U.S. DEPARTMENT OF
HOUSING AND URBAN DEVELOPMENT
OFFICE OF INSPECTOR GENERAL

November 6, 2012

MEMORANDUM NO: 2013-DP-0801

Memorandum

TO: Jerry E. Williams, Chief Information Officer, Q
Karen Newton Cole, Acting Chief Human Capital Officer, A

FROM: Hanh Do, Director, Information Systems Audit Division, GAA

SUBJECT: Improper Release of Personally Identifiable Information

INTRODUCTION

A breach of personally identifiable information (PII) occurred on September 21, 2012, in which an employee from the Office of the Chief Human Capital Officer emailed 8,444 U.S. Department of Housing and Urban Development (HUD) employees an Excel file that contained employees' full names and Social Security numbers. We determined that HUD responded to the incident properly, following United States Computer Emergency Readiness Team (US-CERT), National Institute of Standards and Technology, and HUD policy and other Federal requirements. However, we noted some areas of concern for safeguarding HUD information as well as suggested improvements for limiting the exposure of HUD's information in the future.

METHODOLOGY AND SCOPE

The Office of Inspector General (OIG) was notified of a PII incident on September 24th. We performed a review to determine whether HUD followed proper policies and procedures in responding to the breach of PII. Specifically, for this incident, we identified what actions were taken and any deficiencies within HUD policies, plans, or current practices. We performed this review at HUD headquarters from September 28th-October 19th. We interviewed members of HUD's Breach Notification Response Team who were directly involved in the identification and corrective actions associated with this incident. Interviewees included the senior agency official for privacy, Chief Information Officer, Deputy Chief Information Officer, privacy officer, data center services director, chief information security officer, OIG representative, and Chief Human Capital Officer (manager of the program experiencing the breach). [redacted]

Office of Audit (Information Systems Audit Division)
451 7th Street S.W., Room 8174, Washington, DC 20410
Phone (202) 402-0344, Fax (202) 401-1578
Visit the Office of Inspector General Website at www.hudoig.gov

[redacted]

BACKGROUND

The purpose of the email was to provide employees with information regarding their responsibilities in the process of performance ratings and information on self-assessments in the performance management process. The email contained an attached file. The file contained a table, which upon exploration of the supporting worksheets, exposed employee names and Social Security numbers. Approximately 1 hour after the email was sent, an employee called the help desk to report that the email contained PII. HUD's Breach Notification Response Team, composed of representatives from the various stakeholders within HUD, was notified and convened to address the incident. Members of the team include the following officials or representatives from the following offices:

Senior agency official for privacy
Privacy officer
Chief information security officer
Assistant Secretary for Congressional and Intergovernmental Relations
Associate chief information officer for information assurance
Chief Financial Officer
Chief Information Officer
Chief Procurement Officer
Customer relationship manager
General Counsel
General Deputy Assistant Secretary for Public Affairs
Chief Human Capital Officer
Office of Inspector General
Senior advisor to the Secretary
Affected program manager

[redacted]

RESULTS OF REVIEW

HUD followed proper procedures for responding to the incident. The Office of the Chief Information Officer reviewed the email, confirmed that it contained PII, and notified US-CERT of the incident. Various individuals from the Office of the Chief Information Officer worked together to remove the email from the mail servers and BlackBerrys and issued a recall of the initial email from individual users. [redacted]

However, we noted some areas of concern for safeguarding HUD information as well as suggested improvements for limiting the exposure of HUD's information in the future.

1. Contrary to HUD's electronic mail policy, HUD used a broadcast email in place of the Intranet to disseminate performance-related information. The email had an Excel file attachment that included names and Social Security numbers of 8,444 current HUD employees. HUD's Electronic Mail Policy, section 7.6.c, states, whenever possible, HUD's Intranet should be used in place of broadcast email messages. HUD Policy identifies broadcast email messages as those that are sent to all HUD employees or program area subsets by senior level management to ensure all appropriate employees are aware of HUD sponsored business-related or mandatory events.

2. [redacted]

3. HUD's procedures for notifying individuals of a privacy breach state, "Notice shall be provided without unreasonable delay but no later than 45 days after a risk of harm analysis has been conducted." Allowing up to 45 days for notifying employees of a privacy breach appears to be excessive.

4. [redacted] Office of Management and Budget Memorandum 07-16, issued in May of 2007, requires that agencies implement a solution to reduce the use of Social Security numbers. It instructs agencies to

   A. Eliminate unnecessary use. Agencies must now also review their use of Social Security numbers in agency systems and programs to identify instances in which collection or use of the Social Security number is superfluous. Within 120 days from the date of this memorandum, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of Social Security numbers within 18 months.

   B. Explore alternatives. Agencies must participate in government wide efforts to explore alternatives to agency use of Social Security numbers as a personal identifier for Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

SUGGESTED IMPROVEMENTS

1A. The Office of the Chief Human Capital Officer and all other programs should use a shared Intranet location for large information exchange according to HUD policy.

1B. HUD should explore other options (e.g., Citrix connections) that would provide a safe and secure environment in which to perform work activities for large files and data.

1C. HUD should reinforce the security awareness training of those HUD employees who handle PII or provide additional annual training to those who handle PII more frequently.

2A. [redacted]

3A. HUD should consider reducing the number of days the Department has to notify individuals after a risk of harm analysis is completed.

4A. [redacted]

4B. [redacted]

cc:
Maurice Jones, Deputy Secretary, SD

bcc:

G	Montoya	8256
G	Albert	8256
G	Chron	8256
GA	Rokosz	8286
GA	Chron	8286
GAA	Do	8174
GAA	Bagley	8174
GAA	Bardak	8174
GAA	Chron	8174

Concurrence:

Admin	Bardak	Bagley	Do	Rokosz	Albert	Montoya