



NATIONAL
ARCHIVES

OFFICE of
INSPECTOR GENERAL

Date : September 25, 2013

Reply to

Attn of : Office of Inspector General (OIG)

Subject : Audit Memorandum No. 13-15: NARA's Handling of Paper-Based Disclosure of Personally Identifiable Information (PII)

To : David S. Ferriero, Archivist of the United States

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of NARA's Intrusion Detection and Prevention Systems (IDPSs) and Incident Response. The objective of the audit was to determine whether (1) NARA's IDPSs had been properly implemented and are operating effectively; (2) appropriate logical and physical security, and environmental protection controls are in place, and; (3) NARA's computer security incident response process is effective and efficient, including whether incident response staff are adequately trained. On September 10, 2013, the OIG issued *Audit of NARA's Intrusion Detection and Prevention Systems and Incident Response* (OIG Report No. 13-12). The report outlined weaknesses in NARA's ability to prevent, detect, and respond to security incidents effectively and efficiently. This audit memorandum addresses the issue related to NARA's handling of paper-based PII disclosure events identified during the course of the above audit. The Chief Operating Officer believed addressing this issue separately from electronic-based security incidents, included in the OIG Report No. 13-12, would allow the agency to focus on the issue and act upon it more effectively.

OMB Memorandum M-06-19 specifies United States Computer Emergency Readiness Team (US-CERT) reporting should include all PII incidents whether in electronic or physical form. Therefore, in order to determine whether appropriate actions were taken to resolve and report the incidents effectively and efficiently, we (1) judgmentally selected a sample of 80 security incidents that were reportable or potentially reportable to US-CERT, and were opened between October 2011 and October 2012, and (2) reviewed the sampled incident reports and email communications from/to US-CERT and NARA's Trusted Internet Connections (TIC) contractor.

NATIONAL ARCHIVES *and*
RECORDS ADMINISTRATION

8601 ADELPHI ROAD, ROOM 1300
COLLEGE PARK, MD 20740-6001

Improvement Needed in the Resolution Process

In our sample, 12 incident reports were related to paper-based disclosure of PII originated in the National Personnel Records Center (NPRC) in St. Louis and Valmeyer, MO. The NPRC responds to requests for copies of documents from military and civilian personnel records. Disclosures of PII occur when a document belonging to another person is sent to the requestor, or the document included PII of others without proper redaction.

According to the Training Specialist at NPRC, many recipients return the documents when they file a complaint regarding the incorrect documents, agree to return the documents to NPRC, dispose of the documents prior to filing a complaint, or agree to shred the documents in lieu of returning them to NPRC. However, we found NARA currently does not have a mechanism to match the returned documents to the complaints filed by the recipients. The lack of a mechanism to ensure receipt of documents agreed to be returned may result in inappropriate use of the information by unauthorized individuals.

Recommendations

In order to better protect PII and minimize the adverse impact it may cause in the event of a paper-based PII disclosure, we recommend NARA's Chief Operating Officer:

1. Assess the current process of providing a copy of military or civilian personnel records to the requestor and enhance the control to minimize instances of incorrect records being sent to the requestor.
2. Develop a process to ensure erroneously sent copies of the records containing PII are properly returned to NARA and matched to the complaints.

Management Response

Management concurred with the recommendations.

This audit was conducted in accordance with generally accepted government auditing standards between October 2012 and June 2013. These standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As with all OIG products, we will determine what information is publically posted on our website from this audit report. Should you or management have any redactions suggestions based on FOIA exemptions, please submit them to my counsel within one week from the date of this letter. Should we receive no response from you or management by this timeframe, we will interpret that as confirmation NARA does not desire any redactions to the posted report.

Should you have any questions concerning this report, or require additional information, please contact me at (301) 837-3000.

A handwritten signature in cursive script that reads "James Springs".

James Springs
Acting Inspector General