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

26 JUN 2015

1. Auxiliarists are strongly encouraged to thoroughly review the following message. It was received on June 23, 2015 from the Department of Homeland Security Management Communications network, and it provides updates to information provided in ALAUX 011/15 issued on June 5, 2015 and ALAUX 013/15 issued on June 13, 2015. It indicates that notifications to affected individuals began June 8 and may take several days beyond June 19 to arrive by email or mail.

"This is an update on the recent cyber incidents at the U.S. Office of Personnel Management (OPM).

As the Department has recently shared, on June 4, OPM announced an intrusion impacting personnel information of approximately four million current and former Federal employees. OPM is offering affected individuals credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. Additional information is available on the company's website, https://www.csid.com/opm/ and by calling toll-free 844-777-2743 (international callers: call collect 512-327-0705). More information can also be found on OPM's website: www.opm.gov.

Notifications to individuals affected by this incident began on June 8 on a rolling basis through June 19. However, it may take several days beyond June 19 for a notification to arrive by email or mail. If you have any questions about whether you were among those affected by the incident announced on June 4, you may call the toll free number above.

On June 12, OPM announced a separate cyber intrusion affecting systems that contain information related to background investigations of current, former, and prospective Federal Government employees from across all branches of government, as well as other individuals for whom a Federal background investigation was conducted, including contractors. This incident remains under investigation by OPM, DHS, and the FBI. The investigators are working to determine the exact number and list of potentially affected individuals. We understand that many of you are concerned about this intrusion. As this is an ongoing investigation, please know that OPM is working to notify potentially affected individuals as soon as possible.

As an important reminder, OPM discovered this incident as a result of the agency's concerted and aggressive efforts to strengthen its cybersecurity capabilities and protect the security and integrity of the information entrusted to the agency. In addition, OPM continues to work with the Office of Management and Budget (OMB), DHS, the FBI, and other elements of the Federal Government to enhance the security of its systems and to detect and thwart evolving and persistent cyber threats. As a result of the work by the interagency incident response team, we have confidence in the integrity of the OPM systems and continue to use them in the performance of OPM's mission. OPM continues to process background investigations and carry out other functions on its networks.

Additionally, OMB has instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the resilience of Federal networks. We are working with OMB to ensure we are enforcing the latest standards and tools to protect the security and interests of the DHS workforce.

The Department will continue to update you as more information about the cyber incidents at OPM comes to light. For all updates, including previous messages and important resources, please visit the OPM Cybersecurity Incident Updates <http://dhsconnect.dhs.gov/org/comp/mgmt/Pages/OPM-Cybersecurity-Incident-Updates.aspx> page on Connect.

OPM is the definitive source for information on the recent cyber incidents. Please visit OPM's website for regular updates on both incidents and for answers to frequently asked questions: www.opm.gov/cybersecurity <http://www.opm.gov/news/latest-news/announcements/> . DHS is also interested in your feedback and questions on the incident and our communications. You can reach out to us at privacyhelp@dhs.gov with these comments.

Employees who want to learn additional information about the measures they can take to ensure the safety of their personal information can find resources at the National Counterintelligence and Security Center (NCSC) at http://www.ncsc.gov <http://www.ncsc.gov/about/docs/Dealing_with_a_Breach_of_your_PII.pdf> .

Please note that the OPM 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 experienced a compromise of its network. That notification, which was made via U.S. Postal Service, is separate from the OPM notification. It is possible that some employees are affected by both the DHS and OPM incidents."