INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES and RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

ISOO Notice 2015-04: Update on Recent Cyber Incidents at OPM

July 10, 2015

The following notice provides an update on the recent cyber incidents at the U.S. Office of Personnel Management (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

On 9 July 2015, 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. ISOO and OPM will continue to provide additional information going forward.

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:

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.

BACKGROUND INVESTIGATIONS INCIDENT FAQS

What happened

What happened and when?
OPM recently discovered two cyber security incidents that have impacted the data of Federal government employees, contractors, and others:

In April 2015, OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. This means information such as full name, birth date, home address and Social Security Numbers were affected. This number has not changed since it was announced by OPM in early June and you should have already received a notification if you were impacted.

While investigating this incident, in early June 2015 OPM then discovered that additional information had been compromised: including background investigation records of current, former, and prospective Federal employees and contractors. OPM and the interagency incident response team have 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 1.8million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. Notifications for this incident have not yet begun.

While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel or those who have applied for a Federal job were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

OPM and an interagency team from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) have been investigating these incidents. Based upon the analysis and forensics to date, the interagency incident response team assesses that the adversary is no longer active on OPM's network. At this point, it is most likely that no new significant information about exfiltration will be found regarding these incidents.

How many people were affected by these incidents?
In the personnel data incident, the number of affected individuals is 4.2 million people. In the background investigations incident, it is 21.5 million people. There is an overlap of 3.6 million people who were included in both incidents. Therefore, 22.1 million people are affected by the overall intrusion.

Who is responding to these incidents?
OPM has partnered with the U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT), and the Federal Bureau of Investigation (FBI) to investigate and determine the full impact to Federal personnel. Federal law enforcement agencies continue to investigate the matter and assist with remediation efforts.

Is the threat now resolved?
Based upon analysis and forensics to date, the interagency incident response team assess that the adversary is no longer active on OPM's network.

What information was affected

What information is included in a background investigation?

Types of information involved in the **background investigation records** incident that may have been impacted:

- 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 also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

Note: While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

What is a background investigation?

OPM conducts background investigations to assist agencies in determining whether an individual is trustworthy, reliable, and of good conduct and character for Federal employment.

OPM has a responsibility, where appropriate, to conduct investigations of individuals who will occupy positions that could impact national security, including positions requiring access to classified national security information. The amount of information requested depends on the risk to the public trust, the impact on the national security, and whether an individual has a job that requires access to classified national security information. To see the different forms: (SF-86, SF-85, or SF-85P)

In general, background investigation forms collect personal information for people occupying positions with the Federal government, including SSNs to:

- Check criminal histories;
- Validate background investigation applicants' educations;
- Validate employment histories;
- Validate background investigation applicants' living addresses; and
- Gain insight into the character and conduct of background investigation applicants, through checks of references.

In addition, some people occupying public trust or national security provide additional types of information that may include:

- Personal information of a spouse or a cohabitant (including SSNs);

- Personal information of parents, siblings, other relatives, and close friends (but does not include SSNs);
- Foreign Countries visited and individuals the applicant may know in those countries;
- Current or previous treatment for mental health issues; and/or
- Use of illegal drugs.

For public trust and national security investigations, other information may be collected related to parents, siblings, other relatives, close friends, and previous places a background investigation applicant may have lived, worked, or attended school. This information is used to interview employers, friends, and neighbors about the applicant, their conduct, and personal history, and to conduct local law enforcement checks at previous locations lived.

Who has been affected

Have I been affected by the background investigation records incident?
Social Security Numbers (SSNs) of 21.5 million individuals were 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.

If you 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 you are impacted by this cyber breach. If you underwent a background investigation prior to 2000, you still may be impacted, but it is less likely.

If you are one of the following, you may have been affected:

- Current or former Federal government employee
- Member of the Military, or Veteran
- Current or former Federal contractor
- Job candidate required to complete a background investigation before your start date
- Spouse, co-habitant, minor child, close contact of any of the above groups

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.

In the coming weeks, we will be sending you a notification package, which will provide details on the incident and information on how to access these services. That package will also include detailed information that you can provide to the people you 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.

Who else in my family or other networks is affected by the background investigation incident? How can I determine who these people are?

When you submitted your background investigation, you likely provided the name, address, date of birth, or other similar information of close contacts may have been listed on background investigation forms. 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.

Am I affected by the incident involving personnel data?
Current or former Federal employees may have been affected by the incident involving **personnel data**. (4.2 million current and former Federal employees have been affected). Contractor employees were not affected by this. OPM has sent notifications to those impacted.
How are Federal retirees affected?
For the **background investigation records incident**, for those that underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P), it is highly likely that they are impacted by this cyber breach. This could include retirees. Individuals that submitted this information prior to 2000 may be impacted, but it is less likely.

In the **personnel data incident**, retirees may have been affected. OPM has sent notifications to those impacted.

While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

How are postal workers affected?
For the **background investigation records incident**, for those that underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P), it is highly likely that they are impacted by this cyber breach. This could include postal workers. Individuals that submitted this information prior to 2000 may be impacted, but it is less likely.

In the **personnel data incident**, postal workers may have been affected. OPM has sent notifications to those impacted.

While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

How were Congressional staff affected?
For the **background investigation records incident**, for those that underwent a background

investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P), it is highly likely that they are impacted by this cyber breach. This could include Congressional staff. Individuals that submitted this information prior to 2000 may be impacted, but it is less likely.

In the **personnel data incident**, Congressional staff may have been affected. OPM has sent notifications to those impacted.

While background investigation records do contain some information regarding mental health and financial history provided by applicants and people contacted during the background investigation, there is no evidence that health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

How are non-appropriated fun (NAF) employees affected?
For the **background investigation records incident**, for those that underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P), it is highly likely that they are impacted by this cyber breach. This could include NAF employees. Individuals that submitted this information prior to 2000 may be impacted, but it is less likely.

In the **personnel data incident**, some Department of the Army NAF employees were affected. OPM has sent notifications to those impacted.

Getting notified if your data was compromised

How and when will I be notified if my information was compromised?
In the coming weeks, OPM will begin sending notification letters to people whose Social Security Number appeared on files impacted by the **background investigation records** incident. These individuals include current, former, and prospective Federal employees and contractors and their spouses or co-habitants that are listed on background investigation forms. Each of these individuals will be personally contacted 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 for at least three years. Some individuals may also receive additional contact via email where appropriate. 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.

For the **personnel data** incident, OPM has sent notifications to individuals to ensure that they are provided with the appropriate support and tools to protect their personal information.

What should I do if I received a notice that my information may be compromised?
If you received a notification that your information may have been compromised in the **personnel records incident**, please follow the instructions to sign up for credit monitoring and other services.

Why are you not providing services to family members who are on the form?
In many cases, the information about these individuals is the same as what is generally available in public forums such as online directories or social media, and therefore generally does not present the same level of risk of identity theft or other issues.

These individuals are likely to include immediate family or close contacts whose name, address, date of birth, or other similar information may have been listed on a background investigation form.

Protecting your identity

What should I do if I am concerned about identity theft?
If you are concerned about identity theft, please visit FTC's identitytheft.gov to learn about setting up protections. Visit IdentityTheft.gov to learn how to:

- Spot warning signs of identity theft
- Get a free credit report
- Set up fraud alerts on your accounts
- Protect your children/minors from identity theft

What resources are available to me to protect my identity? My spouse?

For the affected **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.

For those affected by the **personnel data incident**, OPM has sent notifications to provide you with the information for how to access identity protection and insurance services. These services include 18 months of credit monitoring membership, free credit report access, identity theft insurance, and identity restoration. Regardless of whether or not you explicitly take action to enroll in the credit monitoring services, will have access to identity theft insurance and access to full-service identity restoration provided.

What is being done to address these incidents

What is OPM doing to improve their systems now?

OPM continues to take aggressive action to strengthen its broader cyber defenses and IT systems. As outlined in its recent Cybersecurity Action Report, in June, OPM identified 15 new steps to improve security, work with outside experts, modernize its system, and ensure accountability. OPM is currently completing a comprehensive review of its IT systems to find and address any potential vulnerabilities.

It is bringing in experts from in and outside of the government to help with these efforts, including a new cybersecurity advisor. OPM is also working with interagency partners on a review of key questions related to information technology governance, policy, security, and other aspects of the security clearance process, including where such data should be housed in the future.

What is the government doing to make sure all of my information elsewhere is safe?
The Federal government is taking aggressive action to continually strengthen its cyber defenses. For example, all agencies are currently engaged in a 30-day cybersecurity sprint, whereby they are taking immediate steps to further protect information and assets and improve the resilience of Federal networks. For more information, please see: Fact Sheet: Administration Cybersecurity Efforts 2015.

Please direct any questions regarding this ISOO notice to: isoo@nara.gov