EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 14, 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

I am providing you with an assessment of intrusion detection and intrusion prevention capabilities across the Federal enterprise pursuant to Section 226(c)(1)(C) of the Federal Cybersecurity Enhancement Act of 2015 (Pub. L. No. 114-113, 129 Stat. 2242, 2970 (2016)).

The Office of Management and Budget (OMB) acknowledges that there is a need to enhance existing capabilities and programs to better safeguard Federal information systems and data, and we plan to convey this vision as part of the President's 2020 Budget. In order to inform future investment decisions, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) is working on a threat-based security architecture assessment. This threat-based security approach, adopted from the Department of Defense, will provide a holistic assessment of existing Federal cybersecurity capabilities and creates a common framework to discuss and assess cybersecurity capabilities related to threats. The results are being used to inform DHS' cybersecurity investment priorities across Federal civilian departments and agencies in order to enhance enterprise cybersecurity and reduce risk.

Key to the future state of DHS' cybersecurity services is the integration of the National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) programs. Integration of these key programs – in conjunction with the threat-based capability prioritization – allows for DHS to invest in enterprise-wide services through NCPS, while taking a more targeted approach to standardizing agency cybersecurity baselines and capabilities through CDM. We continue to work with DHS as they evolve their programs and capabilities and look forward to working with Congress on the proposal after the release of the 2020 Budget. In the interim, we are providing details about what we know about the effectiveness of intrusion detection and intrusion prevention capabilities across the government.

OMB recently published *The Cybersecurity Risk Determination Report and Action Plan*, which provides a comprehensive review of the cyber risk management programs across the government in support of Executive Order 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The report found that Federal agencies do not possess or properly deploy capabilities to detect or prevent intrusions or minimize the impact of intrusions when they occur.

Congress appropriated $468M in FY 2017 and $402M in FY 2018 for NCPS. NCPS deployed $118M of FY 2017 funding and plans to execute $141M of FY 2018 funding to deploy intrusion detection and prevention capabilities through the EINSTEIN sensor suite, which includes EINSTEIN 1 (E1), EINSTEIN 2 (E2), and EINSTEIN 3 Accelerated (E3A). All Chief

Financial Officer (CFO) Act agencies have deployed at least one of the E3A countermeasures. In the FY 2017 Annual FISMA Report to Congress, we noted that, from January 2016 through April 2017, NCPS detected 1,600 of the 44,823 incidents across Federal civilian networks via the EINSTEIN sensor suite. In addition, NCPS detected 379 of the 39,171 incidents across Federal civilian networks via the EINSTEIN sensor suite from April 2017 to present.

DHS reports that the majority of department and agencies have deployed one of the two E3A countermeasures (email filtering or DNS sinkholing). Email filtering has proven the more challenging of the two to deploy due to the wide range of agency email configurations, including the use of cloud-based email. However, DHS and agencies continue to work to find technical solutions that address the capability requirements of EINSTEIN. Furthermore, DHS's service providers, cloud email service providers, and the Federal Agencies continue to evaluate solutions that enable E3A email filtering adoption.

DHS' recently published Cybersecurity Strategy acknowledges the need to improve the effectiveness of its programs to address the greatest risks first and focus on the highest impact systems, assets, and capabilities, and ensuring maximum return on investment. The threat-based security architecture assessment will begin to address this need, but additional work is needed. OMB concurs with the DHS view on the need to improve program effectiveness and supports an evaluation of enhanced tool sets that would better align with the current and future state of Federal IT, provide additional capabilities to protect the Federal civilian departments and agencies, and maintain cybersecurity situational awareness across the enterprise.

In addition, the Administration is actively working with agencies to execute various information technology (IT) modernization efforts and implementing improved cybersecurity capabilities, as part of Executive Order 13800 and the President's Management Agenda. Specifically, OMB is tracking intrusion detection and prevention capabilities within the Modernize IT to Increase Productivity and Security Cross-Agency Priority goal in response to the findings in *The Risk Determination Report and Action Plan*, and 10 of 23 CFO act agencies have already implemented the capabilities in this goal. OMB will provide the public with quarterly progress updates via Performance.gov on a quarterly basis. We will also provide future updates on intrusion detection and intrusion prevention capabilities via OMB's annual Federal Information Security Modernization Act of 2014 (FISMA) reports.

If you have any questions regarding the contents of this letter, please contact OMB's Office of Legislative Affairs at LegislativeAffairs@omb.eop.gov.

Sincerely,

Suzette Kent
Federal Chief Information Officer
Office of e-Government and Information Technology

Identical Letter Sent to:

The Honorable Michael McCaul
The Honorable Bennie G. Thompson
The Honorable Ron Johnson
The Honorable Claire McCaskill
The Honorable Trey Gowdy
The Honorable Elijah Cummings
The Honorable John Thune
The Honorable Bill Nelson
The Honorable Lamar Smith
The Honorable Eddie Bernice Johnson
The Honorable Gene L. Dodaro