

Cyber Intrusion Compromise of OPM Personnel Records June 25, 2015

In June 2015, the Office of Personnel Management (OPM) announced that cyber intrusions had compromised the personnel records of some current and former Federal employees.

- OPM has posted detailed information and guidance on its website www.opm.gov (check the “What’s New” section or type “cybersecurity incidents” in the search box). OPM will update that guidance as new facts are verified.
- Below is additional guidance that was distributed by the Under Secretary of State for Management on June 19, 2015:

Dear Colleagues,

I am writing to provide you an update on the recent cyber incidents at the U.S. Office of Personnel Management (OPM) which has just been received.

On June 4th, OPM announced an intrusion impacting personnel information of approximately four million current and former Federal employees. OPM is offering affected individuals credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. Additional information is available on the company’s website, <https://www.csid.com/opm/> and by calling toll-free 844-777-2743 (international callers: call collect 512-327-0705). More information can also be found on OPM’s website: www.opm.gov.

Notifications to individuals affected by this incident began on June 8th on a rolling basis through June 19th. However, it may take several days beyond June 19 for a notification to arrive by email or mail. If you have any questions about whether you were among those affected by the incident announced on June 4, you may call the toll free number above.

On June 12th, OPM announced a separate cyber intrusion affecting systems that contain information related to background investigations of current, former, and prospective Federal Government employees from across all branches of government, as well as other individuals for whom a Federal background investigation was conducted, including contractors. This incident remains under investigation by OPM, the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). The investigators are working to determine the exact number and list of potentially affected individuals. We understand that many of you are concerned about this intrusion. As this is an ongoing investigation, please know that OPM is working to notify potentially affected individuals as soon as possible. The Department is working extensively with our interagency colleagues to determine the specific impact on State Department employees.

It is an important reminder that OPM discovered this incident as a result of the agency’s concerted and aggressive efforts to strengthen its cybersecurity capabilities and protect the

security and integrity of the information entrusted to the agency. In addition, OPM continues to work with the Office of Management and Budget (OMB), the Department of Homeland Security, the FBI, and other elements of the Federal Government to enhance the security of its systems and to detect and thwart evolving and persistent cyber threats. As a result of the work by the interagency incident response team, we have confidence in the integrity of the OPM systems and continue to use them in the performance of OPM's mission. OPM continues to process background investigations and carry out other functions on its networks.

Additionally, 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. We are working with OMB to ensure we are enforcing the latest standards and tools to protect the security and interests of the State Department workforce.

We will continue to update you as we learn more about the cyber incidents at OPM. OPM is the definitive source for information on the recent cyber incidents. Please visit OPM's website for regular updates on both incidents and for answers to frequently asked questions: www.opm.gov/cybersecurity. We are also interested in your feedback and questions on the incident and our communications. You can reach out to us at DG DIRECT (DGDirect@state.gov) with these comments.

State Department employees who want to learn additional information about the measures they can take to ensure the safety of their personal information can find resources at the National Counterintelligence and Security Center (NCSC) at <http://www.ncsc.gov>. The following are also 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 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, www.ftc.gov.
- Review resources provided on the FTC identity theft website, www.Identitytheft.gov. 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, <http://www.us-cert.gov/ncas/tips/ST04-013>).
- 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 (<http://www.antiphishing.org>).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, <http://www.us-cert.gov/ncas/tips/ST04-004>; Understanding Anti-Virus Software, <http://www.us-cert.gov/ncas/tips/ST04-005>; and Reducing Spam, <http://www.us-cert.gov/ncas/tips/ST04-007>).
- 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 at www.ic3.gov.
- Additional information about preventative steps by consulting the Federal Trade Commission's website, www.consumer.gov/idtheft. 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
<https://www.identitytheft.gov/>
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502