NIH FAQ on the OPM Data Breach

June 5, 2015

What happened?
The U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have exposed the personal information of current and former Federal employees.

Since the breach was discovered this April, OPM has partnered with the US Department of Homeland Security Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation. OPM has implemented additional security measures.

Who has been affected?
Roughly 4 million federal employees and federal retirees are believed to be affected across at least 99 federal agencies. Roughly half of those affected are retirees and the other half current federal employees, possibly including those from the NIH. Given that possible the number affected of people may increase and that there are approximately 2.7 million current federal employees, the majority of employees will be affected by this breach, therefore it is important for all employees to be mindful of this. Contractors, fellows, and other non-FTEs are not believed to be affected by this breach.

Do we know what kind of information was compromised?
Personally identifiable information was compromised, which may include: birthdates, social security numbers, and other federal employment records.

What are the potential dangers that employees face?
The information involved in the breach may be used to commit identity theft, financial fraud, or “spear phishing” attacks.

Spear phishing is an email that appears to be from a trusted individual or business that you know in a fraudulent attempt to gain unauthorized access to confidential data. The email may ask you to reply with your account details in order to "update security" or for some other reason. Please do not respond to the emails that request passwords or personal financial information. Trusted websites routinely advise that they do not send e-mails requesting this type of information and they recommend caution if you receive such requests.

What do I do if I receive a suspicious email?
If you believe you have received a suspicious email, contact the NIH IT Service Desk or the NIH Incident Response Team.

- NIH IT Service Desk: 301-496-HELP (4357) or http://ITServiceDesk.nih.gov
- NIH Incident Response Team: 301-881-9726 or irt@nih.gov

How will I know if my personal information was compromised?
OPM will be sending notifications via email to those affected beginning June 8 and continuing through June 19.

The email will come from opmcio@csid.com and it will contain information regarding credit monitoring and identity theft protection services. Credit monitoring and identity theft insurance will be provided free of charge for 18 months to those affected.

In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

If NIH receives a listing of our affected employees, we will contact them as soon as possible.

What else can employees do?

Check your credit report. You can request a free credit report at www.AnnualCreditReport.com or call 1-877-322-8228. Look for accounts or charges you don't recognize. Even if the breach didn't involve credit card information, thieves may use your Social Security number, address, and date of birth to open accounts in your name.

You can place a fraud alert on your credit reports to receive notifications of any attempted activity on your credit such as the attempt to open new accounts in your name. To set up a fraud alert, Contact one of the three credit bureaus (that company must tell the other two). The Credit Bureaus are:

- Equifax: www.equifax.com/CreditReportAssistance or 1-888-766-0008
- Experian: www.experian.com/fraudalert or 1-888-397-3742
- TransUnion: www.transUnion.com/fraud or 1-800-680-7289

Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, other NIH employees, 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.

Monitor your financial statements for any suspicious activity.

Consider changing your passwords and security questions.

Where can I find more information?

- OPM: www.opm.gov
  - See the "Information About the Recent Cybersecurity Incident" announcement for more ways to avoid being a victim: http://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.
- Federal Trade Commission's official Identity Theft website: www.identitytheft.gov
  - OPM data breach – what should you do?: http://www.consumer.ftc.gov/blog/opm-data-breach-what-should-you-do
- CSID: www.csid.com/opm