

YOUR PERSONAL INFORMATION: PROTECTING IT FROM EXPLOITATION

Data breaches involving personal information result in a broad range of risks to individuals and organizations. This includes identity theft, targeting of individuals with knowledge of sensitive government information and internal business processes, and other intelligence activities that use personal information of U.S. citizens to undermine national security.

It is in our collective interest that we take actions to limit the risk of our personal information being exploited, and that we are able to recognize any indicators that we may be the target of such activities.

Confirmation that your personal information has been accessed in a data breach is not a guarantee that your information will be misused or that you will be targeted for further exploitation. However, it is important to remain mindful of the risk of such misuse or exploitation. The following information is provided to raise your awareness to this possibility and to help you understand how your personal information may be used by foreign intelligence services, and other “bad actors” (extremists, criminals, hackers, and the like).

The information below is provided to raise awareness and provide guidance for mitigating risks; it is not intended to indicate that the government has observed particular adverse effects from data compromises.

GENERAL AWARENESS AND PROTECTION GUIDANCE

All individuals potentially affected by a breach should be wary of suspicious activities indicating their personal information has been or is being exploited, and follow these protective measures, including:

- Do not provide additional or detailed information about yourself, your family or associates, or your position with any individual who has an unusual or heightened interest in you, or your family and associates;
- Do not share personal, financial, or sensitive information if you are contacted by unknown individuals or groups via e-mail, instant messaging or text, telephone, social media interaction, and personal encounters;
- Do not open attachments or click on links embedded in emails, instant messages or texts from unknown senders, senders who would be unlikely to send an email directly to you, and even from known senders with grammatical errors, misspellings, or if there is no text with the attachment or link;
- Install and maintain up-to-date anti-virus and anti-malware software to guard against viruses, other malicious code, and pop-ups that can appear if your computer is infected;
- Transmit electronic information safely using encryption and by using secure, known websites (e.g., with addresses starting with “https” rather than “http”);
- Share electronic files and photographs only with those you know as they contain embedded metadata such as identity, date and time, and location information;
- Select the highest level of privacy settings on your electronic devices and applications;
- Monitor your credit history and activity through a reputable credit bureau and your account statements for any unauthorized or unusual entries. Free credit reports can be obtained at: <http://www.consumer.ftc.gov/articles/0155-free-credit-reports>;
- Maintain direct positive control of, or leave at home, electronic devices during travel, especially when traveling out of the U.S.;
- Know the locations and contact information for U.S. embassies, consulates, and other diplomatic establishments for any issues or emergencies when

REPORTING

To protect yourself and your family, we urge all affected individuals to exercise caution and remain vigilant to any events appearing out of the ordinary or suspicious.

If you believe you have observed activity related to a personal data compromise or suspect your personal information has been exploited, report your concern promptly as instructed by your leadership.

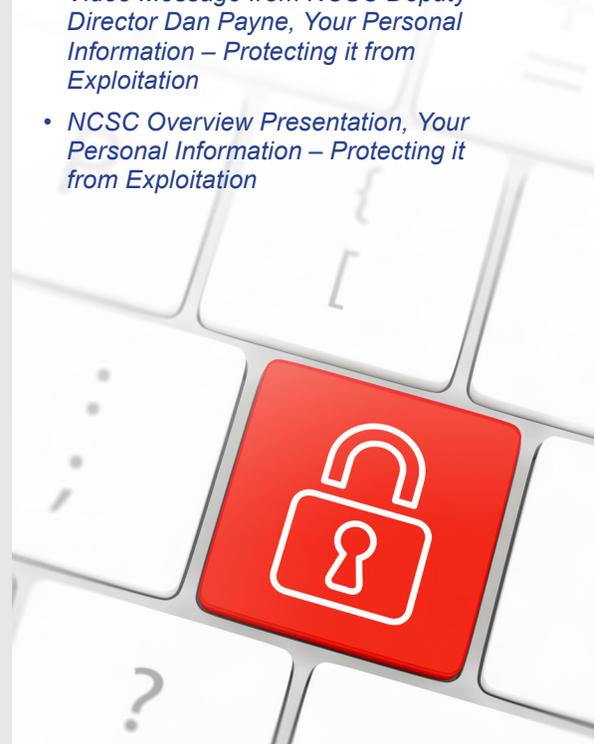
The appropriate Federal government sites may also be used to report specific incidents:

- Report any suspected instances of identity theft to the FBI’s Internet Crime Complaint Center at www.ic3.gov.
- If you notice fraudulent activity, go to the Federal Trade Commission (FTC) website (www.ftc.gov/idtheft or www.identitytheft.gov) and complete an ID theft complaint form and place a fraud alert on your credit report.
- Report unexplained activity related to criminal behavior to the local police department. Provide them with a copy of the FTC form and request a copy of the police report.

More Information:

Additional information can be found at the ncsc.gov web site, including:

- Video Message from NCSC Deputy Director Dan Payne, *Your Personal Information – Protecting it from Exploitation*
- NCSC Overview Presentation, *Your Personal Information – Protecting it from Exploitation*



traveling out of the country. This information can be found at: <http://www.state.gov/misc/list/index.htm>;

- *Report per your department, agency, or company instructions, all suspicious activity, events, or individuals you, relatives, and associates encounter; and*
- *Share these general awareness and protection guidelines with relatives and associates as appropriate. Avoid misconduct or behaviors that leave you vulnerable to blackmail, coercion, or recruitment.*

HOW YOU MIGHT BECOME A VICTIM

SOCIAL ENGINEERING is the term used to describe bad actors using information they have discovered either legally or illegally about you to gain your trust and extract further information or manipulate you to take actions you would not otherwise take.

The use of stolen personal information by cyber operators is highly valuable for social engineering as it can be used to create a compelling illusion that you already know an individual or have a shared interest with them. It opens a means to contact you in either cyber space or the physical world to foster that trust or do harm.

Examples of how bad actors may use your personal information for social engineering and other purposes include:

PHISHING (or spearphishing) is a common method used to contact people through email. With phishing, bad actors use social engineering to target their victims and lure them into taking actions that could ultimately compromise their computer or network. Examples include getting a victim to open a malicious attachment or clicking on a bogus embedded link. Like other social engineering attacks, spear phishing takes advantage of a victim's most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, or respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events. Those who "take the bait," become unwitting participants in a computer network attack by allowing the attackers to bypass many of our technical defenses.

Phishing scams also trick you into providing your confidential information, which is then used to access your accounts. Typically this kind of fraud

involves an email, text message, or pop-up window claiming to come from an official source.

SOCIAL MEDIA DECEPTION (including Facebook, Twitter, Google and LinkedIn) provides bad actors with an avenue to connect to their victims. Attackers may create a fake profile to befriend their victims while posing as a former acquaintance, job recruiter, or someone with a shared interest. Using a fake online persona, an attacker may try and get their victims to reveal more information about themselves or their employers, or they may simply collect more information about their victims from your social media postings.

HUMAN TARGETING is often used by foreign governments to target individuals with access to information of interest to them. For instance, you may unexpectedly meet someone at a venue of interest, such as a conference or child's school event, who shares your interests or views and establishes an ongoing relationship. Your new friend may test you by getting you to do seemingly small "favors" for them or getting you to talk about trivial work-related information. Over time, trivial information may lead them to information that is of interest.

TRAVEL VULNERABILITIES are greater than usual, especially if you are traveling outside of the U.S., as it is common for you to encounter unfamiliar people. Also, your guard may be down because you are traveling for vacation, training, or other relaxing purposes. Therefore, take extra precaution of:

- *Those who approach you in a friendly manner and seem to have a lot in common with you--especially if they wish to maintain contact with you once you return home.*
- *Interactions in social settings where you find you are unusually successful in meeting and impressing others.*

- *A seemingly random and/or other foreign acquaintance who has heightened interest in your work or introduces you to a third party who then wants to continue to meet with you.*

UNSOLICITED TELEPHONE AND TEXT MESSAGES

from toll-free numbers can be set up quickly and sometimes exist solely for the purpose of capturing your confidential information, often simply by playing a prerecorded message about your accounts being in trouble. The message prompts you to enter your 16-digit account number. This is followed by a request for your PIN and other personal information. Or you may receive a text message or a phone call with a prerecorded message that describes an urgent situation that requires immediate action. The message may say, "Your account has been blocked. Please call 800-123-4567 to unlock it." Before you realize you're being scammed, you've given enough information to duplicate your card and access your accounts.

IDENTITY IMPERSONATION is acquiring key pieces of your confidential information, such as your name, address, birthdate, Social Security number, and mother's maiden name, in order to commit fraud. Identity Impersonation can be used as a tactic for corporate exploitation via the newly acquired identity. With this information, an identity thief can take over your financial accounts; open new bank accounts; purchase automobiles; apply for loans, credit cards, and Social Security benefits; rent apartments; and establish services with utility and phone companies, all in your name.





July 15, 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:

- 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.

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.

Director Archuleta has initiated a comprehensive review of the architectural design of OPM's IT systems, to identify and immediately mitigate any other vulnerabilities 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.

Director Archuleta and the entire 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 -

DRAFT AND PRE-DECISIONAL

Dear Colleagues,

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

Update from OPM:

Today, the U.S. Office of Personnel Management (OPM) announced the results of the interagency forensics investigation into a recent cyber incident involving Federal background investigation data and the steps it is taking to protect those impacted. DoD 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:

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

- Full service identity restoration support and victim recovery assistance
- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

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

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

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

The notification package that will be sent to background investigation applicants will include detailed information that the applicant can provide to

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

- 3. Establishing an online cybersecurity incident resource center** – Today, OPM launched a new, online incident resource center - located at <https://www.opm.gov/cybersecurity> - to offer information regarding the OPM incidents as well as direct individuals to materials, training, and useful information on best practices to secure data, protect against identity theft, and stay safe online. This resource site will be regularly updated with the most recent information about both the personnel records and background investigation incidents, responses to frequently asked questions, and tools that can help guard against emerging cyber threats.
- 4. Establishing a call center to respond to questions** – In the coming weeks, a call center will be opened to respond to questions and provide more information. In the interim, individuals are encouraged to visit <https://www.opm.gov/cybersecurity>. Individuals will not be able to receive personalized information until notifications begin and the call center is opened. OPM recognizes that it is important to be able to provide individual assistance to those that reach out with questions, and will work with its partners to establish this call center as quickly as possible.
- 5. Protecting all Federal employees** – In the coming months, the Administration will work with Federal employee representatives and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

In conclusion, I want you to know that I am as concerned about these incidents as you are, and we want to ensure you that we are in constant contact with OPM. The Department's entire leadership is committed to providing you with the most recent resources and support, and we want to keep on hearing from you. Please send your feedback and questions to DOD.DATA.BREACH.QUESTIONS@MAIL.MIL. Thank you.