OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
WASHINGTON, DC 20511

15 September 2015

The Honorable Ron Wyden
221 Dirksen Senate Office Building
Washington DC 20510

Dear Senator Wyden:

Thank you for your August 12, 2015 letter asking for information about what role the National Counterintelligence and Security Center (NCSC) may have had in reviewing or advising the Office of Personnel Management (OPM) on OPM's network security before the recently reported OPM security incidents. Specifically you asked:

1. Did the NCSC identify OPM's security clearance database as a counterintelligence vulnerability prior to these security incidents?
2. Did the NCSC provide OPM with any recommendations about how to secure this information?
3. At least one official has said that the background investigation information compromised in the second OPM hack included information on individuals as far back as 1985. Has the NCSC evaluated whether the retention requirements for background investigation information should be reduced to mitigate the vulnerability of maintaining personal information for a significant period of time? If not, please explain why existing retention periods are necessary.

In response to the first two questions, under the statutory structure established by the Federal Information Security Management Act of 2002 (FISMA), as amended, executive branch oversight of agency information security policies and practices rests with the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). For agencies with Inspectors General (IG) appointed under the Inspector General Act of 1978 (OPM is one of those agencies), independent annual evaluations of each agency's adherence to the instructions of OMB and DHS are carried out by the agency's IG or an independent external auditor chosen by the agency's IG. These responsibilities are discussed in detail in OMB's most recent annual report to Congress on FISMA implementation. The statutory authorities of the National Counterintelligence Executive, which is part of the NCSC, do not include either identifying information technology (IT) vulnerabilities to agencies or providing recommendations to them on how to secure their IT systems.

In response to the third question, the timelines for retention of personnel security files were established by the National Archives General Records Schedule 18, Item 22 (September 2014). While it is possible that we may incur certain vulnerabilities with the retention of background investigation information over a significant period of time, its retention has value for personnel security purposes. The ability to assess the "whole person" over a long period of time enables security clearance adjudicators to identify and address any issues (personnel security or counterintelligence-related) that may exist or may arise.

The Honorable Ron Wyden

Please contact Ms. Deirdre M. Walsh, Director of the Office of Legislative Affairs, at 703-275-2474 if you have any additional questions regarding this matter.

Sincerely,

William R. Evanina