Information About the Recent Cybersecurity Incident

Updated June 18, 2015

Frequently Asked Questions:

We'll continue updating these FAQs as more information becomes available. Please check back often.

Through the course of the ongoing investigation into the cyber intrusion that compromised personnel records of current and former Federal employees announced on June 4, OPM has recently discovered that additional systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective Federal government employees, as well as other individuals for whom a Federal background investigation was conducted.

This separate incident – like the one that was announced on June 4th affecting personnel information of current and former federal employees – was discovered as a result of OPM's aggressive efforts to update its cybersecurity posture, adding numerous tools and capabilities to its network.

OPM, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI) are working as part of this ongoing investigation to determine the number of people affected by this separate intrusion. OPM will notify those individuals whose information may have been compromised as soon as practicable. OPM will provide updates when we have more information on how and when these notifications will occur.

OPM remains committed to improving its security capabilities and has invested significant resources in implementing tools to strengthen its security barriers. Additionally, the Office of Management and Budget (OMB) has instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks.

For those individuals potentially affected by the incident announced on June 4 regarding personnel information, OPM is offering affected individuals credit monitoring services and identity theft insurance in order to mitigate the risk of fraud and identity theft with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services and is available immediately at no cost to affected individuals identified by OPM. Additional information is available on the company's website, (external link) and by calling toll-free 844-777-2743 (International callers: call collect 512-327-0705).

Protecting the integrity of the information OPM maintains is the agency's highest priority. OPM continually evaluates our IT security protocols to make sure that sensitive data is protected to the greatest extent possible, across all networks. Because cybercrime is an evolving and pervasive

threat, we are continuously working to identify and mitigate threats when they occur. The following are some key reminders of the seriousness of cyber threats and of the importance of vigilance in protecting our systems and data.

Steps for Monitoring Your Identity and Financial Information

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com (external link) or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website. (external link)
- Review resources provided on the FTC identity theft website. (external link) The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place 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.

Precautions to Help You Avoid Becoming a Victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy. (external link)
- Pay attention to the URL of a website. Malicious websites 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 are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website 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. (external link))
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls; (external link) Understanding Anti-Virus Software; (external link) and Reducing Spam. (external link)

- Take advantage of any anti-phishing features offered by your email client and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center. (external link)
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.identitytheft.gov (external link). The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.

  Identity Theft Clearinghouse
  Federal Trade Commission
  600 Pennsylvania Avenue, NW
  Washington, DC 20580
  www.identitytheft.gov (external link)
  1-877-IDTHEFT (438-4338)
  TDD: 1-202-326-2502

Frequently Asked Questions

Updated June 18, 2015

What happened? Was there one intrusion or two?

OPM became aware of an intrusion affecting its systems and data in April 2015 and launched an investigation with its agency partners, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). In May 2015, through this investigation, OPM became aware of the potential compromise of data related to personnel records for current and former Federal employees. The agency began notifying potentially affected individuals on June 8. OPM is currently in the process of sending notifications to the approximately 4 million individuals whose personally identifiable information (PII) may have been compromised in that incident. Since the investigation is ongoing, additional PII exposures may come to light; in that case, OPM will conduct additional notifications as necessary.

During the ongoing investigation into the cyber intrusion of OPM that compromised personnel records (announced June 4), OPM, with its interagency partners, became aware of the possibility of a separate intrusion affecting a different set of OPM systems and data.

On June 8, as the investigation into the initial intrusion proceeded, the Interagency Response Team shared with relevant 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.

OPM, DHS, and the FBI are working as part of this ongoing investigation to determine the number of people affected by this separate intrusion. Since the investigation is ongoing, we are in the process of assessing the scope of the information that has been compromised, but we expect OPM will conduct additional notifications as necessary.

Am I affected by the breach of personnel records? Can I expect to receive a notification that any of my records were involved?

As part of our ongoing notification process, we are committed to providing the most up-to-date information to ensure affected individuals have the necessary resources and information available to protect their interests and security. OPM is continuing to examine the data and systems that may have been compromised. For example, we have confirmed that any Federal employee from across all branches of government whose organization submitted records to OPM for future retirement processing may have been compromised—even if their full personnel file is not stored on OPM's system.

These individuals were included in OPM's initial estimate of approximately 4 million individuals whose data may have been compromised and are currently being notified. These records include service history records (such as the SF 2806), court orders, and other records and information that pertain to annuity calculations. The Personally Identifiable Information (PII) contained in these records includes name, Social Security numbers, dates of birth, and possibly other sensitive information.

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.
- They 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 moves from one agency or organization to another.
    - When an individual separates from an organization.
    - When an individual retires from an organization.
    - When an organization has a change in payroll service center.

If you are unsure whether your organization submits related documentation to OPM to support future retirement processing, please contact your organization's Human Resources Office.

How will I be notified if my data is affected?

OPM began conducting notifications to individuals whose personnel records were affected using email and/or USPS First Class mail on a rolling basis from June 8, 2015 through June 19, 2015. However, it may take several days beyond June 19 for a notification to arrive.

In the case of the incident involving background investigations information, the investigation is still ongoing, and we will notify affected individuals as soon as is practicable. As with any such event, it takes time to conduct a thorough investigation and to identify the affected individuals.

What information was compromised in the intrusion involving personnel records?

OPM maintains personnel records for the Federal workforce. The kind of data that may have been compromised includes your name, Social Security number, date and place of birth, and current and former addresses. It could include the type of information you would typically find in a personnel file, such as job assignments, training records, and benefit selection decisions. The notifications to potentially affected individuals will state exactly what information may have been compromised.

In the case of the incident involving background investigations information, the investigation is still ongoing, and we will notify affected individuals if their data was affected as soon as is practicable. As with any such event, it takes time to conduct a thorough investigation and to identify the affected individuals.

Was background clearance information was compromised?

During the investigation into the cyber intrusion of OPM that compromised personnel records (announced June 4), OPM, with its interagency partners, became aware of the possibility of a separate intrusion affecting a different set of OPM systems and data.

On June 8, as the investigation into the initial intrusion proceeded, the response team shared with relevant 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.

Since the investigation is ongoing, additional exposures may come to light. In that case, OPM will conduct additional notifications as necessary.

How many people were affected by both incidents? Do you have an estimate?

OPM is currently in the process of sending notifications to approximately 4 million current and former Federal civilian employees whose personally identifiable information (PII) may have been compromised in the incident impacting personnel records. It is important to note that this is an ongoing investigation that could reveal additional exposures. If that occurs, OPM will conduct additional notifications as necessary.

Were members of the military or contractors affected by either breach?

As of now, we do not believe the first incident involved personnel records of active military personnel. It did affect current and former Department of Defense civilian employees. Additionally, in the first incident, no contractors were affected unless they previously held Federal civilian positions.

However, since the investigation is ongoing, additional exposures may come to light; in that case, OPM will conduct additional notifications as necessary.

Are Federal retirees affected by either breach?

Some Federal retirees are affected by the incident involving personnel records announced on June 4 and they are among the approximately 4 million current and former Federal civilian employees receiving notifications. We have not yet determined the scope and impact of the separate incident involving background investigation data. Since the investigations into both incidents ongoing, additional exposures may come to light; in that case, OPM will conduct additional notifications as necessary.

Have the police been notified?

Since both incidents were identified, 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. OPM immediately implemented additional security measures and will continue to improve security for the sensitive information it manages.

When did this happen?

OPM became aware of the intrusions into its systems in April (affecting personnel records) and May (affecting background investigations data) of 2015 after implementing tough new measures to deter and detect cyberattacks. The actual intrusions predated OPM's discovery, but the precise timing is still a matter under investigation.

Was the data that was exfiltrated encrypted?

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 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.

What systems were affected?

For security reasons, OPM cannot publicly discuss specifics of the systems that might be affected by the compromise of personnel data. Additionally, due to the ongoing investigation, it would be inappropriate to publicly provide information that may impact the current work by law enforcement. OPM has added additional security controls to better protect overall networks and systems and the data they store and process.

Why didn't OPM tell affected individuals about the loss of the data sooner?

OPM became aware of the first intrusion in April 2015. OPM worked with US-CERT and the FBI as quickly as possible to assess the extent of the malicious activity and to identify the records that may have been compromised. In May 2015, through this investigation, OPM became aware of the potential compromise of data related to personnel records for current and former Federal employees. During the investigation into the cyber intrusion of OPM that compromised personnel records (announced June 4), OPM, with its interagency partners, became aware of the possibility of a separate intrusion affecting a different set of OPM systems and data involving background investigations.

As with any such event, it takes time to conduct a thorough investigation and to identify the affected individuals.

What is OPM doing to prevent this kind of loss from happening again?

We are committed to making this right and are investing the internal processes, tools, and resources to reduce the likelihood that this can happen again. Because cyber threats are evolving and pervasive, OPM is continuously working to identify and mitigate threats when they occur. OPM evaluates its IT security protocols on a continuous basis to make sure that sensitive data is protected to the greatest extent possible, across all networks where OPM data resides—including those managed by government partners and contractors.

What has OPM done to shore up its systems?

OPM has been making steady improvements in its cybersecurity posture over the past year. In February 2014, OPM Director Archuleta, in one of her first major initiatives as the Director of OPM, developed and approved an IT Strategic Plan to bolster OPM's IT networks and databases and adopt state of the art security protocols.

This plan included upgrading Security Assessment and Authorization for several systems and implementing continuous monitoring to enhance the ability to identify and respond, in real time or near real time, to cyber threats.

Additional upgrades included the installation of more firewalls that allow us to filter network traffic; restricting remote access for network administrators and restricting network administration functions remotely; reviews of all connections to ensure that only legitimate business connections have access to the Internet; and deploying anti-malware software across the environment to protect and prevent the deployment or execution of cybercrime tools that could compromise out networks.

That undertaking resulted in OPM having tough new security measures in place by the spring of this year. That is the reason the agency was able to detect in April 2015 an intrusion that happened some time earlier. The agency immediately began working with relevant Federal agencies, DHS, and the FBI to investigate and mitigate the intrusion.

After the incidents were discovered, OPM also immediately implemented additional security measures and will continue to add protections for the sensitive information it manages.

Has the information been misused?

At this time, we have no evidence that there has been any use or attempted use of the information compromised in this incident. This is an ongoing investigation and OPM will continue to be vigilant to ensure that necessary security measures are in place to further strengthen and protect our networks, systems, and data.

What are the risks of identity theft with the information that was compromised?

Receiving a notice – email or letter – does not mean that the recipient is a victim of identity theft. OPM is recommending that people review their notices and the recommendations provided. In order to mitigate the risk of fraud and identity theft, we are offering credit monitoring service and identity theft insurance for 18 months. Every affected individual, regardless of whether or not they explicitly take action to enroll, will have $1 million of identity theft insurance and access to full-service identity restoration.

How long will it take to inform all the potential victims involved in the incidents?

OPM began conducting notifications to individuals whose personnel records were affected using email and/or USPS First Class mail on June 8, 2015 and will continue notifications on a rolling basis through June 19, 2015. It may take several days beyond June 19 for a notification to arrive by email or mail.

In the case of the incident involving background investigations information, the investigation is still ongoing, and we will notify affected individuals as soon as is practicable. As with any such event, it takes time to conduct a thorough investigation and to identify the affected individuals.

Who is responsible for this incident?

OPM does not assign attribution for cybercrimes. That question is best addressed by law enforcement agencies.

Can you say with confidence that the adversary is not currently in the system?

At this time, we have no indications that the actors remain in the OPM networks. The agency's enhanced security measures not only enabled us to detect the intruder, but have allowed us to identify, isolate, and prevent even sophisticated actors who are using new techniques. It is also worth noting that the malicious activity that OPM found was latent; the intrusions occurred well before they were discovered by OPM.

However, this is an ongoing investigation and we are still getting new information on what occurred on OPM's networks.

Can my family members also receive services if they are part of my file/records?

At this time, we have no evidence to suggest that family members of employees were affected by the breach of personnel data. Since the investigation relating to the breach of background investigation data is ongoing, additional exposures may come to light. In that case, OPM will conduct additional notifications as necessary.

May employees be granted duty time and use government telephones and computers to contact CSID to determine whether their employment information was accessed and to register for identify theft coverage?

OPM strongly encourages agencies to allow employees to contact CSID while on duty time. If an employee does not have Internet access, OPM strongly encourages agencies to work with those individuals, as appropriate, to provide them access.

What has been the operational or mission impact to OPM?

There has been no operational impact to OPM. The agency has continued to operate at full capacity since the incident occurred.

I haven't gotten an email or a letter yet. Does this mean I am not affected?

For those individuals potentially affected by the incident announced on June 4 regarding personnel information, all notifications will be sent by June 19. Because of the volume of affected individuals, OPM is sending notifications on a rolling basis. Please note that while all emails and letters will be mailed by June 19 it may take several days beyond June 19 for notification to arrive.

Since the investigation is ongoing, additional exposures may come to light; in that case, OPM will conduct additional notifications as necessary.

I received an email from opmcio@csid.com. Is this email from OPM, or is this a phishing scam?

OPM has contracted with a firm called CSID to help it send notifications as quickly as possible. For those individuals potentially affected by the incident involving personnel information, the emails will come from the sender "OPM CIO" from this address: opmcio@csid.com.

If you get an email about the breach from a different address, it may be phishing, which is defined as a criminal effort to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. Do not click on any links or provide any personal information if you suspect an email is phishing.

In a valid email, there will be a link in the body of the email that takes you to www.csid.com/opm (external link), where you will need to click the "Enroll Now" button and provide your information. When you enroll, you will be required to provide personal information to begin your credit monitoring services.

If you would like to confirm that the email you received is valid, contact your agency's privacy officer. The government's privacy officers have been provided information by OPM to help them validate the emails for you.

How will OPM contact me if I no longer work for the government? What if I have changed agencies once or multiple times in recent years?

For those individuals potentially affected by the incident involving personnel information (June 4 announcement) who 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.

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.

Since the investigation is ongoing, additional exposures may come to light; in that case, OPM will conduct additional notifications as necessary.

What is OPM doing to make sure Federal employees are protected?

OPM is currently in the process of sending notifications to individuals whose personally identifiable information (PII) may have been compromised by the incident involving personnel records. Since the investigation is ongoing, additional exposures may come to light; in that case, OPM will conduct additional notifications as necessary.

In addition, OPM has been working with the leadership of affected Federal agencies to inform them to the fullest extent possible what data was compromised so that each affected Federal employee has the resources available to protect their interests.

In order to mitigate the risk of fraud and identity theft, OPM is offering credit report access, credit monitoring services, and identity theft insurance to potentially affected individuals, at no cost to them. The comprehensive, 18-month membership includes credit monitoring and $1 million in identity theft protection services.

Additionally, it is an important reminder that we discovered this incident as a result of OPM's concerted and aggressive efforts to strengthen its cybersecurity capabilities and protect the security and integrity of the information entrusted to the agency. Accordingly, OPM has been working with the Department of Homeland Security and the Office of Management and Budget to determine what steps can be taken to accelerate already planned network and systems enhancements and institute the necessary tools to detect and mitigate emerging cyber threats.

I received a notification that my personally identifiable information may have been exposed, but it came from the Department of Homeland Security. Is this the same incident?

This is a separate incident involving Department of Homeland Security employees. Please refer to the DHS-specific cybersecurity intrusion page for more information: www.dhs.gov/intrusion (external link).

I am undergoing a background investigation and have been asked to complete my SF-86 (or provide information pertaining to someone else's background investigation) but understand that the systems that house OPM's background investigations data have been compromised. Can I be assured that the data I submit is secure?

OPM remains committed to improving its security capabilities and has invested significant resources in implementing tools to strengthen its security barriers. Additionally, the Office of Management and Budget (OMB) has instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks.

OPM continues to process background investigations and is working closely with OMB, the Department of Homeland Security and other experts across the government to detect and thwart evolving and persistent threats.

Protecting the security and integrity of the information entrusted to OPM is central to our mission, and we will continue to keep you apprised as the investigation continues.