ALAUX 11-15 - OFFICE OF PERSONNEL MANAGEMENT (OPM) CYBERSECURITY INCIDENT

06 JUN 2015

1. The following message was delivered to Coast Guard personnel late last night through the Department of Homeland Security Management Communications network. Although yet to be confirmed, it is reasonable to presume that Coast Guard Auxiliarists may be included in the population of affected individuals. The message indicates that notifications will be sent by email and U.S. mail to affected individuals during the June 8-19, 2015 time period. Auxiliarists are strongly encouraged to closely monitor their email and mail during this upcoming two week time period for possible notification. Any additional details regarding the source and content of these notifications will be forwarded to you as soon as they become available.

"Cybersecurity Incident

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, including employees of the Department of Homeland Security.

Since the incident was identified, OPM has partnered with the Department's U.S. Computer Emergency Readiness Team and the Federal Bureau of Investigation to determine the impact to Federal personnel. As a result of this investigation, OPM is notifying approximately 4 million individuals whose Personally Identifiable Information may have been compromised. The notifications will be sent beginning June 8 and continuing through June 19 by email and U.S. mail.

In order to mitigate the risk of fraud and identity theft, OPM will offer affected individuals credit monitoring services and identity theft insurance through CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance and recovery services and is available immediately at no cost to affected individuals identified by OPM. Employees whose information was affected will receive a notification directly from CSID. If you have any questions about the impact of this incident to your data or if you receive a notice and have questions about the services being offered, contact CSID directly beginning at 8 a.m. CST on June 8, 2015. The company's website is www.csid.com/opm, and its toll free is 844-222-2743 (International callers: Call collect 512-327-0700).

Following this incident, OPM took immediate action to implement additional security measures in order to protect the sensitive personnel data it manages. Please remain vigilant in helping to protect our systems and data.

Below is information about identify fraud which you may find useful.

Steps for Monitoring Your Identity and Financial Information

* Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.

* Request a free credit report at www.AnnualCreditReport.com <http://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(r), Experian(r), and TransUnion(r) - 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(r) at 1-800-680-7289 to place this alert. TransUnion(r) will then notify the other two credit bureaus on your behalf.

Precautions to Help You Avoid Becoming a Victim

* Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues 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.

* 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, 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.

* Additional information about preventative steps by consulting the Federal Trade Commission's website, www.consumer.gov/idtheft. The FTC also encourages those who discover that their information has been misused to file a complaint with the commission using the contact information below.

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"