Ames Research Center

IT Security news

National Aeronautics and Space Administration

Knowledge is power.
Protect yourself.

July—September 2015 Special Excerpt

"Those who are willing to sacrifice security for convenience will get neither."

The OPM Breach
By Patrick Bryant, IT Security Specialist

What Happened?
As of July 1, 2015, there were at least two separate intrusions into the OPM's computer systems. One affected Civil Service personnel records, and the other scooped up information submitted in federal background check applications: the behemoth 127 page questionnaire known as Standard Form 86 (SF-86). You can review the questions asked on the SF-86 by viewing the blank form here: https://www.opm.gov/forms/pdf_fill/sf86.pdf.

The information stolen could go back - according to some reports - as far as 1985. As of the date of this writing, notifications of the breach have been sent to civil servants whose personnel files were compromised, with additional details of the depth of the breach coming out almost daily. Notifications have not yet been sent to the much broader number of persons whose SF-86 data was compromised. The stolen information has been in the hands of the hackers for as long as a year.

The best technical description I can find on the details of the breach is titled: "EPIC fail—how OPM hackers tapped the mother lode of espionage data," http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/. The cyber attack's severity is still being assessed but there's agreement it was one of the worst security breaches in U.S. history.

What makes this incident so serious is the *irreparability* of the harm it has caused. Most information security breaches have a path to recovery. Identify the cause, correct the weakness, restore the data…and you're done. But there is no recovery from a breach of personally identifying information. You can't change your date of birth, your mother's maiden name, your birth place… and though you can conceivably change your social security number, the process is so arduous that only 250 SSNs were changed last year. The information that was lost represents literally everything about you.

OPM's own Inspector General reports make it clear that OPM failed to perform baseline security practices. It's easy to get mired in the technical details of what went wrong, but at the root of the failure is OPM's non-compliance with the most basic business practices, many involving low-tech activities like keeping an accurate inventory of its systems. A November 2014 report from the OPM's Inspector General warned that "OPM does not maintain a comprehensive inventory of servers, databases and network devices," and thus did not know what was connecting to each of those systems. One of the axioms of cyber security is: "You can't secure what you don't know you have." The OPM breach was a complete and catastrophic failure of cyber security at its most fundamental levels.

Who was affected?
We may never know exactly, but the current count is over 21-million people. OPM didn't retain logs going back far enough to see the full extent of the breach activity. It is prudent to assume civil servants have had their personnel records stolen, and if you ever filled out a background check form on the e-QIP system (which is presently shut down), at least all of the information you provided on that form has been compromised. The *results* of the background investigation (the "clearance adjudication information") – interviews with former employers, therapists, doctors, co-workers, neighbors, friends, spouses, etc., and any derogatory information about your habits and behaviors may also have been stolen. Any foreign contacts you reported – some of whom may live in countries that will take a dim view of that contact – may also have been disclosed. Foreign contacts and family living abroad who

were disclosed on the SF-86 could be subjected to reprisals or exploited for coercion by foreign governments. Some information on the SF-86 - even though it was disclosed to OPM - could nevertheless be embarrassing to some people and therefore blackmail fodder.

Were contractors affected?

As of the time of this writing, there is no direct and definitive answer to that question. However, the OPM Director told Congress: "there is a high degree of confidence that systems related to background investigations of current, former, and prospective federal government employees, and those for whom a federal background investigation was conducted may have been exfiltrated." If you are a contractor who completed an e-QIP questionnaire (form SF-86), it is prudent to assume your information was compromised.

Even if the OPM Breach information was stolen by non-state-sponsored hackers, foreign governments will have a keen interest in obtaining it, because it can replace an enormous amount of espionage effort. Consequently, regardless of the motive, your information is probably exposed to both the threats of identity theft and espionage.

Motives:

The most commonly believed motive for the OPM breach is espionage – and not identify theft. The most likely scenario for exploiting your information is to use it in targeted phishing attacks ("spear phishing"), to masquerade as authorized remote users to gain direct access to federal information systems, and to create a kind of LinkedIn database of U.S. personnel for their intelligence operations. Unfortunately, even if that's true, the only assurance you have that your personal information will not fall into the hands of identity thieves is based on the presumption that whoever stole your information will do a better job than OPM at protecting it. Since this theft is the Mother Lode of information needed to compromise the finances of millions of Americans, the motivation to exploit the information for financial gain is just too great to support any faith that it will *not* be exploited for unauthorized access to your financial accounts and theft of your identity.

Espionage-as-the-motive is only a hypothesis, and is based on the observed sophistication and methods used by the perpetrators. Even so, there is nothing preventing them from dumping your information on the black-market as a diversionary tactic. Contrary to the espionage-only hypothesis, Sen. Mark Warner, D-Va., on Monday, June 22nd wrote to Internal Revenue Commissioner John Koskinen that there have already been reports "that the credentials and identities of government breach victims are appearing for sale online to potential identity thieves."

Scope and duration of the damage:

The duration of the damage is permanent. With the confidentiality of your personal information irretrievably lost, any system or person that uses information, hints, or questionnaires about your past may be exploited by persons masquerading as you. Details such as these – which are contained in your SF-86 – may no longer be relied upon by anyone to authenticate you, including:

- Social security number
- Your passport number
- Date of birth
- Location of birth
- Mother's maiden name
- Current and former addresses and cohabitants
- Schools attended
- Current and/or former spouse's names
- Children's and Sibling's names
- Names of past friends and acquaintances
- Foreign countries visited
- Military experience…and the list goes on.

Fortunately, the SF-86 doesn't ask for your pets' names, so that's probably still safe. Everything else should be presumed as being permanently compromised. You can no longer reliably identify yourself to anyone using only your knowledge of your past.

Since there are probably many Internet sites containing your personal financial records that use questionnaires to either authenticate you or to allow you to change your password, any information contained in these sites is vulnerable to someone masquerading as you, and is no longer safe (not that it ever was completely safe).

It's important to avoid a logical fallacy called: "normalization of deviance." If you find yourself thinking: "My information was never completely safe, so this is just another incremental loss of privacy," the OPM breach is far worse than taking a slide a little farther down the slope of lost privacy. This hack is like falling off a cliff: it represents a loss that is many orders of magnitude worse than the piecemeal items you may have lost in the past. It is a complete dossier of everything an identity thief needs to compromise your finances – for the rest of your life.

Damage Control:

The procedures recommended by OPM are appropriate for an incident involving a lost credit card number. They are woefully inadequate for this incident. You can change a credit card number - but you cannot change your personally identifying information. The burden of inconvenience unfortunately falls on you to protect your identity.

It is a commonly held fallacy that information security is a compromise between *security* and *accessibility*. In fact, done properly, information security should place no access hurdles in front of the authorized user beyond authentication. Information security is in fact a compromise between *security* and *convenience*. One of the axioms of cyber security is: "Those who are willing to sacrifice security for convenience will get neither." It was convenient to place the SF-86 form on line rather than use a printed form. It was convenient to store that information on computers that were accessible via the Internet. We are now faced with a catastrophic security breach necessitating a significant amount of personal inconvenience. You now have neither security nor convenience.

While the damage may be done, there are steps you can take to limit the extent of the personal harm this damage can do. How much inconvenience you chose to endure depends on your own personal appetite for risk. Listed below are minimal

It's important to avoid a logical fallacy called:
Normalization of Deviance
If you find yourself thinking, "*My information was never completely safe, so this is just another incremental loss of privacy*." Stop! The OPM breach is far worse than taking a slide a little farther down the slope of lost privacy. This hack is like falling off a cliff. It represents a loss many orders of magnitude worse than the piecemeal items you may have lost in the past. It is a complete dossier of everything an identity thief needs to compromise your finances – for the rest of your life.

and maximal steps you can take. Because of the nature of the OPM breach, these steps will be a lifelong endeavor. If you are married, you should also undertake all of the same steps for your spouse, because much of their personal information was also included in the SF-86.

Minimal Damage Control:

1. First and foremost: be aware that information about you that you once thought was private – no longer is. Think like a spy or an identity thief. What are your greatest vulnerabilities and assets (police reports/convictions, 401k/TSP retirement accounts, etc.)? This will vary significantly from person to person. Do what you can to minimize those vulnerabilities and apply additional protections to your greatest assets.
2. Keep up on daily news and developments regarding the breach. The breach is complex and technical, and (speaking as a former news writer myself) it will probably not receive top billing in news outlets. You will have to search it out. Typing "OPM breach" into news.google.com should yield most of the current information.
3. File a police report referencing the OPM breach. Some police agencies (such as San Jose P.D.) will allow you to do this on line. Keep a copy of the police report to reference in other actions you take to lock down your information.
4. File a "fraud alert" with the credit reporting agencies. The process for filing a fraud alert is somewhat streamlined: you only have to file it with one credit reporting agency – Transunion. Transunion will then inform the other agencies. Be sure to file a police report first so you are eligible for an extended fraud alert, which lasts for seven years. Otherwise, the fraud alert will disappear after 90 days. Note that the email and letters sent by OPM to victims fail to mention the temporary nature of ordinary (non-extended) fraud alerts. Transunion can be contacted by phone at 1-800-680-7289 or on line here: http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page. You will get more complete protection from a credit report security freeze (also unmentioned in the OPM letters) described in Maximal Damage Control below.
5. Participate in credit monitoring. If you are a contractor, OPM hasn't yet offered you free credit monitoring. However, there have been so many breaches (Target, Home Depot, Anthem, etc.) that it is likely you are already eligible for free credit monitoring. Credit monitoring provides very limited protection, but it may give you a warning that someone is exploiting your private information. OPM thus far is only offering 18 months of free credit monitoring (and only to those who have so far been notified). The risk to your credit however is permanent. Shop around for credit monitoring to use after those 18 months have passed. You'll need it for life. You may want to call or write your Congressional representative about the inadequacy of the 18-month time limit.
6. Routinely order a copy of your credit reports from all of the credit reporting agencies. Review them carefully with special scrutiny given to any new accounts you don't recognize and inquires for your credit report from unrecognized entities. Repeat this process frequently. You can get a free report once each year from all three primary reporting bureaus from annualcreditreport.com, telephone 1-877-322-8228. You will be asked questions to authenticate yourself that, ironically, can also be answered by whoever breached OPM.
7. Exercise extreme caution when receiving anything by email pertaining to the OPM breach. Since as many as 20-million Americans (maybe more) were impacted by the breach, identity thieves will leverage the publicity and will certainly be exploiting this incident to obtain information from victims to facilitate identity theft and fraud. These emails will probably take the form of bogus notifications, identity theft protection, and credit monitoring services. If you want these services, go directly to the service provider – don't respond to links in email solicitations. Also be extremely cautious of any telephone calls pertaining to the breach. OPM is not calling people on the phone.
8. File your tax returns early so your return has a chance of arriving at the IRS before bogus returns are filed in your name by identity thieves. If you make a mistake and find you are entitled to a bigger refund, you can re-file up to April 15th without having to do an amended return. Cases of tax-related identity theft numbered 2.9 million in 2013, according to the Treasury Inspector General for Tax Administration. Stay informed about any new tax return authentication processes offered by the IRS.
9. Come up with new answers to common password reset questions, and change those answers wherever you can. The answers don't have to be genuine – they only have to be memorable. Write them down and save them somewhere safe. Computers won't care if you change your mother's maiden name to "Kangaroo."
10. Review information about additional preventative steps by consulting the Federal Trade Commission's website: www.identitytheft.gov.
11. Report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center: www.ic3.gov.

Maximal Damage Control:

In addition to all of the steps above:

1. Obtain a copy of all of the information OPM maintains about you. You are entitled to this information under the Privacy Act of 1974. Use this information to assess how much damage may have been caused by the breach. You

already know what you provided on the SF-86, but you do not know what investigatory information (comments from people interviewed) was entered into your file. This is known as the "adjudication information." You are also entitled under the Freedom of Information Act (FOIA) to any information that can be publicly released about the breach. I recommend requesting that information as well in your Privacy Act request. Instructions for filing a Privacy Act request are posted at https://www.opm.gov/forms/pdf_fill/inv100.pdf. I suggest selecting "*All Investigations and Standard Forms*" under the Records Requested section (section 3).

2. Place a "security freeze" on release of your credit reports. This will prevent anyone (including OPM) from accessing your credit reports. You will be given a different PIN from each of the agencies to temporarily or permanently unfreeze your credit reports. Save those PINs in a safe place. Unfreeze your reports only when you apply for new credit, try to determine which agency the creditor will query for the report and only unfreeze that agency's report, and unfreeze your report for as short a period as possible. You are creating a window of vulnerability while your report is unfrozen. Remember to re-freeze the report when your credit application is completed. There are commercial services such as *Lifelock* that can perform this for you, for a fee, or you can contact each of the four credit agencies (Equifax, Experian, Innovis, and Trans Union) directly. ***Links to the four credit agencies, and details about security freezes (how they work) are listed at the end of this article.** If you filed a police report, you can freeze your credit report for free. Otherwise, the credit reporting agencies will charge you $10 each ($40 total) for California residents.
3. Advise your bank that your identity has been compromised and that changes to your account should only be accepted when you personally appear at a branch to make those changes. Tell them not to send new blank-check orders to your home address, but instead arrange to pick up the check order at a branch (see item 8 below for an explanation). Restrict use of your bank debit card to use only at trusted ATMs. Don't use your debit card as you would use a credit card – the personal consequences of having your checking account emptied are just too dire.
4. Place a Consumer Reported Identity Theft Security alert in your ChexSystems consumer file to make it harder for identity thieves to open checking accounts in your name. Details are located here: https://www.consumerdebit.com/consumerinfo/us/en/chexsystems/theftaffidavit/index.htm. The alert will expire after 90 days unless you provide a notarized affidavit, which will extend the alert to seven years. Be aware that not all banks and credit unions use ChexSystems.
5. Keep enough cash saved away in a safe place to meet your immediate needs for at least a week or two in case your bank account is corrupted or frozen. (You should do this anyway in case you lose access to cash after a disaster.)
6. Notify all of your professional colleagues and everyone identified in your SF-86 that your identity has been compromised, that their information on your SF-86 has also been compromised, and that there is a risk that someone may masquerade as you in email and other on line correspondence. Advise them to be suspicious of any correspondence from you and to contact you by phone if anything unusual is received.
7. Try to use only on line services that provide two-factor (or at least two-step) authentication.
8. Be cautious that someone may forward your personal mail to another address. If your mail suddenly stops arriving, contact your local post office to determine whether a bogus forwarding order has been filed. Since it would be *inconvenient* to require people to come to a post office to verify their identity when mail forwarding services are ordered, the only identity verification used by the post office is a $1.05 charge to a (potentially stolen) credit card number. As a countermeasure, consider having all of your mail delivered to a commercial mail receiving agency (CMRA), such as a UPS Store, etc., and then notify all your correspondents to send mail only to the CMRA address. Postal regulations prohibit the post office from forwarding mail addressed to you at a CMRA address on to another forwarding address (it will however forward mail from your home to a CMRA), so someone masquerading as you cannot intercept your mail by having it forwarded from a CMRA address.
9. Review your social media postings and remove information that can give spies and identity thieves detailed information about your activities, travels, tastes, and behaviors.

First and foremost: be aware the information about you, that you once thought was private – no longer is. Think like a spy or an identity thief. What are your greatest vulnerabilities and assets?

Finally, don't let down your guard. As time passes, and nothing happens, it will be tempting to assume you are in the clear. The most likely adversary to have gotten your information has a habit of being very patient and waiting for things to cool down before launching attacks. And there is no guarantee that the "hacker won't be hacked" at a later date, exposing your information to a whole new spectrum of threats.

Try to stay positive and avoid ruminating too much on this topic. If you allow it to adversely affect your health and your state of mind, then you will truly become a causality in this cyber war. Take solace in the knowledge that you have done all you can to protect yourself and your family, and that there are so many people affected (including members of Congress) that this incident may spur the beginning of replacing the outdated practices and credentials that have no place in the 21st Century.

*** <u>Credit Reporting Agencies:</u>**

- **Equifax:** https://help.equifax.com/app/answers/detail/a_id/75/search/1
- **Experian**: https://www.experian.com/freeze/center.html
- **Innovis:** https://www.innovis.com/personal/securityFreeze
- **TransUnion**: http://www.transunion.com/securityfreeze
- **Security Freezes**: https://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/