FOR IMMEDIATE RELEASE
EMBARGOED UNTIL 5:00 PM ET ON
JUNE 4, 2015

Contact: Sam Schumach
(202) 606-2402 or
samuel.schumach@opm.gov

OPM to Notify Employees of Cybersecurity Incident

WASHINGTON, DC – The U.S. Office of Personnel Management (OPM) has identified a cybersecurity incident potentially affecting personnel data for current and former federal employees, including personally identifiable information (PII).

Within the last year, the OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. As a result, in April 2015, OPM detected a cyber-intrusion affecting its information technology (IT) systems and data. The intrusion predated the adoption of the tougher security controls.

OPM has partnered with the U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation (FBI) to determine the full impact to Federal personnel. OPM continues to improve security for the sensitive information it manages and evaluates its IT security protocols on a continuous basis to protect sensitive data to the greatest extent possible. Since the intrusion, OPM has instituted additional network security precautions, including: restricting remote access for network administrators and restricting network administration functions remotely; a review of all connections to ensure that only legitimate business connections have access to the internet; and deploying anti-malware software across the environment to protect and prevent the deployment or execution of tools that could compromise the network.

As a result of the incident, OPM will send notifications to approximately 4 million individuals whose PII may have been compromised. Since the investigation is on-going, additional PII exposures may come to light; in that case, OPM will conduct additional notifications as necessary. In order to mitigate the risk of fraud and identity theft, OPM is offering credit report access, credit monitoring and identify theft insurance and recovery services to potentially affected individuals through CSID®, a company that specializes in these services. This comprehensive, 18-month membership includes credit monitoring and $1 million in identity theft protection services at no cost to enrollees.

"Protecting our Federal employee data from malicious cyber incidents is of the highest priority at OPM," said **OPM Director Katherine Archuleta**. "We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our

experienced team is constantly identifying opportunities to further protect the data with which we are entrusted."

OPM has issued the following guidance to affected individuals:

- 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.

How to avoid being a victim:

- 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 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.

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

- end -