Cybersecurity Incidents

Archived: 2026-04-05 18:47:49 UTC

What Happened

In 2015, OPM announced **two separate but related cybersecurity incidents** that have impacted the data of Federal government employees, contractors, and others:

1. In June 2015, OPM discovered that the **background investigation records of current, former, and prospective Federal employees and contractors had been stolen.** 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 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 5.6 million include 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 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).

2. Earlier in 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.

Back to Top

How You May Be Affected

If you underwent a Federal background investigation in 2000 or afterwards (which occurs through the submission of forms SF-86(PDF file), SF-85(PDF file), or SF-85P(PDF file) for either a new investigation or a reinvestigation), it is highly likely that you were impacted by the incident involving background investigations. If you underwent a background investigation prior to 2000, you still may have been impacted, but it is less likely. Current or former Federal employees may also have been impacted by the separate but related incident involving personnel records.

Learn more about who was impacted and the protections we are working to put into place.

- Current and former Federal government employees

- If you are a current or former Federal government employee, including members of the U.S. military, your data may have been impacted by the incident announced in 2015 impacting **background investigation records**. Current or former Federal government employees may also have been impacted by the separate incident involving **personnel records**.

    - 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 could also include:

        - Findings from interviews conducted by background investigators
        - Fingerprints
        - Usernames and passwords used to fill out your forms

      If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

    - Types of information involved in **personnel records** incident include:
        - Name
        - Social Security number
        - Date and place of birth
        - Current and former addresses
        - Common personnel file information such as job assignments, training records, and benefit selection decisions

    Services available to you:

    If your data was impacted by the **background investigation records incident or personnel records incident**, you should have received a notification letter and PIN code in the mail providing details on the incident and the services available to you and your minor dependent children, such as:

    - Full service identity restoration, which helps to repair your identity following fraudulent activity. Those impacted by the background investigation incident can review the identity theft monitoring and restoration services information.
    - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
    - Continuous identity and credit monitoring.

Instructions on how to enroll in other services were included in your notification. If you have not yet received a notification but believe you were impacted by the 2015 cybersecurity incidents, please visit the Verification Center.(external link)

- Active duty servicemembers and veterans
    - If you are an active duty servicemember or veteran, you may have been impacted by the 2015 incident impacting **background investigation records**. We have no evidence to suggest that active duty servicemembers or veterans were affected by the **personnel records incident**.

      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 could also include:

        - Findings from interviews conducted by background investigators.
        - Fingerprints
        - Usernames and passwords used to fill out your forms

      If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

      Services available to you:

      If your data was impacted by the **background investigation incident**, you should have received a notification letter and PIN code in the mail providing details on the incident and the services available to you and your minor dependent children, such as:

        - Full service identity restoration, which helps to repair your identity following fraudulent activity. Those affected by the background investigation incident can review the identity theft monitoring and restoration services information.
        - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
        - Continuous identity and credit monitoring
- Current and former Federal contractors
    - Current or former Federal contractors may have been impacted by the 2015 incident impacting **background investigation records**. We have no evidence to suggest that current or

former Federal contractors were affected by **personnel records incident**.

Types of information in the incident **involving background investigation records**:

- Social Security Numbers
- Residency and educational history
- Employment history
- Information about immediate family and personal and business acquaintances
- Health, criminal and financial history

Some records could also include:

- Findings from interviews conducted by background investigators
- Fingerprints
- Usernames and passwords used to fill out your forms

If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

Services available to you:

If your data was impacted by the **background investigation incident,** you should have received a notification letter and PIN code in the mail providing details on the incident and the services available to you and your minor dependent children, such as:

- Full service identity restoration, which helps to repair your identity following fraudulent activity. Those affected by the background investigation incident can review the identity theft monitoring and restoration services information.
- Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
- Continuous identity and credit monitoring

- Job candidates for federal employment who were required to complete a background investigation
    - Candidates who were required to complete a background investigation form prior to employment may have been impacted by the 2015 incident affecting **background investigation records**. We have no evidence to suggest that job candidates were affected by the **personnel records incident**.

      Types of information in background investigation 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

      Some records could also include:

    - Findings from interviews conducted by background investigators
    - Fingerprints
    - Usernames and passwords used to fill out your forms

  If you may have used your e-QIP (the online system used to process forms) password for other accounts or services, you should change your passwords for those accounts immediately and not reuse any passwords that you used in the e-QIP system.

  Services available to you:

  If your data was impacted by the **background investigation incident** you should have received a notification letter and PIN code in the mail providing details on the incident and the services available to you and your minor dependent children, such as:

    - Full service identity restoration, which helps to repair your identity following fraudulent activity. Those affected by the background investigation incident can review the identity theft monitoring and restoration services information.
    - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
    - Continuous identity and credit monitoring

- Spouses and co-habitants of current and former Federal employees, contractors, and job candidates whose information was stolen

  - If your information was listed on a background investigation form by a spouse or co-habitant, the stolen information may include your name, Social Security number, address, date and place of birth, and in some cases, your citizenship information.

    Services available to you:

    If your data was impacted by the **background investigation incident** you should have received a notification letter and PIN code in the mail providing details on the incident and the services available to you and your minor dependent children, such as:

    - Full service identity restoration, which helps to repair your identity following fraudulent activity. Those affected by the background investigation incident can review the identity theft monitoring and restoration services information.
    - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
    - Continuous identity and credit monitoring

- Immediate family, close contacts, and references of current and former Federal employees, contractors, and job candidates whose information was stolen

  - Beyond applicants and their spouses or co-habitants described above, you may be someone whose name, address, date of birth, or other similar information may have been listed on a background investigation form. In many cases, the information about these people is the same as what is generally available in public forums such as online directories or social media, and generally does

not present the same level of risk of identity theft or other issues. While services will not be provided to you at no cost, there are a number of steps you can take to protect your identity (see below).

Back to Top

What You Can Do

Here are steps you can take to protect your identity:

- Spot the warning signs of identity theft
    - Visit IdentityTheft.gov(external link) to learn how to set up protections:
        - Get a free credit report(external link)
        - Set up fraud alerts on your accounts
        - Protect your children/minors from identity theft(external link)
- Be aware of phishing scams
    - Phishing(external link) is when a fraudster impersonates a business or someone you trust in order to get your private information. Never click on links you don't trust and don't give out your personal information. Legitimate organizations never ask for your information through texts, pop-up messages, or email. Scammers may call and pretend to be from the government or a business to try to get you to give them sensitive information. If a caller asks for your information, call back using a number you know to be legitimate.
- Update your passwords
    - If the information in your background investigation forms could be used to guess your passwords or if you are using the same password that you did when you filled out your background investigation form, change them. Use complex passwords of 10-12 characters, combining letters, numbers, and special characters. Don't use something that is easily guessable for someone who knows you or has information about you. Don't repeat passwords for several accounts. For more information on how to choose a strong password, review the United States Computer Emergency Response Team's (US-CERT) tips for Choosing and Protecting Passwords(external link).
- Get up to speed on computer security
    - Review and check up on your practices for safe, secure and responsible online activity. The Federal Trade Commission(external link) lists helpful steps you can take to make sure your computer is as safe as possible. For additional information on computer security, including information about firewalls, anti-virus software, and identifying security threats, review tips and the latest cybersecurity alerts and bulletins from the US-CERT's National Cyber Awareness System(external link).
- If you think your identity has been stolen

    - If you believe your information has been misused, there are several steps you should take.
        - If you are concerned that you are **experiencing identity theft,** visit identitytheft.gov(external link). This site explains steps you can take to recover your identity.
        - If you are concerned about your **child's** identity being stolen, the Federal Trade Commission has information and resources(external link) to know what to look for and how to get help.
        - You can also file a claim with the FBI.(external link)
- Learn how to keep your information safe from exploitation
    - You can find information about the measures you can take to ensure the safety of your personal information at the National Counterintelligence and Security Center (NCSC) at http://www.ncsc.gov(external link).
- Tips for practicing safe online behavior every day
    - Practicing safer online behavior helps you protect yourself from identity theft, fraud, and other online crimes and malicious activity. Learn what you can do to protect yourself, your family, and your workplace through tips and free resources from Stop.Think.Connect™(external link), a national cybersecurity awareness campaign led by the Department of Homeland Security and the National Cyber Security Alliance.

Back to Top

What We're Doing to Help

- Supporting people who have been impacted
    - Identity theft restoration and credit monitoring services have been provided at no cost to individuals whose information was compromised in the OPM cyber incidents. Certain services are also available to the dependent minor children of impacted individuals who were under the age of 18 as of July 1, 2015. These services include:
        - Full service identity restoration, which helps to repair your identity following fraudulent activity.
        - Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.
        - Continuous identity and credit monitoring

      If you've received a notification letter and PIN code from OPM, please sign up for MyIDCare.

      Instructions on how to enroll in other services were included in your notification. If you have not yet received a notification but believe you were impacted by the 2015 cybersecurity incidents please visit the Verification Center(external link).