

August 12, 2015

Director William Evanina
National Counterintelligence Executive
National Counterintelligence and Security Center
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Evanina:

The National Counterintelligence and Security Center (NCSC) is tasked with a very important mission, which includes defending the nation's classified information and assets from exploitation by foreign adversaries. The importance of this mission has recently been underscored by compromises of sensitive US government personnel data.

In April 2015, the Office of Personnel Management (OPM) announced that that it had been the target in the first of two security incidents. The first security incident affected 4.2 million current federal employees and included personal information such as names, birth dates, home addresses and Social Security numbers. In June 2015, OPM announced a second security incident affecting 21.5 million individuals—including current, former, and prospective employees and their relatives and associates—had compromised sensitive background investigation information and, in some cases, fingerprints. This information could clearly be of significant value to foreign intelligence services.

There appear to have been significant warning signals regarding the security of OPM's networks, including a report from the OPM Inspector General that specifically noted weaknesses in two of OPM's systems that support suitability and security clearance determinations.

The fact that such sensitive information was not adequately protected raises real questions about how well the government can protect personnel information in the future, especially as the security clearance process moves toward conducting ongoing evaluations and incorporating publicly available electronic information.

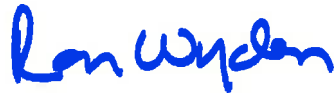
I would like to know what actions the NCSC took prior to these OPM security incidents and what the NCSC will be doing to prepare for future attacks that will similarly target personnel and background investigation information. Specifically, I ask that you answer the following questions:

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 at 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.

Strong cybersecurity protections are obviously an essential part of effective counterintelligence, and thoughtful risk management is the best way to ensure both. I appreciate your attention to this important matter, and I look forward to your response.

Sincerely,

A handwritten signature in blue ink that reads "Ron Wyden". The signature is fluid and cursive, with the first letters of "Ron" and "Wyden" being capitalized and prominent.

Ron Wyden
United States Senator