OCHR FACTSHEET

OPM Employee Data Breach

Issued: June 2015

SPECIAL ISSUE

This Fact Sheet:

- Alerts employees about a data breach at OPM
- Provides information about next steps
- Shares information on precautionary measures

NOTE: If employees receive suspected phishing emails, contact Command security officials to report.

Email notification comes from OPMcio@csid.com.

DEPARTMENT OF THE NAVY
CIVILIAN CAREERS

Where Purpose and Patriotism Unite

Background

On June 4, 2015, the U.S. Office of Personnel Management (OPM) announced a cybersecurity breach potentially impacting personnel data, to include personally identifiable information (PII), on current and former federal employees. About 4 million individuals may be impacted.

What Happens Next

OPM will begin notifying affected current and former federal employees on Monday, June 8.The notification will continue through June 19, 2015 (or until complete). Notifications will be sent by U.S. Postal Service via a letter or from the email sender opmcio@csid.com.

OPM will provide affected employees with credit monitoring services and identity theft insurance through the company, CSID, to include credit report access, credit monitoring and identity theft insurance and recovery services. This coverage will be offered at no cost to affected employees for 18 months. Beginning Monday, June 8, OPM will refer all questions from current and former federal employees to CSID at www.csid.com/opm (1-844-222-2743; international callers can call collect at 512-327-0700) – the high volume of calls may result in extended wait times.

The Department of the Navy Civilian Employee Assistance Program (DONCEAP) also provides support for financial issues and identity theft for all DON civilians and their families. The 24/7 number is **1-844-DONCEAP** (1-844-366-2327) TTY 1-888-262-7848, International 001-866-829-0270. Information is also available at http://DONCEAP.foh.hhs.gov.

Precautions and Advisory

OPM recommends that affected employees:

- Monitor financial account statement – report any suspicious or unusual activity to financial institutions
- Request a free credit report at www.AnnualCreditReport.com or call 1-877-322-8228. (Law entitles consumers to one free credit report per year from each of the three major credit bureaus (Equifax, Experian and TransUnion). Contact information for the credit bureaus is found at the Federal Trade Commission (FTC) website www.ftc.gov
- FTC provides identify theft resources at www.identitytheft.gov
- Consider placing a fraud alert on credit files to advise creditors to initiate contact before opening a new account in your name – Call TransUnion (1-800-680-7289) to set up an alert

More information on page 2

OCHR FACTSHEET

Avoid Being a Victim (provided by OPM)

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or 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 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 email clients 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.

Potentially affected individuals can obtain additional information about the steps they can take to avoid identity theft from the following agencies. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

For California Residents:
Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft

For Kentucky Residents:
Office of the Attorney General of Kentucky
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
Telephone: 1-502-696-5300

For Maryland Residents:
Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Telephone: 1-888-743-0023

For North Carolina Residents:
Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
www.ncdoj.com/
Telephone: 1-919-716-6400

For all other US Residents:
Identity Theft Clearinghouse, Federal Trade Commission
600 Pennsylvania Avenue, NW, Washington, DC 20580
www.consumer.gov/idtheft 1-877-IDTHEFT (438-4338), TDD: 1-202-326-2502

Still Need Assistance?

For additional questions, email the DON HR FAQ box at DONhrFAQ@navy.mil.

DEPARTMENT OF THE NAVY — OFFICE of CIVILIAN HUMAN RESOURCES

OCHR FACTSHEET