Frequently Asked Questions

OPM Data Breach

Department of the Navy

24 July 2015 pm
(*Information identified by Incident #1 and #2*)

Table of Contents

Summary 2

Incident #1 – Background & Update 3

eQIP 3

Recap – *New* 4

Incident #1 4

Incident #2 4

Who is Affected 5

Notification Update 7

General Information 10

What's Next 13

eQIP Update *New* 18

Need More Information & Phishing Alerts *New* 20

Appendix A – Interim HR Process during Temporary Suspension of e-QIP 22

Appendix B - Guidance for Federal Employees and Retirees 23

Appendix C - DONCEAP Identity Theft Information 24

Appendix D - Removing Yourself from Public Websites 26

Appendix E – OPM Announcement 29

Note: As the OPM Data Breach is under federal investigation, this document will continue to be updated as more information becomes available. This latest version identifies responses specific to the incidents reported by OPM. Current FAQs also may be found at **www.secnav.navy.mil/OPMBreachDON/.**

Summary

On July 9, 2015, the Office of Personnel Management (OPM) announced the details of a second cyber incident that involves background investigation information of current, former and prospective employees (civilian, military and contractor). The data system that was compromised included personal and sensitive information about the employees typically provided on the Standard Form (SF) 85, 85p and 86 to include Social Security numbers (SSNs), residency and educational history, health and medical information, employment history, marital status, foreign travels, information about children and other relatives as well as personal friends and business acquaintances, financial history, criminal and non-criminal court cases, and passport information. Some information may also include finding from interviews conducted by background investigators and fingerprints. Usernames and passwords that applicants submitted during the background investigation were also stolen.

OPM confirmed stolen records likely include the SSNs of 19.7 million people who applied for background investigations as well as 1.8 million non-applicants to include spouses or co-habitants of the applicants. Additionally, 1.1 million fingerprint records were stolen as part of Incident #2. According to OPM, individuals likely to be impacted underwent a background investigation through OPM in 2000 or afterwards; those undergoing an investigation prior to 2000 may be impacted but it is less likely. OPM does not have evidence that separate systems that store information regarding the health, financial, payroll and retirement records (such as annuity rolls, retirement records, USAJOBS, Employee Express) were impacted by the second incident.

OPM will notify affected individuals through U.S. Postal Mail. OPM notifications will include details on the incident and information on how to access the suite of monitoring and protection services which will be offered. *Notification has not yet begun.*

The 21.5 million individuals (applicants and non-applicants) whose SSNs and other sensitive information were stolen will be provided a suite of monitoring and protection services for at least three years at no charge. Services include full-service identity restoration support and victim recovery assistance, identity theft insurance, identity monitoring for minor children, continuous credit monitoring, and fraud monitoring service beyond credit files.

Records for approximately 3.6 million people were included in both incidents; in total, 22.1 million people were affected by the cybersecurity.

Incident #1 – Background & Update

In April 2015, the Office of Personnel Management (OPM) became aware of a cybersecurity incident affecting its systems and data that may have compromised the personal information of current and former federal employees. (Incident #1) OPM estimates that 4.2 million employees were impacted by the first breach.

OPM began conducting notifications to affected individuals using email and/or USPS First Class mail on June 8, 2015. Recognizing the inherent security concerns in this methodology, with OPM and CSID support, DoD suspended notifications to employees on June 11, 2015, until an improved, more secure notification and response process is in place. Late June 15, 2015, OPM advised that email notification resumed. *Notifications to employees about Incident #1 are still ongoing.*

Individuals impacted by Incident #1 have been offered 18 months of identity theft insurance and credit monitoring services through CSID – a company that specializes in identity theft protection and fraud resolution. The 18-month CSID membership is offered at no cost to those individuals identified by OPM.

In the course of the ongoing investigation into the first cyber intrusion that compromised personnel records of current and former federal employees (announced June 4), OPM discovered that additional OPM systems were compromised. These systems contain information related to background investigations.

eQIP

As a precautionary measure, on Monday, June 29, OPM announced that it was suspending eQIP for 4-6 weeks. eQIP is the automated Electronic Questionnaires for Investigations Processing system for submission of SF85s and 86s to OPM for workforce suitability and clearance eligibility determinations and investigations. OPM announced 23 July 2015 that it would re-enable the eQIP system.

Recap – *New*

Incident #1

- ~4.2 M current and former **civilian** employees impacted by a cybersecurity incident (December 2014)
- Personal information includes: name, SSN, place and DOB, current and former addresses, education, training, employment information, etc.
- Notification email and letters in process (begun June 8); likely that not all personnel have been contacted
- 18-months of free identity theft insurance for up to $1 million; optional 18 months of credit monitoring available (**IF** employees opt to enroll)
- CSID (identity theft contractor) toll-free number 1-844-777-2743

Incident #2

- ~21.5 million former and current civilian, military and contractor employees who submitted background investigation applications **and** spouses (or co-habitants) Social Security Numbers (SSNs)
- Highly likely to impact those who underwent a background investigation through OPM since 2000
- Information accessed includes data from SF85, 85p, 86 (includes SSNs, Residency and educational history, Employment history, information about immediate family, personal and business acquaintances, health, criminal and financial history, usernames and passwords used to fill out background investigation forms — complete listing available in this document)
- 3 years of monitoring and protection services offered at no charge to impacted employees, their spouses (co-habitants) whose SSNs were compromised **and** minor children
- OPM has not yet begun notifications to impacted employees

Who is Affected

1. **Q: How many individuals were impacted by the data breach?**
   A: Incident #1 – OPM estimates about 4 million current and former employees may have had personally identifiable information (PII) compromised in the breach detected in April 2015. Since the investigation is ongoing, additional PII exposures may come to light. If OPM determines that more individuals have been impacted, they will conduct additional notifications.

   Incident #2 – OPM estimates that about 21.5 million individuals may have had information compromised in the second incident. Those affected individuals include current and former military members, current and former civilians, and prospective applicants as well as contractors who may have submitted a background investigation questionnaire. (There is an overlap of 3.6 million people who were included in both incidents.)

2. **Q: How many Department of Navy (DON) employees were affected?**
   A: Currently that information is not available.

3. **Q: Are retirees impacted by the data breach?**
   A: Incident #1 – OPM continues to examine the data and systems that may have been compromised. For example, OPM has confirmed that any federal employee whose organization submitted records to OPM for future retirement process may have been compromised – even if their full personnel file is not stored on OPM's system. These individuals are included in the estimated 4 million individuals impacted by the first incident. Records that may have been compromised for these individuals may include service history records, court orders, and other records and information that pertain to annuity calculations. The PII data in these records includes name, Social Security numbers, and dates of birth as well as other information. Individuals who do not have a work email of record will be notified by U.S. Postal mail.

   Incident #2 — Yes. Affected individuals could include retired members of the civilian, military and contractor workforce. It is highly likely that any individuals who submitted background investigation information to OPM in 2000 or afterwards were impacted by this incident; individuals who submitted information prior to 2000 might be impacted, but it is less likely.

4. **Q: Were contractors affected by the breach?**
   A: Incident #1 – Contractors were not affected unless they were previously a federal civilian employee.

   Incident #2 – Contractors who had to complete an OPM background investigation may have been affected by the breach. OPM will notify the individuals whose Social Security Number

appeared on the files impacted by the second breach. It is highly likely that any individuals who submitted background investigation information to OPM in 2000 or afterwards were impacted by this incident; individuals who submitted information prior to 2000 might be impacted, but it is less likely.

5. **Q: Were current, retired or former military members affected?**
   A: Incident #1 – OPM does not believe the first incident affected military member records, unless they held a federal civilian position.

   Incident #2 – Yes, current, retired or former members of the military may be affected. It is highly likely that any individuals who submitted background investigation information to OPM in 2000 or afterwards were impacted by this incident; individuals who submitted information prior to 2000 might be impacted, but it is less likely.

6. **Q: Were NAF (Non Appropriated Funds) Employees impacted since OPM does background investigations for the NAF workforce?**
   A: Incident #1- Some Department of the Army NAF employees were affected and are being notified by OPM.

   Incident #2- It is possible that current, former or prospective NAF employees who submitted background investigation information to OPM in 2000 or afterwards were impacted by this incident; individuals who submitted information prior to 2000 may be impacted, but it is less likely.

7. **Q: Was the information in USAJOBS compromised?** ***New***
   A: OPM has confirmed that USAJOBS data was not affected. However, USAJOBS recently issued an alert about a phishing attempt to capture the USAJOBS user's login information. The USAJOBS system is not sending out email notifications asking users to revalidate account login information such as Username and Password; by clicking a link within the email. Do not click on any links in the email. Any emails received on that subject should be deleted immediately. If you have any questions go to https://my.usajobs.gov/support. *New*

8. **Q: Who else is affected?**
   A: Incident #1: Current and former federal employees, from all branches of government may receive a notice if:
   - They currently work for a federal agency for which OPM maintains the personnel records.
   - They previously worked for a Federal agency for which OPM maintains the personnel records.
   - The worked for a Federal agency or organization that submitted to OPM service history documentation to support future retirement processing. While organizations across all branches of government must submit these records under certain conditions, organizations may also submit these for various reasons at various times, at their discretion. Some of these reasons could include:

- When an individual separates from an organization.
- When an individual retires from an organization.
- When an organization has a change in payroll service center.

Incident #2 — 19.7 million people who applied for background investigations as well as 1.8 million non-applicants to include spouses or co-habitants of the applicants. Additionally, 1.1 million fingerprint records were stolen as part of Incident #2. According to OPM, individuals likely to be impacted underwent a background investigation through OPM in 2000 or afterwards; those undergoing an investigation prior to 2000 may be impacted but it is less likely. OPM does not have evidence that separate systems that store information regarding the health, financial, payroll and retirement records (such as annuity rolls, retirement records, USAJOBS, Employee Express) were impacted by the second incident.

9. **Q: What is my coverage if I have been impacted by both incidents?**
A: Given the type of data stolen in the background investigations incident and its impact to both applicants and their spouses (or co-habitants), OPM has determined that the comprehensive suite of identity theft protection and monitoring services should be made available for a period of at least three years at no charge.

Notification Update

10. **Q: How will I be notified if I am an affected individual?**
A: Incident #1 – OPM began conducting notifications to affected individuals using email and/or USPS First Class mail on June 8, 2015. Recognizing the inherent security concerns in this methodology, DoD, with OPM and CSID support, suspended notifications to employees between June 11-15, until an improved, more secure notification and response process was in place. Late June 15, 2015, OPM advised that email notification resumed — notification continues for those employees impacted by the first incident.

A: Incident #2 – OPM will send notification letters to affected individuals; some individuals may also receive additional contact through email. To the extent that emails are used for notification, 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. Notifications have not yet begun for the second cybersecurity incident.

11. **Q: What do I need to do when I get the email?** ***New***
A: Incident #1 – The email now advises employees to paste or type a link to an https site. CSID also has changed the form on their initial page and only requires an employee to enter the unique PIN#. Additionally, employees may be asked to solve a CAPTCHA to help CSID block automated cyber-attack programs. Once the PIN# and CAPTCHA (if required) are accepted, employees can proceed to the credit monitoring signup page – this is where personal information must be entered. *New*

Employees who have received a notification via email from the email account OPMcio@csid.com (or via letter from U.S. Postal Service) and entered their assigned PIN, are registered for the credit monitoring services.

Affected employees who disregarded that email or deleted the email or affected employees who have not yet received the email will *automatically* be enrolled in the identity theft insurance. These employees will be re-notified by email with a PIN#.

Incident #2 — OPM notifications will include details on the available services and resources. It will also include information that the employee can provide to individuals he/she may have listed on a background investigation form.

12. Q: What happens if I did not activate my PIN#?

A: Incident #1 – Employees who were notified by email **before** June 15 **and** who did **not** activate their PIN#, will be **re-notified** by another email**.** Employees impacted by Incident #1 are automatically covered by identity theft insurance for 18 months. Employees may call the CSID toll free number 1-844-777-2743 to authenticate their status and receive their PIN#.

13. Q: Where will/did employees receive the email notification?

A: Incident #1 – Current federal employees who were affected should receive email notification using their work email. Some employees have indicated that the email notification went to their junk mail. It is strongly recommended that employees FIRST check their junk mail for OPM's email notification. The email notification should come from OPMcio@csid.com.

Incident #2 — Email notifications will be sent to government email addresses.

14. Q: Will I receive notification by U.S. Postal mail if I don't receive an email notification?

A: Incident #1 – Employees may not receive notification by U. S. Postal mail unless employees do not have a work email address or if the email was rejected. If no notification is received, employees may call the CSID toll free number 1-844-777-2743 to authenticate their status and receive their PIN#.

Incident #2 — OPM will send notification letters to affected individuals; some individuals may also receive additional contact through email. To the extent that emails are used for notification, 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. Notifications have not yet begun for the second cybersecurity incident.

15. Q: I've left federal service. How will I be notified if I have been impacted?
A: Incident #1 – If you have left the government, OPM will send you a notification via postal mail to the last address the agency has on file. OPM will verify this address with the National Change of Address (NCOA) service before mailing a letter.

16. Q: I recently switched from one federal agency to another. How will I be notified if I have been impacted?
A: Incident #1 – If you have moved between agencies, OPM will send an email notification to your government email account for the agency at which you are currently employed. If your email address is unavailable, notification will be sent via postal mail.

17. Q: I can't access the CSID website?
A: Incident #1 – As this is an evolving situation; there may be intermittent connectivity issues with the website. There also may be issues with volume and the large numbers of people trying to access the site. DoD CIO has asked Components to avoid blocking the CSID.COM/OPM website.

18. Q: I have enrolled with CSID - why can't I login to my account?
A: Incident #1 – The web address for enrolling is https://www.CSID.com/OPM -- this site is for employees to set up accounts. Once you have enrolled, to login at a later time, go to https://opm.csid.com.

19. Q: I received an email from opmcio@csid.com. Is this email from OPM, or is this a phishing message?
A: Incident #1 – The sender "OPM CIO" and email address "opmcio@csid.com" are the sender and email address that OPM is using to notify affected individuals. If you get an email about the breach from a different address, it is spam. Do not click on any links or provide any personal information. Contact privacy or security officers or follow Command or USMC protocols if receiving a suspected phishing message.

20. Q: I believe I may have deleted the email notification. What do I do now?
A1: Follow these steps to attempt to retrieve the email:
1. Open Outlook
2. Click on "Deleted Items" Folder - on the left menu bar.
3. On the very top of the page click "FOLDER" then --> Click the icon that says "Recover Deleted Items"
5. Go through the list and select (mouse click on them) the ones to recover
6. Navigate to the top of the screen and click the second icon on the top left (says "Recover Selected Items")
7. This will recover the deleted email and return the email to the "Deleted Items" outlook folder
8. Simply move the email to your inbox

A2: Incident #1 – Call CSID at 1-844-777-2743 and they will authenticate your status as an impacted government employee and reissue your PIN on the phone. The employee will then use the PIN to register at the CSID website.

21. **Q: What if I have not received notification by email or U.S. Postal mail?** ***New***
A: Incident #1 – If you believe you have been impacted by Incident #1, employees may call the CSID toll free number 1-844-777-2743 to authenticate their status, receive their PIN#. and enroll in the program. The call center representative will ask for the person's name, last four of the SSN and their address. The call center may be able to verify an employee's status as affected. *New*

22. **Q: What should I do if my agency's filter blocks delivery of my notification? What if my notification bounces back to CSID?**
A: If you suspect your email has been blocked by your agency's filter, work with your IT support office or help desk to release the email. If you want to verify the authenticity of the email, contact your Privacy officer or CIO. OPM has provided those offices with information for verifying the notification emails. In addition, in cases in which CSID receives email bounce-back messages for notifications, it is sending out additional notifications during the week of 22-26 June.

General Information

23. **Q: When did this happen?**
A: Incident #1 – OPM believes that the intrusion occurred in December 2014. OPM became aware of the intrusion into its systems in April 2015 after implementing tough new measures to deter and detect cyberattacks.

A: Incident #2 – During its investigation, OPM became aware of intrusions into its systems in May (affecting background investigations data). On June 8, 2015, OPM alerted agencies that there was a high degree of confidence that OPM systems containing information related to the background investigations of current, former and prospective federal government employees **and** those for whom a federal background investigation was conducted, *may have been* compromised. On July 9, 2015, OPM confirmed with a 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 who applied for a background investigation and 1.8 million non-applicants (mostly spouses or co-habitants of applicants). Some records also include findings from interviews conducted by background investigators and approximately 1.1 million fingerprints.

24. **Q: What personal information was compromised?**
A: Incident #1 – OPM maintains personnel records for the federal workforce. The kind of data that may have been compromised in this incident could include name, Social Security Number, date and place of birth, and current and former addresses. It is the type of information you would typically find in a personnel file, such as job assignments, training

records, and benefit selection decisions. OPM has indicated that it does not appear that names of family members, beneficiaries or information contained in actual policies were compromised. Please note, however, that DoD and DON employees and retirees may have had their information included in the human resources information that was compromised. The OPM notification will indicate what information may have been compromised.

Incident #2 – The system impacted by the second incident contains information related to background investigations – information typically entered in the Standard Forms (SF) 85, 85p and 86. Information includes personal and sensitive data such as:

- Social Security Numbers
- Residency and educational history
- Employment history
- Selective service record
- Military history
- Personal and business acquaintances
- Marital status
- Information about children, immediate family and other relatives
- Foreign contacts
- Foreign activities, foreign business, professional activities, foreign government contacts
- Foreign travel, passport information
- Psychological and emotional health information
- Police record, illegal use of drugs and drug activity, alcohol use
- Investigations and clearance record
- Financial history
- Criminal and non-criminal court cases
- Association records

Some records also include findings from interviews conducted by background investigators and fingerprints. Usernames and passwords that 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 sources 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 employees were impacted by the second incident (i.e., annuity rolls, retirement records, USAJOBS, Employee Express).

25. Q: Why didn't OPM tell affected individuals about the loss of the data sooner?

A: Incident #1 – OPM became aware of an intrusion in April 2015. OPM worked with the DHS Computer Emergency Readiness Team (US-CERT) as quickly as possible to assess the extent of the malicious activity and to identify the records of individuals who may have been compromised. During the investigation, OPM became aware of potentially compromised data

in May 2015. With any such event, it takes time to conduct a thorough investigation and identify the affected individuals.

26. Q: What systems were affected? Were DoD or DON systems affected?
A: Incident #1 — This incident impacts the OPM systems and data. Please note, however, that DoD and DON employees and retirees may have had their information included in the human resources information. For security reasons and due to the ongoing investigation, OPM cannot publicly discuss specifics that might be affected by the compromise of personnel data. OPM has added additional security controls to better protect overall networks and systems and the data they store and process.

Incident #2 — If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs by submitting forms SF85, SF85p, SF86 for a new investigation or a periodic re-investigation), it is highly likely that the individual is impacted by the second incident. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely.

27. Q: Are TSP accounts impacted by the OPM cybersecurity incidents?
A: TSP account numbers are not shared with OPM and, as such, were not impacted.

28. Q: Was banking information, including direct deposit forms, compromised? What about Employee Express or W2 information?
A: Incident #1- OPM indicated that banking information, TSP and Employee Express and tax information were not compromised.

A: Incident #2 – 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 sources 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 (i.e. annuity rolls, retirement records, USA JOBS, Employee Express).

29. Q: Was other information compromised?
A: Incident #2 –The systems containing information related to background investigations may have been compromised. Types of information involved in the background investigation records incident that may have been impacted include Social Security Numbers, residency and educational history, employment history, information about immediate family and personal and business acquaintances, health, criminal and financial history that would have been provided as part of your background investigation. Some records could also include: findings from interviews conducted by background investigators, your fingerprints, and usernames and passwords used to fill out your forms. Some information may also include findings from interviews conducted by background investigations.

30. Q: Was the data that was exfiltrated encrypted?

A: Though data encryption is a valuable protection method, today's adversaries are sophisticated enough that encryption alone does not guarantee protection. OPM utilizes a number of different protection mechanisms for systems and data, and utilizes encryption when possible. However, due to the age of some of our legacy systems, data encryption isn't always possible. In fact, encryption in this instance would not have protected the data. Currently, we are increasing the types of methods utilized to encrypt our data. These methods include not only data at rest, but also data in transit, and data displayed through masking or redaction. OPM's IT security team is actively building new systems with technology that will allow the agency to not only better identify intrusions, but to encrypt even more of our data.

31. Q: How do we know that enrollment with CSID is secure and will not expose us to a second breach of our PII?

A: CSID is an industry leader when it comes to identity theft protection and has a successful history of partnering with both public and private companies. Their company is embedded with security means to protect your information. CSID's site is scanned daily for thousands of hacker vulnerabilities and displays the McAfee SECURE trustmark.

32. Q: Will CSID sell my information to third parties?

A: CSID adheres to strict Federal Privacy Guidelines and has advised that no additional marketing or solicitation will occur to individuals without OPM's explicit request or approval.

What's Next

33. Q: I received a letter stating that I have been affected. What should I do next?

A: Incident #1 — Please refer to the instructions in the letter or email. Typically, enrollment is a two-step process. First employees will register their PIN# at the website. **IF** employees want to register for the complementary credit monitoring through CSID, they will be redirected to a secure website where they may enter their personal information. Enrollment in the CSID credit monitoring services, will ensure that your credit and credit card accounts are monitored for any suspicious or fraudulent activity. Impacted employees may also call 1-844-777-2743; (international callers can call collect at 512-327-0700) if they have questions. Due to a high volume of calls, employees may experience wait times of 5-6 minutes. Typically, employees will not be able to register for the credit services by phone.

34. Q: What is planned to protect federal employees in the future?

A: 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.

35. Q: Can I register by calling the CSID line?

A: Incident #1 — Possibly. After receiving notification, typically employees who have received the OPM notification must register online. However, employees can verify if they have been impacted, authenticate their identity and receive their PIN# by calling CSID at 1-844-777-2743. During peak hours, you may experience wait times of 5-6 minutes.

36. Q: What happens after I register?

A: Incident #1 — Within about 24-72 hours after registering, employees will receive a subsequent email that advises the employee "Your CSID identity protection report is now available. One or more of your reports have been updated." Typically, the email follows by listing information which will be available to the employee to include:

- PayDay Loan - A PayDay Loan alert/report may include new inquires of new loans requested at a pay-day loan location using your identity;
- CyberAgentSM - A CyberAgentSM alert/report may contain matches for your information related to criminal chat rooms, news groups and other web sites where criminals trade or sell stolen identities;
- Court Records - A Court Records alert/report may contain matches for name and date of birth from county courts, Department of Corrections (DOC), Administration of the Courts (AOC), and other legal agencies. The types of offenses include felonies, misdemeanors, sexual offenses, traffic citations and more;
- Sex Offender - A Sex Offender alert/report may contain matches for your identity within Sex Offender registry files or may be an update to registered Sex Offenders in your zip code;
- Social Security Trace - A Social Security Trace alert/report may lists addresses associated with your identity found in public records. A Social Security Trace alert/report may contain matches for your identity found in public records. If you have utilized a nickname in the past when applying for credit or you have changed your last name due to marriage, additional names may be reported. The email ends with a reminder to the employee to log in to their account at https://opm.CSID.com to view the details of this alert.

37. Q: What is OPM doing to prevent this kind of loss from happening again?

A: Information on OPM actions are found at www.opm.gov.

38. Q: I did not receive a letter stating that my information was compromised, but feel that I should have. Can you help me?

A: Incident #1 – OPM has identified the individuals who have been impacted and began to notify individuals on June 8. They continue to notify affected employees. If you believe you should have been contacted, employees may call the CSID toll free number 1-844-777-2743 to authenticate their status and receive their PIN#. (International callers can call collect at 512-327-0700)

Incident #2 — OPM has not yet begun to notify individuals impacted by Incident #2. It is highly likely that anyone who underwent a background investigation since 2000 will be

impacted by Incident #2. OPM will notify impacted individuals first by U.S. Postal Mail; some additional notifications may be made by government emails.

39. **Q: Can my family members also receive services if they are part of my file/records?**
A: Incident #1 – OPM has indicated that family members of employees were not affected by this breach. Therefore, they are not entitled to the credit monitoring and identity theft services provided by CSID through OPM.

Incident #2 – The 21.5 million individuals (applicants and non-applicants) whose SSNs and other sensitive information were stolen will be provided a suite of monitoring and protection services for at least three years at no charge. Services include full-service identity restoration support and victim recovery assistance, identity theft insurance, identity monitoring for minor children, continuous credit monitoring, and fraud monitoring service beyond credit files. Also, in the notification package OPM provides information that the employee can provide to individuals he or she may have listed on a background investigation form, to include the types of data that may have been included as well as best practices to protect themselves and the resources available to address questions.

40. **Q: I received a notice for a family member who is deceased, what do I do?**
A: Incident #1 – Update contact information or the information about a deceased former employee by calling CSID's call center at 1-844-777-2743. If the notification was received by mail, OPM advises family members to destroy the letter and the mailer. No further action is required by the next of kin.

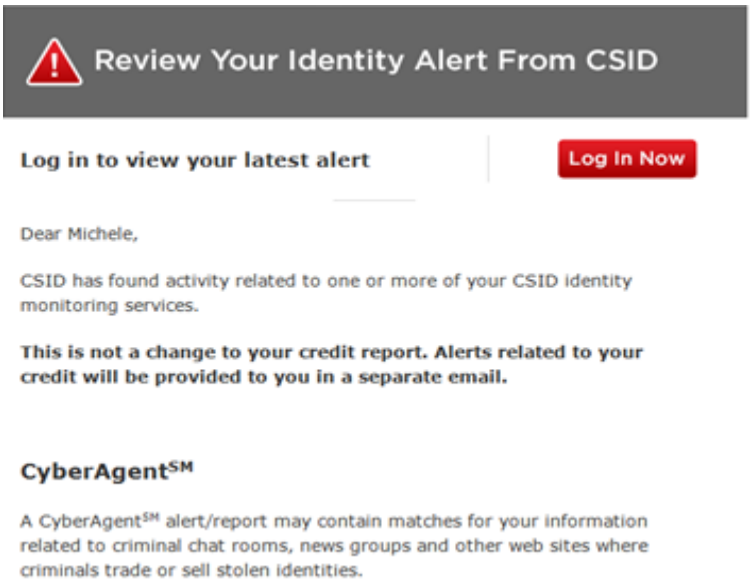
41. **Q: Will coverage be extended to family members who were minors when the background investigations were initiated but who are now adults?**
A: Incident #2 — Identity monitoring services will be provided to minor children – this does not extend to children who now are adults.

42. **Q: Is it possible to decline CSID identity theft insurance?**
A: Incident #1 – Affected individuals are given complimentary identity theft insurance free of charge for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll, will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID until December 7, 2016. If an employee wants to opt out of the free OPM-provided identity theft insurance, they should contact CSID directly to remove them from the program.

43. **Q: What if someone uses my identity to place unauthorized charges to my account?**
A: Incident #1 – Impacted individuals will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID which includes loss of income, child care, elderly care, unauthorized electronic funds transfer and legal costs. Impacted individuals who have enrolled and need to file a claim for fraudulent charges should call 1-844-777-2743.

44. Q: I received an email from CSID (opmsupport@csid.com) directing me to "review my identity alert". What is this?

A: Incident #1 – If you receive this email, CSID has identified activity through their monitoring systems. This is not a change to your credit report. Alerts related to your credit will be provided to you in a separate email. You will be prompted to log in to your account to view the details of the activity via an alert (sample screen shot below).



45. Q: Can you confirm that the CSID monitoring program and insurance policy will not conflict with or adversely affect other protection I have with another company?

A: Incident #1 – That is a question best addressed by credit professionals. While it may be unlikely that multiple credit monitoring services will adversely affect one another, it is not necessary (or recommended) that affected employees have two separate credit monitoring services.

46. Q: Will my credit be impacted if I accept a credit report through the CSID monitoring program?

A: This is a government-sponsored service provided to affected employees and accepting the service will not, in and of itself, impact credit scores.

47. Q: How do I contact the CSID representatives?

A: Incident #1 – Current and former federal employees can contact CSID between 7 a.m. and 10 p.m. CST, Monday through Friday, and 8 a.m. to 8 p.m., CST, on Saturdays, by calling the toll-free number 1-844-777-2743 (International callers may call collect at 512-327-0705). Highest call volume occurs between 9 a.m. and noon.

48. Q: Do I need to notify my security office if I have detected fraudulent activity?
A: Employees should notify their security officer or supervisor in writing if fraudulent activity occurs.

49. Q: Does DON offer any services or information about identity theft?
A: The Department of the Navy Civilian Employee Assistance Program (DONCEAP) provides support for financial issues and identity theft for all DON civilians and their families. The 24/7 number is **1-844-DONCEAP** (1-844-366-2327) TTY 1-888-262-7848, International 001-866-829-0270. Information is also available at http://DONCEAP.foh.hhs.gov. A listing of resources also is available at www.secnav.navy.mil/OPMBreachDon/ and OPM has launched a cybersecurity incident resource center at https://www.opm.gov/cybersecurity

50. Q: I received a possible phishing message. Is this related to the breach? Who should I report the possible phishing?
A: If you believe you have received a possible phishing scheme, please report it to your CIO or security office as soon as possible. Employees may also send potential phishing messages to NMCI_SPAM@navy.mil

51. Q: I've noticed the identity theft protection provided by OPM is only available for 18 months. Will the CSID coverage be extended beyond 18 months?
A: Incident #1 - At present, OPM will provide the credit monitoring and theft identity services at no cost to impacted individuals for 18 months – the industry standard for identity theft protection. Impacted individuals will have up to $1 million of identity theft insurance and access to full-service identity restoration provided by CSID. OPM will continue to assess and evaluate the need for additional measures should they be necessary.

52. Q: Is there anything else I can do?
A: OPM has provided guidance on safeguarding your identity that is found in this FAQ document. Also, OPM has launched a new incident resource center to provide information regarding the two OPM cybersecurity incidents as well as best practices, materials, training and information to secure data and protect against identity theft — https://www.opm.gov/cybersecurity. In the weeks ahead, OPM will be establishing a call center to respond to questions and provide additional information.

53. Q: Are there websites where I can get information, resources?
A: OPM — https://www.opm.gov/cybersecurity
DoD Email — DOD.DATA.BREACH.QUESTIONS@MAIL.MIL
DON Webpage — www.secnav.navy.mil/OPMBreachDON/
DON Email — DONhrFAQ@navy.mil

54. Q: What resources are available for Service Members and their families at the Fleet and Family Support Center (FFSC)?

A: Although not subject matter experts regarding the breach or cyber security, the FFSC can provide general budgeting and financial management services. In addition, stress management classes and individual counseling services are available.

55. Q: Who is eligible for services at the FFSC?

A: All active duty service members, their family members, members of the reserve component of the military Services and their family members while on a call or orders to active duty, and retirees are eligible for services.

eQIP Update *New*

56. Q: What is eQIP?

A: The electronic Questionnaires for Investigations Processing (eQIP) system is a web-based automated system than enables processing of standard forms (SF) 85, 85P and 86 – forms used to collect personal history information when conducting background investigations for federal security, suitability, fitness and credentialing.

57. Q: Why was eQIP offline? *New*

A: On June 29, 2015, OPM temporarily suspended eQIP as part of a review of its security for the IT systems. OPM has concluded it review and re-enabled eQIP on July 23, 2015. In returning eQIP to service, OPM announced the following security enhancements: *New*

- Passwords: User password length was increased and encryption of the stored passwords in the system was enhanced
- Data Input: All information coming into the system is examined to detect and remove malicious functions multiple times before being added to the database
- Hardware: Hardware with known vulnerabilities has been replaced or removed from the system
- Software: Software brought up to date
- Configuration: All elements of the system configuration have been updated to meet Federal standards
- Design: e-QIP software received security enhancements at the code level to sanitize and remove vulnerable functions

58. Q: What does this mean for new employees? *New*

A: The suspension of eQIP impacted the ability to initiate investigations for new employees, contractors and individuals due for reinvestigation. OPM has re-enabled eQIP as of July 23, 2015. During the temporary suspension of eQIP, new hires followed an interim process. That process remains in effect. Consult with your Command Security Officer for details. *New*

59. Q: What happens next? ***New***

A: Until the eQIP fully returns to service, new hires will complete and submit the appropriate security clearance questionnaire using a fillable PDF. Prospective employees will receive instructions as to which form(s) must be submitted — fillable forms are available at https://www.opm.gov/forms/standard-forms/ or http://www.gsa.gov/portal/forms/type/SF. Prospective employees must retain a copy of the form as they will be required to enter their responses electronically into the OPM eQIP system when it returns to full operational capability. (*See Appendix A for the Interim HR Solution during the temporary suspension of eQIP*.) *New*

60. Q: Will information that was entered into e-QIP before it was taken offline on June 26 still be in the system when users log back in? ***New***

A: Yes, information entered into e-QIP by users before the system was taken offline should be repopulated in the system when their Command Security Office reinitiates users. OPM will re-enable eQIP users incrementally to resume the service in an efficient and orderly manner. *New*

61. Q: Given OPM's track record on cyber security, how can I be assured that e-QIP is actually secure? ***New***

A: During the time that the system was offline, OPM has worked closely with the Office of Management and Budget, the Department of Homeland Security and other interagency partners to implement security enhancements. OPM has indicated that the improvements further enhanced password protections, secured the transmission of data within the application, and implemented additional protections against external threats. Additionally, OPM had experts from across government test the enhancements to safeguard their effectiveness. Based on these security enhancements and the extensive testing that has been completed, OPM is re-enabling access to e-QIP with confidence in the security of the system. *New*

62. Q: Where can I get more information about eQIP?

A: OPM maintains information about eQIP at https://www.opm.gov/investigations/e-qip-application/.

Need More Information & Phishing Alerts *New*

- www.SECNAV.navy.mil/OPMBreachDON
- www.opm.gov/cybersecurity
- DoD.Data.Breach.Questions@Mail.mil
- DONhrFAQ@navy.mil

Blank SF85 — https://www.opm.gov/forms/pdf_fill/sf85.pdf
Blank SF85P — https://www.opm.gov/forms/pdf_fill/sf85p.pdf
Blank SF86 — https://www.opm.gov/forms/pdf_fill/sf86.pdf

There have been recent phishing reports under the misrepresentation of the Federal Trade Commission and USAJOBS. Following are advisories issued by the agencies about the phishing attempts. *New*

Advisory: Issued by Federal Trade Commission *New*

It's NOT the FTC calling re: OPM breach, FTC, Division of Consumer and Business Education

If you're an OPM data breach victim, you probably know to look out for identity theft. But what about imposter scams? In the latest twist, imposters are pretending to be the FTC offering money to OPM data breach victims.

Here's how it works: A man calls and says he's from the FTC and has money for you because you were an OPM data breach victim. All you need to do is give him some information.

Stop. Don't tell him anything. He's not from the FTC.

One fake name the caller used was Dave Johnson, with the FTC in Las Vegas, Nevada. There's not even an FTC office in Las Vegas. The FTC won't be calling to ask for your personal information. We won't be giving money to OPM data breach victims either.

That's just one example of the type of scam you might see. You may get a different call or email. Here are some tips for recognizing and preventing government imposter scams <http://www.consumer.ftc.gov/articles/0048-government-imposter-scams> and other phishing scams <https://www.consumer.ftc.gov/articles/0003-phishing> :

- Don't give personal information. Don't provide any personal or financial information unless you've initiated the call and it's to a phone number you know to be correct. Never provide financial information by email.
- Don't wire money. The government won't ask you to wire money or put it on a prepaid debit card. Also, the government won't ask you to pay money to claim a grant, prize or refund.
- Don't trust caller ID. Scammers can spoof their numbers so it looks like they are calling from a government agency, even when they are not. Federal agencies will not call to tell you they are giving you money.

If you've received a call or email that you think is fake, report it to the FTC at https://www.ftc.gov/complaint.

Phishing emails related to the OPM breach should be forwarded to US-CERT at phishing-report@us-cert.gov.

USAJOBS Web Posting

July 23, 2015 - Important Message Concerning Email Scams

Please be advised that the USAJOBS system is not sending out email notifications asking users to revalidate account login information such as Username and Password; by clicking a link within the email. Do not click on any links in the email. This is a phishing attempt to capture the USAJOBS user's login information. Any emails received on that subject should be deleted immediately.

If you have any questions contact support at https://my.usajobs.gov/support

Information about OPM Cybersecurity Incidents can be found at https://www.opm.gov/cybersecurity/

Appendix A – Interim HR Process during Temporary Suspension of e-QIP

Working across the Department and with DoD and OPM, we have identified an interim solution to be used until the OPM system for Electronic Questionnaires for Investigations Processing (e-QIP) returns to service. The DON expects the interim solution to minimize impact on hiring and is similar to the processes used previously before the electronic system was activated. The interim solution applies to new hires who must complete and submit a security clearance questionnaire using a fillable PDF (employees will enter their responses electronically into e-QIP when it becomes available). It is important to note that hiring has not and will not stop.

1. HR offices send tentative job offers by using the Onboarding Manager system; advises prospective employees of the clearance requirements and instructs the prospective employee to complete assigned forms (to include OF 306, Declaration for Federal Employment) using Onboarding Manager.
2. HR offices send resumes and completed OF 306 to the servicing security office.
3. Security offices review the resume and completed OF 306. The security office advises prospective employees to complete the SF85, 85p or 86 as appropriate to their position for review by security BEFORE they can onboard. Security offices informs the HRO of the clearance outcome.
4. Security Managers and HR personnel are required to review the SF85/85P & SF86 using the Adjudicative/Suitability Guidelines for derogatory information. If derogatory information is present, the prospective employee is not granted interim access to sensitive or classified information. Additionally, if derogatory information is present, the prospective employee will have to wait until the investigation is completed and adjudicated before access is granted or denied.
5. Paper SFs will not be submitted to OPM; therefore, prospective employees will be required to submit all information into e-QIP once the system returns to service.
6. OCHR has revised tentative and formal job offer templates in Onboarding Manager to include the following requirement as a condition of employment -- selectees will be required to re-submit all information from the SF85/85P/86 into e-QIP upon system availability

Appendix B - Guidance for Federal Employees and Retirees

The following guidance is provided by OPM:

- Do not answer unsolicited phone calls, in-person visits or e-mails from anyone asking about federal employees or other internal information in your agency.
- Do not provide personal information or any information about your agency or how it is organized to anyone unless you know them or have verified that they are legitimate.
- Don't reveal your personal or financial information in e-mail — and don't follow links sent through e-mail.
- Do not send sensitive information over the Internet before checking a Web site's security.
- Pay attention to the URL of a Web site. Malicious Web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you're unsure whether an e-mail request is legitimate, try to verify it by contacting the sender directly. Don't use contact information provided on a Web site connected to the request — instead check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
- Install and maintain anti-virus software, firewalls and e-mail filters to reduce some of this traffic (for more information, see Understanding Firewalls www.us-cert.gov/ncas/tips/ST04-004 (external link); Understanding Anti-Virus Software, www.us-cert.gov/ncas/tips/ST04-005 (external link); and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007 (external link).
- Take advantage of any anti-phishing features offered by your agency.
- Monitor your checking and other financial accounts, and immediately report any suspicious or unusual activity to your bank.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. You're entitled by law to one free credit report per year from each of the three major credit bureaus. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) Web site, www.ftc.gov.
- Review the FTC identity theft Web site, www.identitytheft.gov. The agency lists a variety of consumer publications that have a lot of information on computer intrusions and identity theft.
- Consider placing a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.

Appendix C - DONCEAP Identity Theft Information

The following information is provided as a service by DONCEAP.

Are you a victim of ID Theft?

Has something like this happened to you?

- You get a phone call or letter telling you that you have been approved or denied credit for accounts that you never opened.
- You no longer receive your credit card statements, or you notice that some of your mail seems to be missing.
- Your credit card statement includes charges for things you know you never purchased.
- A collection agency contacts you for an account you never opened.

It's possible you have become a victim of identity theft. If you suspect any improper or illegal activity is taking place, here are some recommended steps:

1. Order a copy of your credit report to see if any new accounts or credit inquiries show up. Virtually all of your credit information is in your credit report. If someone is opening accounts in your name, it should show up there. If you suspect you have been a victim of fraud (for example; you have had your mail stolen, lost your wallet, or been contacted by a collection agency for an account you have never heard of), you should contact the fraud department of each credit bureau. You are eligible for a free credit report sent via U.S. mail if you are a victim of fraud or ID Theft.

2. Contact the fraud departments of each of the three major credit bureaus and report that you think your identity has been stolen. Request that a "Fraud Alert" be placed on your file and that no new credit be granted without your approval.

3. Research the crime and file complaints. Contact each company where you think you might have been a victim. Talk to their security or fraud department and explain what has happened. Review your account with them for any incorrect charges or a change of address. If you find something is wrong, you may need to close the account. If you open any new accounts, ask the company to put passwords on the account.

4. File a police report. File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime later on. Also, make sure that the crime is reported under identity theft.

5. Keep a log of all conversations and activities. Make notes of everyone you speak with; ask for names, department names, phone extensions, and record the date you spoke to them. Don't throw these notes away. Keep all notes and letters together in case they are needed in the future. Keep track of the time you spend documenting this information and lost hours at

work. You will need this information if the perpetrator is ever caught. You can be reimbursed for the time spent and hours lost.

6. File a complaint with the Federal Trade Commission (FTC). The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission assists victims of identity theft by providing them with information to help them resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for further action. If you are a victim of identity theft, you can file a complaint with the FTC by contacting their hotline.

   By phone: Toll-free 1-877-ID-THEFT (438-4338)
   Online: https://www.ftccomplaintassistant.gov/#crnt&panel1-1

7. Call the Social Security Administration if you suspect that your Social Security number is being fraudulently used.

   By phone: Toll-free 1-800-269-0271
   Online: www.ssa.gov

8. Contact the Internal Revenue Service if you suspect the improper use of identification information in connection with tax violations.

   By phone: Toll-free 1-800-908-4490
   Online: http://www.irs.gov/Individuals/Identity-Protection

9. For additional information on identity theft, including steps you can take to protect yourself from identity theft, or for assistance from DONCEAP's highly trained Fraud Resolution Specialists, civilian employees can contact DONCEAP 24 hours a day at 1-844-DONCEAP (1-844-366-2327) / (TTY: 1-888-262-7848) / International: 001-866-829-0270 or at DONCEAP.foh.hhs.gov.

Appendix D - Removing Yourself from Public Websites

1. Intelius

On the page where you select your report, the site lists the information that the report includes when available. The site generates a report from its own regularly updated database that is built from billions of public records. These records are obtained from a wide variety of public and commercial sources.

To opt out, go to https://www.intelius.com/optout.php

2. ZebaSearch

All information found using ZabaSearch comes from public records databases. That means information collected by the government, such as court records, country records, state records, such as the kind of information that becomes public when you buy a new house or file a change-of-address form with the United States Postal Service. More often than not, individuals themselves put their own information into the public domain, without realizing they are doing so.

To opt out, you need to provide proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are faxing a copy of your driver's license, they require that you cross out the photo and the driver's license number. They only need to see the name, address and date of birth, and they will only use this information to process your opt-out request. Please fax to (425) 974-6194 and allow 7-14 days to process your request. For more information, go to http://www.zabasearch.com/block_records/

3. Spokeo

Spokeo organizes data from various sources, including public record data, surveys, and social data (that has not been deemed private). Spokeo makes this information more easily accessible for people to research themselves or others.

To opt out, go to http://www.spokeo.com/opt_out/new. For more information, go to http://www.spokeo.com/faqs

4. PeekYou

PeekYou collects and combines scattered content from social sites, news sources, homepages, and blog platforms to present comprehensive online identities. Google calculates the likelihood of any link being associated with a keyword. PeekYou calculates the likelihood of any link being associated with an individual.

To opt out, go to http://www.peekyou.com/about/contact/optout/index.php

5. US Search

US Search's network of databases contains information from a variety of publicly available sources including government records, court documents, professional licensing organizations, and phone books. US Search gathers data from various state and private agencies, and their network extends nationwide, as not all counties and states report the same information.

To opt out, go to http://www.ussearch.com/privacylock

6. PeopleFinders

PeopleFinders is a Data-as-a-Service ("DaaS") provider for consumers and businesses seeking detailed insights on people, places and things. The Company is one of the largest owners of public records data in the U.S. including information on virtually every adult in the U.S., and has unique access to other commercial data sources.
To opt out, go to http://www.peoplefinders.com/manage/default.aspx

7. PeopleSmart

The site provides search access to contact information and public records. Recently, the site updated the information for each State's Court Agency page in our public records database. This is where users can go to find information about retrieving public records from a state's court office.
To opt out, go to https://www.peoplesmart.com/member/optout-go

8. PrivateEye

Currently the web site offers name and address records, phone records, marriage records, divorce records, death records, real property records, bankruptcy/tax lien/civil judgment records, and criminal records. The site constantly updates its data and adding new public records sources.
To opt out, go to http://secure.privateeye.com/optout-form.pdf

9. WhitePages

The site ingests billions of records every month from a variety of public sources and organizes that data by linking individual records to create an intricate contact graph of names, phone numbers, and addresses.
To opt out, go to https://support.whitepages.com/hc/en-us/articles/203263794-How-do-I-remove-my-people-search-profile

10. USA People Search

On USA People Search, users get access to the most recent public records. These records include full names, phone numbers, addresses, and other useful information. It is the easiest way to find people today, or learn more about them.
To opt out, go to http://www.usa-people-search.com/manage/default.aspx

11. Removing Information about You from Google

Removing data from Google and its caches can be extremely difficult, however not impossible.
1. The first step is to remove the information from the original source, meaning whichever website has published the information, remove the data from that publishing and hosting site first. Most websites are not under obligation to remove your data from the site. In fact when you submit, publish, interact, or take part in the website, you most likely fall under the sites terms and conditions, which automatically mean you will lose any right to the data that you have posted, as soon as you post it or take part in the site. The most important thing to remember is that whatever you post to the internet will be there forever, otherwise known as a “digital tattoo.”
2. Do not take no for an answer. Persistence wins in this game. The key is to continuously seek to find a person who manages the website and then continuously follow up and be polite but persistent, send emails, and call.

3. Be nice. They are not only busy, but they are under no obligation to help you. If they do help, it is really as a favor. No one will want to help you if you are unpleasant, so be nice!
4. Delete things from Google using Google's URL Removal tool. https://www.google.com/webmasters/tools/removals?pli=1 Site the reason as "outdated content" and Google will over write the cached data when they re-index the web pages. Just fill in the form from the link above and enter a word that is still cached but not on the live site and they will send a response within 48 hours. You will need to have a Google account to do this. It may take longer than 48 hours for the re-indexing to overwrite the record.

Appendix E – OPM Announcement

July 24, 2015

Contact: OPM Office of Communications
(202) 606-2402 or media@opm.gov

OPM ANNOUNCES STEPS TO PROTECT FEDERAL WORKERS AND OTHERS FROM CYBER THREATS

WASHINGTON, D.C. –

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. Throughout this investigation, OPM has been committed to providing information in a timely, transparent and accurate manner. As information has become available and verifiable, the agency has updated Congress, the Inspector General, Federal employee representatives, and – most importantly – those that are affected. Today's announcement is the latest in this series of updates, 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 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 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.

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

- 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.

- **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.
- **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.

- **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.

- **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.

Continuing to strengthen OPM cybersecurity. OPM continues to take aggressive action to strengthen its broader cyber defenses and information technology (IT) systems, in partnership with experts from DOD, the Department of Homeland Security, the Federal Bureau of Investigation, and its other interagency partners. As outlined in its recent Cybersecurity Action Report, in June, OPM identified 15 new steps to improve security, leverage outside expertise, modernize its systems, and ensure internal accountability in its cyber practices. This includes completing deployment of two-factor Strong Authentication for all users, expanding continuous monitoring of its systems, and hiring a new cybersecurity advisor.

OPM has initiated a comprehensive review of the architectural design of OPM's IT systems, to identify and immediately mitigate any other vulnerability that may exist, and assess OPM's data sharing and use policies. That review is ongoing. In addition, OPM will also continue to participate in a Federal Government-wide 30-day cybersecurity sprint, whereby immediate steps are being taken to further protect information and assets and improve the resilience of Federal networks, and will participate in a 90-day interagency review of key questions related to information security, governance, policy, and other aspects of this the security and suitability determination process, to ensure that it is conducted in the most efficient, effective and secure manner possible.

The Director and Office of Personnel Management are committed to protecting the safety and security of the information of Federal employees and contractors. OPM is also committed to helping those that have been impacted by this incident, safeguarding its systems and data, and fulfilling its mission to serve Federal workers.

- END -