Version 3
August 6, 2015

OPM Cyber Incidents
Talking Points for DOE Leadership

Summary

- OPM has identified ***two cyber-security incidents*** that impacted the data of Federal government employees, contractors, and others:
    - Personnel Records Incident that affected the personnel data of 4.2 million current and former federal employees.
    - Background Investigations Records Incident that affected the sensitive information of 21.5 million individuals, to include federal employees, contractors, and others.

- Separate from the cyber incidents, OPM identified vulnerability in the Electronic Questionnaires for Investigations Processing (e-QIP) system, and temporarily took this system offline to facilitate the implementation of security enhancements. OPM has completed these enhancements, and, after extensive testing, the e-QIP system has been brought back online.

- OMB has led a Cybersecurity Sprint in the wake of the OPM incident to address key cybersecurity capabilities across the government. The sprint focuses on the implementation of multi-factor authentication for both privileged and standard users, the addressing of vulnerabilities identified through DHS scanning, and the identification of 'high value assets' to include systems containing PII.

Key Talking Points

❖ ***Personnel Records Incident***

- On June 4, OPM announced that the personnel data of 4.2 million current and former federal employees had been compromised.

- Notifications for this incident are complete.

- If an individual has not received notification or misplaced the notification, they should contact CSID at 844-222-2743 to verify whether they should have received notification. Employees will need to provide CSID with their name and last four digits of their SSN to determine their status.

- OPM is offering the following services through CSID for a period of 18 months as a result of this incident:
    - Credit report access (must enroll to receive)
    - Credit monitoring (must enroll to receive)
    - Identity monitoring (must enroll to receive)
    - Identity theft insurance (automatic enrollment)
    - Identity restoration services (automatic enrollment)

❖ ***Backgrounds Investigations Records Incident***

- On June 12, OPM announced a second breach involving systems that contain background investigation records. OPM identified that sensitive information of 21.5 million individuals, to include former, current, and prospective federal employees, contractors, and others, including spouses/co-habitants of background investigation applicants, was compromised.

- If an individual underwent a background investigation through OPM in 2000 or afterwards, it is highly likely that the individual is impacted by this breach. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely.

- Notifications for this incident have NOT yet occurred. It is anticipated that notifications will begin in mid-September and continue through December.
    - More information on the method by which notifications will be provided and the content of the notifications will be

- The following services are anticipated to be available to impacted individuals for a period of three years, not to exceed December 31, 2018:
    - Credit monitoring (must enroll to receive)
    - Credit reports (must enroll to receive)
    - Identity monitoring (must enroll to receive)
    - Identity theft insurance (automatic enrollment)
    - Identity restoration services (automatic enrollment)

- The protection and monitoring services will also be made available to currently minor, dependent children of the impacted individuals.

❖ ***e-QIP Suspension***

- OPM identified vulnerability in the Electronic Questionnaires for Investigations Processing (e-QIP) system, and temporarily took this system offline.

- OPM has conducted security enhancements in the system, and, after extensive testing, the e-QIP system has been brought back online.

❖ ***Phishing Attempts***

- Employees should be aware of phishing attempts and should never provide sensitive or personal information over the phone, internet, texts, or emails. Following are examples of recent phishing attempts related to the OPM cyber incidents:

    - FTC Phone Scam: The Federal Trade Commission (FTC) has identified a phone scam related to the OPM cyber incidents in which individuals are receiving a phone call from an individual claiming he is with the FTC and has money for victims of the cyber breaches. Employees should

NOT provide any information - the FTC will never call and ask for personally identifiable information, such as social security or bank account numbers.

- USAJOBS Phishing Scam: OPM has provided warnings about email scams purporting to come from the Federal government's USAJOBS website. The USAJOBS system will not send emails requesting that users validate account information. Employees should not click on links in these phishing attempts.

Additional Information / Background

❖ ***Cyber Incidents, Generally***

- OPM recently became aware of malicious activity affecting information technology (IT) systems and data and partnered with the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation to determine the impact to Federal personnel.

- OPM became aware of the intrusion in April 2015, and worked with US-CERT to assess the extent of the malicious activity and to identify records that may have been compromised. As with any such event, it takes time to conduct a thorough investigation and to identify affected individuals.

❖ ***Personnel Records Incident***

- OPM identified that the personally identifiable information (PII) of approximately 4 million current and former Federal employees across Executive Branch agencies may have been exposed in this incident.

- OPM maintains personnel records for the Federal workforce. The kind of data that may have been compromised in this breach could include employee names, Social Security Numbers, date and place of birth, and current and former addresses.

- From June 8 through June 19, 2015, OPM provided notifications to individuals affected by this incident via email and the U.S. Postal Service. All employees affected should have received notification at this point. If an individual believes they are affected and has not received notification, they should contact CSID at 844-222-2743 (International callers: call collect 512-327-0700) to verify whether they should have received notification. Employees will need to provide CSID with their name and last four digits of their SSN to determine their status.

- OPM is offering individuals affected by the Personnel Records incident credit monitoring services and identity theft insurance through CSID, a company that specializes in identity theft protection and fraud resolution. This 18-month membership includes credit report access, credit monitoring, identity theft insurance and recovery services and is available immediately at no cost to affected individuals identified by OPM.

- Employees need to opt in to receive the credit monitoring services.
- Every affected individual, regardless of whether or not they take action to enroll, will automatically receive $1 million of identity theft insurance and access to full-service identity restoration provided by CSID.
- Employees with questions about credit reporting and monitoring, theft protection, fraud, etc. may contact CSID directly, beginning at 8:00 a.m. CST on June 8, 2015, at www.csid.com/opm or 844-222-2743 (International callers: call collect 512-327-0700). Employees are encouraged to wait to call CSID until receiving their individual notification from OPM/CSID, as this notice will include a unique PIN for use with CSID.

- CSID is working on the personnel records incident only and does not have further information about the background investigations records incident.

❖ ***Background Investigations Records Incident***

- In May, OPM discovered an incident affecting background investigation records of current, former, and prospective Federal employees and contractors. OPM has 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.

- There is an overlap of ~3.6M individuals affected by the personnel records incident and the background investigations incident

- 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.

- The types of information in these records include:
  - Identification details, including 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 details
  - Some records also include findings from interviews conducted by background investigators and fingerprints
  - Usernames and passwords that background investigation applicants used to fill out their background investigation forms

- OPM will provide a suite of monitoring and protection services for background investigation applicants and non-applicants whose SSNs were stolen, which generally includes applicants, spouses, and co-habitants.
  - OPM and the Department of Defense (DOD) will work with private-sector firm(s) 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
    - These services will be provided for at least three years at no charge to the employee.

- Beyond background investigation applicants and their spouses or co-habitants, 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. Information will be made available to these individuals to explain the types of data that may have been included on the form, best practices they can exercise to protect themselves, and publicly available resources to address questions or concerns.

- OPM is still working through determining the details for the notification process following the background investigations records cyber security incident, but has provided some information to agencies:
    - No notifications have occurred to date.
    - In the coming weeks, OPM (likely via the Department of Defense) will begin sending notification letters to individuals whose SSNs appeared on files impacted by this incident. This includes current and former federal employees, contractors, and others who completed a background investigations application, and their spouses and/or co-habitants that are listed on the forms
    - Each affected individual will be notified – likely by mail – to inform them of the breach and the type of information that was potentially exposed. The communication will include an offer of credit monitoring and identity theft assistance at no charge
    - To the extent that emails are used for notifications, the communication will come from a Federal government email address, to alleviate confusion about the source of the notification and to address concerns that it may be illegitimate or a spear-phishing attempt
    - Contractors will be notified as individuals, in the same manner as federal employees; to receive notification, contractors must be cleared/have completed an SF-85 or SF-86

- The Administration is working 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.

- Employee requests for individual copies of SF-85 or SF-86 information – OPM is establishing a more streamlined system/process for requesting copies of completed SF-85 and SF-86 forms
    - Employees are encouraged to wait until this process is available rather than submitting FOIA/Privacy Act requests
    - This process will likely not include the ability to obtain adjudicative information

❖ ***e-QIP Suspension***

- OPM identified vulnerability in the Electronic Questionnaires for Investigations Processing (e-QIP) system, and temporarily took this system offline. OPM has conducted security enhancements in the system, and, after extensive testing, the e-QIP system has been brought back online.

- e-QIP is a web-based automated system designed to facilitate the processing of standard forms (SF) 85, SF 85P, and SF 86 to collect personal history information used when conducting background investigations for Federal security, suitability, fitness and credentialing purposes. An agency initiates a background investigation through e-QIP by having the applicant electronically enter, update, sign, and transmit his or her personal information and related releases over a secure internet connection to the requesting agency.

- Now that e-QIP has been restored, required investigations will be completed through the regular process, and the interim procedures have been superseded.

❖ ***Cyber Sprint***

- On Thursday, June 11, 2015, Tony Scott, the Federal Chief Information Officer (CIO), sent a message to Agencies outlining the "Priority Cybersecurity Action Items" for all Federal Agencies.

- The targets set by OMB are intended to secure Federal networks and include tightening policies for privileged users, implementing multifactor authentication for both privileged and standard users and ensuring identified vulnerabilities are quickly addressed.

- DOE is addressing the OMB cyber sprint actions and is reporting regularly on the actions. These are high visibility and a high priority for the Department.

Resources Available

- DOE is committed to providing employees with the most recent resources and support, and will continue to provide updates as we learn more about the cyber incidents affecting OPM.

- OPM has launched an online resource – www.opm.gov/cybersecurity - to offer information regarding these OPM incidents and provide access to materials, training, and useful information on best practices to secure data, protect against identity theft, and stay safe online.
    - A new "Stay Informed" feature has also been added that allows users to receive automatic email alerts when new information is posted on the website.

- The DOE call center hotline is 855-719-4496. Due to declining call volumes and the availability of other useful resources, the call center will not be operational after August 7, 2015.

- The Cyber Incident Email Inbox (inquiry.doe@hq.doe.gov) is available to receive and respond to questions regarding the incidents.
    - When contacting the DOE email inbox, employees should not include Personally Identifiable Information (PII) in your inquiry or comment.

- DOE has established a website on its intranet to provide up-to-date information and resources. Employees can access the website at: https://powerpedia.energy.gov/wiki/OPM_Cyber_Incident

- As we move forward from this incident, employees are encouraged to take proactive measures to ensure there are no adverse impacts. This includes monitoring financial account statements and reporting suspicious or unusual activity; being suspicious of unsolicited calls and email messages asking about the employee, their colleagues, and other internal information; not providing personal or financial information in email; avoiding phishing attempts; and reviewing available resources and information on websites such as www.identitytheft.gov, http://www.us-cert.gov/ncas/tips/ST04-013, http://www.antiphishing.org, and www.consumer.gov/idtheft.

- Cybersecurity will remain a constant and evolving challenge as we become more reliant on information technology and systems. This incident reminds us of the seriousness of the cyber threats that we face and the importance of vigilance in protecting our systems. These threats are dynamic, they are constantly evolving, and they require that we endeavor to stay ahead of them. We can't fix it once and then be done -- we have to keep up our skills and capabilities and processes to share information.