UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Breach of Personally Identifiable Information in Retirement Services
(Report No. 4A-RI-00-12-033)

The purpose of this memorandum is to communicate to you the conclusions resulting from our review of a release of personally identifiable information (PII) that occurred when a contractor for the Retirement Services (RS) program office mailed postcards related to the Federal Employees Health Benefits Program (FEHBP) open season enrollment to Federal government annuitants.

Executive Summary

Our review indicated that several missing or bypassed information technology (IT) security controls resulted in postcards containing exposed PII, including Social Security Numbers (SSN), to be printed and mailed through the U.S. Postal Service. In addition, several individuals across multiple U.S. Office of Personnel Management (OPM) organizations did not follow the appropriate procedures for reporting the breach to OPM's Situation Room.

As a result, we recommend that the Office of the Chief Information Officer (OCIO) strengthen its change management procedures and conduct agency-wide training and awareness campaigns related to incident response and reporting. We also recommend that RS implement a data reconciliation process with its contractor and consider providing free credit monitoring services to every individual whose SSN was printed and mailed.

Background

OPM contracts with Vangent, Inc. to manage the annual FEHBP open season enrollment process for Federal government annuitants. One of Vangent's responsibilities is to mail postcards alerting annuitants who have suspended their FEHBP enrollment of the upcoming open season and their eligibility to re-enroll in the program. In October 2011, Vangent unintentionally printed and mailed approximately 3,000 postcards that contained annuitant's SSNs on the cover.

Scope and Methodology

We conducted interviews with individuals from RS and OCIO and reviewed the information security incident report from OPM's situation room.

Our review was not conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). The nature and scope of the work performed was consistent with that expected of a GAGAS audit; however, because we consider this to be a review, the documentation, reporting, and quality control standards are not as stringent.

Review Results

Our review indicated that several missing or bypassed IT security controls allowed the data breach to occur and that several individuals across multiple OPM organizations did not follow the appropriate procedures for reporting the breach to OPM's situation room.

a) Failed security controls that allowed the breach to occur

In July 2011, the OCIO sent test data to Vangent to test the creation of the database used to populate the FEHBP open season postcards to be mailed to Federal annuitants. However, Vangent informed the OCIO that there was an error with the test file. In an attempt to fix the problem, an OCIO programmer edited the code that was used to create the test data file. This edit was treated as an "emergency change" and the typical change control process, that requires several levels of approval and testing, was not followed.

After the change was complete, the OCIO re-ran the data extract process and delivered a data file to Vangent that was to be used in the production database. Vangent detected that something was still wrong with this file, as many rows of data were rejected by Vangent's database validity checks. It was also determined that this file inappropriately contained SSNs. As a result, the OCIO implemented a second emergency change in an attempt to fix the file. The extract was run a second time and a second production file was sent to Vangent. It would be determined later that the second production file was still incorrect (it contained far too many rows), but it no longer contained SSNs.

Vangent proceeded to update its database with the second production file. However, it never "refreshed" the database to delete the first production file that contained SSNs. As a result, postcards containing clearly exposed SSNs were printed and mailed the week of October 24, 2011. Due to the other errors in the data file, the postcards were mailed to government agencies that have collection accounts for annuitants, and not to the individual's homes. Although the database contained too many rows of data, these errors were not detected because there is no reconciliation process to verify that the number of rows produced by RS matches the number processed by Vangent.

Although a reconciliation process could have alerted Vangent that there were still errors in the database, the original problem was caused by weak change management controls in the OCIO.

Since the code edits were treated as emergency changes, limited testing was done on the changes, and nobody other than the programmer approved the change. The programmer checked the code out of production, made edits, and then delivered it to the mainframe Production Control team to place back into production. Although there is certainly a need for an emergency change process in a programming environment, the process should still require at least one level of managerial approval so that the programmer cannot facilitate the entire process alone.

RS estimated that approximately 3,000 postcards containing SSNs were mailed. The majority of the postcards were recovered from the government agencies to which they were mailed, but approximately 650 postcards were not recovered. Free credit monitoring services were offered to those individuals whose information was exposed on the non-recovered postcards, but nothing was offered to those individuals whose information was printed on postcards that were recovered. The mailed postcards were bundled in stacks of about 150 and the only exposed SSN was the postcard on top. Although only one out of every 150 postcards was easily visible, and most of the postcards were recovered, it is impossible to determine how many people had physical access to the trays as they were routed through the print vendor's facility and the U.S. Postal Service.

Recommendation 1
We recommend that the OCIO improve its change management procedures so that emergency changes require management approval prior to being placed into production.

Recommendation 2
We recommend that RS develop a reconciliation process with Vangent to ensure that the data files passed between the organizations contain the appropriate quantity of data.

Recommendation 3
We recommend that RS reevaluate its decision to not provide credit monitoring services to individuals whose information was printed on postcards that were recovered.

b) Timely reporting of the security breach

On Saturday, October 29, 2011, an RS staff member received a telephone call from an official at the Eagan, Minnesota post office distribution center to report a large volume of postcards from OPM containing SSNs. The individual that received the call immediately notified a branch chief in the OCIO and a group chief in RS. By the evening of October 30, an OCIO group chief and the Associate Director of RS had also been notified. By the morning of Monday, October 31, OPM's Chief Information Officer was also aware of the situation.

Although multiple people across several OPM program offices were aware of the breach, it was not reported to OPM's Situation Room until Wednesday, November 2; four days after the incident was first detected.

OPM's Incident Response and Reporting Guide is an agency-wide policy that states "OPM employees and contractors must report any breach or potential breach of PII to the OPM

Situation Room within 30 minutes of becoming aware of the risk – regardless of the time or day of the week." Although several OCIO and RS employees reported the incident to their direct managers, every person that knew about the event had the responsibility to report it to the Situation Room. We believe that this indicates that OPM employees are not fully aware of the requirements outlined in the Incident Response and Reporting Guide

Recommendation 4

We recommend that the OCIO conduct improved agency-wide training and awareness campaigns related to incident response and reporting.

cc: Elizabeth A. Montoya
Chief of Staff

Richard B. Lowe
Director, Executive Secretariat and Ombudsman

Matthew E. Perry
Chief Information Officer

Kenneth J. Zawodny, Jr.
Associate Director, Retirement Services

[redacted]
Director
Internal Oversight & Compliance

[redacted]
Deputy Director
Internal Oversight & Compliance

[redacted]
Chief, Policy and Internal Control