Cyber Intrusion Compromise of OPM Personnel Records

July 10, 2015

Dear Colleagues,

I am writing to provide an update on the recent cyber incidents at the U.S. Office of Personnel Management (OPM). We are committed to providing you updates as soon as they are available and we are reaching out today to share updated information from OPM. The information below can be found on OPM's new, online incident resource center – *https://www.opm.gov/cybersecurity*. This site will offer information regarding the OPM incidents and will direct individuals to materials, training, and useful information on best practices to secure data, protect against identity theft, and stay safe online.

Update from OPM:

Today, the U.S. Office of Personnel Management (OPM) announced the results of the interagency forensics investigation into a recent cyber incident involving Federal background investigation data and the steps it is taking to protect those impacted. The Department of State and OPM will continue to provide additional information going forward.

Background on the intrusion into OPM's systems. Since the end of 2013, OPM has undertaken an aggressive effort to upgrade the agency's cybersecurity posture, adding numerous tools and capabilities to its various legacy networks. As a direct result of these steps, OPM was able to identify two separate but related cybersecurity incidents on its systems.

Today, OPM announced the results of the interagency forensic investigation into the second incident. As previously announced, in late-May 2015, as a result of ongoing efforts to secure its systems, OPM discovered an incident affecting **background investigation records** of current, former, and prospective Federal employees and contractors. Following the conclusion of the forensics investigation, OPM has determined that the types of information in these records include identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history; and other. Some records also include findings from interviews conducted by background investigators and fingerprints. (NB: If an individual underwent a background investigation done by Diplomatic Security the background investigation records are held only by Diplomatic Security.) Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

While background investigation records do contain some information regarding mental health and financial history provided by those that have applied for a security clearance and by individuals contacted during the background investigation, there is no evidence that separate

systems that store information regarding the health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

This incident is separate but related to a previous incident, discovered in April 2015, affecting **personnel data** for current and former Federal employees. OPM and its interagency partners concluded with a high degree of confidence that personnel data for 4.2 million individuals had been stolen. This number has not changed since it was announced by OPM in early June, and OPM has worked to notify all of these individuals and ensure that they are provided with the appropriate support and tools to protect their personal information.

Analysis of background investigation incident. Since learning of the incident affecting background investigation records, OPM and the interagency incident response team have moved swiftly and thoroughly to assess the breach, analyze what data may have been stolen, and identify those individuals who may be affected. The team has now concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants. As noted above, some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. There is no information at this time to suggest any misuse or further dissemination of the information that was stolen from OPM's systems.

If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P for a new investigation or periodic reinvestigation), it is highly likely that the individual is impacted by this cyber breach. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely. (NB: If an individual underwent a background investigation done by Diplomatic Security the background investigation records are held only by Diplomatic Security.)

Assistance for impacted individuals. OPM is also announcing the steps it is taking to protect those impacted:

1. **Providing a comprehensive suite of monitoring and protection services for background investigation applicants and non-applicants whose Social Security Numbers, and in many cases other sensitive information, were stolen** – For the 21.5 million background investigation applicants, spouses or co-habitants with Social Security Numbers and other sensitive information that was stolen from OPM databases, OPM and the Department of Defense (DOD) will work with a private-sector firm specializing in credit and identity theft monitoring to provide services such as:
    - Full service identity restoration support and victim recovery assistance

- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

The protections in this suite of services are tailored to address potential risks created by this particular incident, and will be provided for a period of at least 3 years, at no charge.

In the coming weeks, OPM will begin to send notification packages to these individuals, which will provide details on the incident and information on how to access these services. OPM will also provide educational materials and guidance to help them prevent identity theft, better secure their personal and work-related data, and become more generally informed about cyber threats and other risks presented by malicious actors.

2. **Helping other individuals who had other information included on background investigation forms –** Beyond background investigation applicants and their spouses or co-habitants described above, there are other individuals whose name, address, date of birth, or other similar information may have been listed on a background investigation form, but whose Social Security Numbers are not included. These individuals could include immediate family members or other close contacts of the applicant. In many cases, the information about these individuals is the same as information generally available in public forums, such as online directories or social media, and therefore the compromise of this information generally does not present the same level of risk of identity theft or other issues.

   The notification package that will be sent to background investigation applicants will include detailed information that the applicant can provide to individuals he or she may have listed on a background investigation form. This information will explain the types of data that may have been included on the form, best practices they can exercise to protect themselves, and the resources publicly available to address questions or concerns.

3. **Establishing an online cybersecurity incident resource center –** Today, OPM launched a new, online incident resource center - located at https://www.opm.gov/cybersecurity - to offer information regarding the OPM incidents as well as direct individuals to materials, training, and useful information on best practices to secure data, protect against identity theft, and stay safe online. This resource site will be regularly updated with the most recent information about both the personnel records and background investigation incidents, responses to frequently asked questions, and tools that can help guard against emerging cyber threats.

4. **Establishing a call center to respond to questions** – In the coming weeks, a call center will be opened to respond to questions and provide more information. In the interim, individuals are encouraged to visit https://www.opm.gov/cybersecurity. Individuals will not be able to receive personalized information until notifications begin and the call center is opened. OPM recognizes that it is important to be able to provide individual assistance to those that reach out with questions, and will work with its partners to establish this call center as quickly as possible.

5. **Protecting all Federal employees –** In the coming months, the Administration will work with Federal employee representatives and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

In conclusion, I want you to know that I am as concerned about these incidents as you are, and we want to ensure you that we are in constant contact with OPM. The Department of State's entire leadership is committed to providing you with the most recent resources and support, and we want to keep on hearing from you. Please keep sending your feedback and questions to DGDirect@state.gov. Thank you.