TO: ALAUX
From: CHDIRAUX
SUBJ: OFFICE OF PERSONNEL MANAGEMENT (OPM) CYBERSECURITY INCIDENT - UPDATE -013/15

1. The following message was recently received from the Department of Homeland Security Management Communications network. It provides an update to information first provided in ALAUX 011/15 issued on June 5, 2015. Notifications to affected individuals began June 8 and will continue thru June 19. Auxiliarists are strongly encouraged to thoroughly review this following message:

"As was communicated on June 4, 2015, 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 Personally Identifiable Information (PII) of some current and former federal employees. This email provides additional information regarding next steps for DHS employees.

Beginning June 8 and continuing through June 19, OPM will be sending notifications to individuals whose PII was potentially compromised in this incident. OPM has retained a private vendor, CSID, to transmit the notifications on behalf of OPM. Consequently, the email will come from opmcio@csid.com and will not come from a .gov email address. The notification will feature a CSID logo and will contain information regarding credit monitoring and identity theft protection services being provided to those federal employees impacted by the data breach. In the event OPM does not have an email address for the individual on file, a standard letter will be sent via the U.S. Postal Service.

This notification is different from other notifications you may have already received. The Department is also in the process of notifying some DHS employees in CBP, ICE, TSA, and in a small number of other components that one of the companies that DHS contracts with to conduct background investigations and credit checks may have had a compromise of its network. That notification, which was made via U.S. Postal Service, is separate from this OPM notification.

As a note of caution, confirm that the email you receive is, in fact, the official notification. It’s possible that malicious groups may leverage this event to launch phishing attacks. To protect yourself, we encourage you to do the following:

1. Make sure the sender email address is “opmcio@csid.com.”

2. The email should not contain any attachments. If it does, do not open them, and forward the email to dhsspam@hq.dhs.gov.

3. The email is sent exclusively to your email address. No other individuals should be in the TO, CC, or BCC fields.

4. The email subject should be exactly “Important Message from the U.S. Office of Personnel Management CIO.”

5. The email will feature an embedded “Enroll Now” button. Do not click on the included link. Instead, record the provided PIN code, open a web browser then manually type the URL - http://www.csid.com/opm - into the address bar and press enter. You can then use the provided instructions to enroll using the OPM/CSID website.

6. The email should not contain any attachments. However, once you visit the OPM/CSID website (http://www.csid.com/opm) to enter your PIN code, you will be asked to provide personal information to verify your identity.

7. The official email should look like this sample screenshot <http://dhsconnect.dhs.gov/org/comp/mgmt/SiteAssets/Pages/OPM-Cybersecurity-Incident-Update-/OPM_Breach_email1.png> .

8. If you would prefer not to enter your personal information on the OPM/CSID website (http://www.csid.com/opm), you may call the CSID call center toll-free at 844-777-2743 or 844-222-2743. (International callers: call collect 512-327-0705).

9. OPM will not proactively call you about the breach. If you receive a phone call about the breach claiming to be OPM, then it iot provide any personal information. CSID, not OPM, is making all notifications about this breach, and the notifications are by email or through the U.S. Postal Service.

Additional information is also available on CSID’s website, http://www.csid.com/opm (external link), or you can call them toll-free at 1-844-777-2743 (International callers: call collect at 1-512-327-0705).

Regardless of whether or not you receive this notification, you should take extra care to ensure that they are following recommended cyber and personal security procedures. If you suspect that you have received a phishing attack, contact your component’s security office <http://dhsconnect.dhs.gov/org/comp/mgmt/cso/Pages/DHS_Security_Offices.aspx> .

In general, government employees are often frequent targets of “phishing” attacks, which are surreptitious approaches to stealing your identity, accessing official computer systems, running up bills in your name, or even committing crimes using your identity. Phishing schemes use email or websites to trick you into disclosing personal and sensitive information.

We will continue to keep you advised of new developments regarding this cybersecurity incident as we learn more from OPM. The following includes helpful information for monitoring your identity and financial information and precautions to help you avoid being a victim.

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 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. You can find contact information for the credit bureaus on the Federal Trade Commission (FTC) website, www.ftc.gov.

* Review resources provided on the FTC identity theft webitytheft.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.

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).

· You should take steps to monitor your personable 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, D.C. 20580

https://www.identitytheft.gov/
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502"

2. The purpose of this list is to keep Auxiliarists as well as all other interested parties abreast of current developments, policies, manuals, etc. All information contained herein and linked is OFFICIAL policy and Information.

3. Internet Release and Distribution is Authorized.

4. CG-BSX sends.