FOR IMMEDIATE RELEASE
Tuesday, September 1, 2015

Contact: Office of Communications
(202) 606-2402 or media@opm.gov

OPM, DoD Announce Identity Theft Protection and Credit Monitoring Contract

Victims of Cybercrime to Receive Three Years of Services

WASHINGTON, D.C. – The U.S. Office of Personnel Management (OPM) and the U.S. Department of Defense (DoD) today announced the award of a $133,263,550 contract to Identity Theft Guard Solutions LLC, doing business as ID Experts, for identity theft protection services for 21.5 million individuals whose personal information was stolen in one of the largest cybercrimes ever carried out against the United States Government. These services will be provided at no cost to the victims whose sensitive information, including Social Security numbers, were compromised in the cyber incident involving background investigations.

"We remain fully committed to assisting the victims of these serious cybercrimes and to taking every step possible to prevent the theft of sensitive data in the future," **said Beth Cobert, Acting Director of the Office of Personnel Management**. "Millions of individuals, through no fault of their own, had their personal information stolen and we're committed to standing by them, supporting them, and protecting them against further victimization. And as someone whose own information was stolen, I completely understand the concern and frustration people are feeling."

ID Experts will provide all impacted individuals and their dependent minor children (under the age of 18 as of July 1, 2015) with credit monitoring, identity monitoring, identity theft insurance, and identity restoration services for a period of three years. This task order was awarded under GSA's Blanket Purchase Agreements (BPA) for Identity Monitoring, Data Breach Response and Protection Services which GSA awarded today.

The U.S. Government, through the Department of Defense, will notify those impacted beginning later this month and continue over the next several weeks. Notifications will be sent directly to impacted individuals.

For more information, or to sign up for email alerts, please visit https://www.opm.gov/cybersecurity.

OPM has previously 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.ftc.gov/idtheft. 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.

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 -