Acquisitions* (online at <https://policy.cio.gov/cybersecurity-protections-in-federal-acquisitions/>) (accessed Mar. 10, 2017).

⁴ *Id.*

⁵ *Id.*

⁶ See generally *id.* (discussing the timeframe for public feedback and final issuance of the proposed guidance).

⁷ *Id.*

A handwritten signature in blue ink, reading "Gerald E. Connolly". The signature is stylized, with the first name "Gerald" and last name "Connolly" clearly legible, and "E." as a small middle initial.

Gerald E. Connolly
Ranking Member
Subcommittee on Government Operations