



United States Department of Agriculture

Departmental
Management

Office of the Chief
Information Officer

1400 Independence
Avenue S.W.
Washington, DC
20250

TO: All USDA Employees

FROM: Joyce M. Hunter
Acting Chief Information Officer (CIO)
Office of the Chief Information Officer

Ravoyne Payton
Chief Privacy Officer
Office of the Chief Information Officer

SUBJECT: Information for Employees Regarding the OPM Breach

As you may have heard in the news, as well as my previous email dated June 5th, 2015, an Office of Personnel Management (OPM) system suffered a breach. USDA was informed by OPM that USDA current and former employee information was compromised. OPM established a call center, and began sending out email notification to those impacted on June 8, 2015. This week USDA employees began receiving the official notification email from OPM. The official email notification from OPM will come from opmcio@csid.com. If you received the OPM notification, we recommend that you immediately take the appropriate actions outlined in the notification to protect yourself. If you have not received the notification from OPM, we ask that you check your home mail, and email addresses, to include your spam or junk email folders. We encourage you to visit www.opm.gov for additional updates, and steps you can take to protect yourself. We encourage you to share this information with USDA employees.

In an effort to assist you, we are sharing the following information from OPM.

--OPM's Office of the Chief Information Officer recently became aware of a cybersecurity incident affecting its systems and data that may have compromised the personal information of approximately 4 million current and past federal employees.

--Within the last year, 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 became aware of a malicious activity potentially affecting our information technology (IT) systems and data that predated the adoption of the tougher security controls. After the malicious activity was discovered, OPM immediately implemented additional security measures and will continue to add protections for the sensitive information we manage.

--Also since the incident was identified, OPM has partnered with the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation to determine the impact to Federal personnel.

--As a result of this investigation, OPM concluded that personally identifiable information for current and former Federal employees across Executive Branch agencies **may have** been exposed in this incident. Beginning June 8 and continuing through June 19, 2015, OPM will be sending official notifications to affected individuals via email and the U.S. Postal Service. In addition, the investigation is ongoing. OPM will do additional notifications if necessary.

--If personal information is at risk, individuals will receive notification from OPM either in the form of a letter via the U.S. Postal Service, or, in an email from this email address: opmcio@csid.com.

--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.

--Beginning at 9 a.m. EDT on June 8, 2015, questions from current and former Federal employees were directed to CSID. The company's website is www.csid.com/opm and its toll free number is 844-222-2743 (International callers: Call collect 512-327-0700).

Joyce Hunter
Acting CIO

Ray Payton
Chief Privacy Officer