Office of Audits
Office of Inspector General
U.S. General Services Administration

Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015

Report Number A160028/O/T/F16003
September 28, 2016

REPORT ABSTRACT

OBJECTIVE

Our objective was to determine whether GSA identified and notified individuals affected by the September 18, 2015, personally identifiable information (PII) breach pursuant to federal requirements and applicable guidance and policy.

Acquisition and Information Technology Audit Office (JA-T)
1800 F Street, NW, Room 5215
Washington, DC 20405
(202) 273-7245

Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015

Report Number A160028/O/T/F16003
September 28, 2016

WHAT WE FOUND

GSA failed to notify over 8,200 individuals affected by the PII breach within 30 days as required by Agency policy. This occurred due to a series of lapses in GSA's breach response process. Although GSA made several attempts to notify the affected individuals, it has not been able to show that its efforts were fully successful. Without timely and effective notice of a PII breach, individuals cannot take appropriate steps to protect themselves against the possibility of harm resulting from the exposure of their PII.

WHAT WE RECOMMEND

We recommend the Senior Agency Official for Privacy/Chief Information Officer:

1. Review and certify GSA's September 18, 2015, breach notification efforts and determine if any additional action is needed to ensure all affected individuals have been notified.
2. Develop and implement a training program for Agency Response Team members regarding their specific roles and responsibilities.
3. Evaluate the Agency's breach response capability by:
   a. Assessing the technical tools that will be used to identify and notify the individuals affected by a potential breach to ensure they are operating as intended;
   b. Requiring periodic testing of the Agency Response Teams to ensure members understand their roles and responsibilities, training is effective, and lessons learned are identified and incorporated; and
   c. Requiring an after action assessment of Agency Response Teams' response to actual breach incidents to identify and incorporate lessons learned.
4. Assess policies to ensure objectives are clear, roles and responsibilities are detailed, and comprehensive procedures are established for Agency Response Teams to communicate and document relevant information necessary for making decisions and taking action in response to a PII breach. Take appropriate actions to address and correct those areas identified as deficient.

GSA COMMENTS

The Deputy Chief Information Officer concurred with the audit report finding and recommendations. GSA's written comments to the draft report are included in their entirety as ***Appendix B.***

Table of Contents

Introduction **1**

Results

Finding – GSA failed to notify individuals affected by the PII breach as required by GSA policy, due to a breakdown in its breach response process *3*

Conclusion **9**

Recommendations **9**

GSA Comments **10**

Appendixes

Appendix A – Scope and Methodology **A-1**

Appendix B – GSA Comments **B-1**

Appendix C – Report Distribution **C-1**

Introduction

On September 18, 2015, in response to a request for a listing of active Agency travel cardholders, a GSA employee transmitted an unencrypted file to the Agency's independent external financial statement auditor. The file contained personally identifiable information (PII) such as the names, home addresses, and personal email addresses for over 8,200 current and former GSA and GSA Office of Inspector General (OIG) employees, including special agents and criminal investigators. The external auditor determined that the file contained PII that it did not need to know and promptly notified GSA. GSA subsequently determined that a breach occurred.

We performed an audit of GSA's response to this breach. We found that GSA failed to notify individuals affected by the breach within 30 days as required by Agency policy. Although GSA made several attempts to notify the affected individuals, we could not confirm whether these attempts were entirely successful.

Purpose

We performed this audit after discovering that GSA OIG employees, who are also GSA travel cardholders and were affected by the September 18, 2015, breach, did not receive notification regarding the exposure of their PII. We determined that GSA's initial attempt to notify individuals affected by the PII breach failed. Given the scope of the breach and the potential risk to the individuals whose information was exposed, we initiated an audit on November 18, 2015, of GSA's response to the breach.

Objective

Our objective was to determine whether GSA identified and notified individuals affected by the September 18, 2015, PII breach pursuant to federal requirements and applicable guidance and policy.

Background

GSA's Privacy Act Program (Privacy Program) was established to ensure that the Agency fulfills the requirements of the Privacy Act of 1974 (the Act). The Act balances an individual's right to privacy with the federal government's need to use personal information to accomplish its mission. The Act requires agencies to maintain systems of records that retain and collect only relevant and necessary information about an individual. Agencies are also required to:

> …establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could

> result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[1]

The Privacy Program applies to all GSA services, staff offices, and regional components. It also applies to all GSA employees who manage, acquire, maintain, disseminate, or use PII protected by the Act. The *GSA Information Breach Notification Policy* (Breach Notification Policy), citing policy and guidance promulgated by the Office of Management and Budget (OMB), defines PII as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[2] Further, the Breach Notification Policy states that determining whether information constitutes PII requires a "case-by-case assessment" and provides examples of PII that include, among others, social security numbers, name, date of birth, home address, and personal email.

Under this policy, GSA also identifies specific individuals to form its Agency Response Teams to address suspected breaches of PII. The nature and potential impact of the breach determines which team will be convened. The Initial Agency Response Team consists of the program manager of the program experiencing the breach, the Office of the Chief Information Security Officer, the Privacy Officer, and a member of the Office of General Counsel. This team determines if a breach occurred, the scope of the information breached, the potential impact of the breached information on individuals and on GSA, and whether the Full Agency Response Team needs to be convened. This team is made up of the four-member Initial Agency Response Team plus the Senior Agency Official for Privacy, the Chief Information Officer (CIO), and representatives from the Office of Communications and Marketing and the Office of Congressional and Intergovernmental Affairs.[3]

See ***Appendix A*** – Scope and Methodology for additional details.

[1] 5 U.S.C. 552a(e)(10) (2016)
[2] GSA Order CIO 9297.2B, March 31, 2015, citing *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (OMB Memorandum M-07-16, May 22, 2007) and *Guidance for Agency use of Third-Party Websites and Applications* (OMB Memorandum M-10-23, June 25, 2010).
[3] GSA's Chief Information Officer is also its Senior Agency Official for Privacy.

Results

GSA failed to notify individuals affected by the breach within 30 days as required by Agency policy. Although GSA made several attempts to notify the affected individuals, it has not been able to show that those efforts were fully successful. As a result, some affected individuals still may not know that their PII was breached. Without timely and effective notice of a PII breach, individuals cannot take appropriate steps to protect themselves against the possibility of harm resulting from the exposure of their PII. GSA must take measures to ensure future responses to PII breaches are handled according to federal requirements and applicable guidance and policy.

Finding – GSA failed to notify individuals affected by the PII breach as required by GSA policy, due to a breakdown in its breach response process.

GSA became aware of a PII breach affecting current and former employees on September 18, 2015, and promptly reported the breach to the United States Computer Emergency Readiness Team (US-CERT). Although GSA made an initial attempt to notify the affected individuals within 30 days of the US-CERT report as required by applicable policy, this notification reached less than 1 percent of the intended recipients. This occurred due to weaknesses in GSA's breach response processes including, but not limited to, an incomplete understanding of roles and responsibilities, inadequate communication between team members, overreliance on email to notify affected individuals, and insufficient oversight of the breach notification effort. GSA made several subsequent attempts to notify affected individuals and considered its notification efforts to be complete on January 6, 2016. However, we were unable to validate whether these attempts reached all affected individuals.

I. PII breach and failed notification

On September 18, 2015, in response to a request for a listing of active Agency travel cardholders, a GSA employee from the Travel & Purchase Card Program Division within the Office of Administrative Services (Program Office) transmitted an unencrypted file to the Agency's independent external financial statement auditor. The file contained PII such as the names, home addresses, and personal email addresses for over 8,200 current and former GSA and GSA OIG employees, including special agents and criminal investigators. The independent external financial statement auditor determined that the file contained PII that it did not have a need to know and promptly notified GSA.

Under OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, federal agencies are required to "report all incidents involving personally identifiable information to US-CERT." US-CERT acts as the information security incident center for the federal government in accordance with the Federal Information Security Management Act of 2002.[4] Accordingly, GSA filed a US-CERT report on the incident the day it occurred. A summary report of the incident

[4] 44 U.S.C. 3546 (2016)

was provided to the Privacy Officer who subsequently convened the Initial Agency Response Team, in accordance with the Breach Notification Policy.

The Initial Agency Response Team evaluated the breach and determined that it was necessary to convene the Full Agency Response Team because the breach affected over 1,000 individuals. The Full Agency Response Team determined that the affected individuals required notification regarding the exposure of their PII. In addition, the Full Agency Response Team concluded that those affected would not be offered credit monitoring. Instead, GSA would encourage them to leverage any credit monitoring that may have been offered by the Office of Personnel Management (OPM) in response to a separate OPM data breach discovered in June 2015.

GSA's Breach Notification Policy requires initial communication to affected individuals within 30 calendar days of the US-CERT report. In accordance with this requirement, GSA made an initial attempt to notify all individuals affected by the breach via a bulk email on October 9, 2015 – 21 days after the breach occurred. Although unknown at the time, this attempt reached less than 1 percent of the intended recipients because the email was intercepted and quarantined by GSA's spam filter. The email was quarantined because the spam filter flagged it as potentially containing sensitive information; however, the message did not actually contain any sensitive information. GSA was not aware that the message had been quarantined, because the spam filter was not monitored.

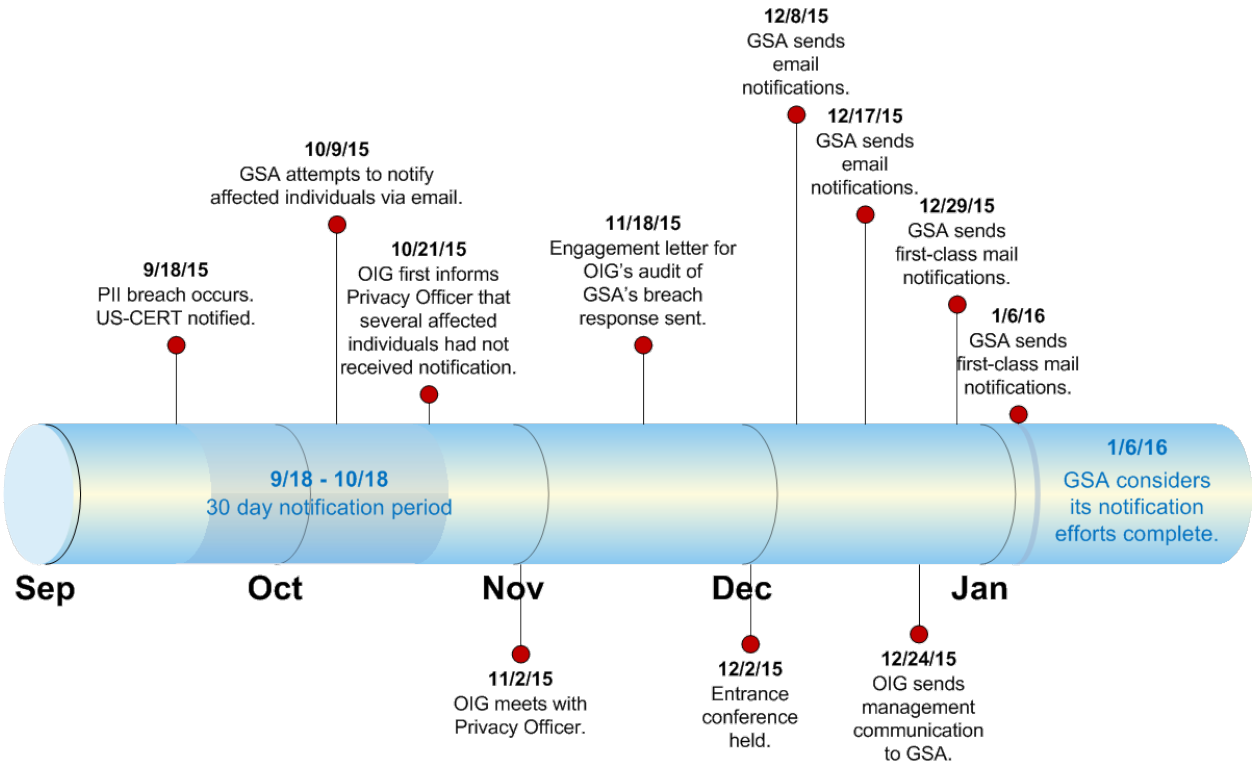
On October 21, 2015, we discovered that OIG employees who were affected by the September 18, 2015, breach did not receive notification regarding the exposure of their PII. That same day, we informed the Privacy Officer that the email notification may not have been fully successful; however, GSA took no further action. We met with the Privacy Officer on November 2, 2015, to determine why some individuals may not have received notification. However, neither the Privacy Officer nor an employee with GSA's Client and Remote Mail Branch she referred us to were able to explain why this email did not reach all intended recipients.

As a result of our concerns, we initiated our audit of GSA's breach response on November 18, 2015. At the audit entrance conference, held December 2, 2015, we again informed Agency officials that some affected individuals had not been notified. It was not until after this meeting that GSA took action to determine the cause of the notification failure. Subsequently, on December 8, 2015 – nearly 7 weeks after we initially informed GSA that affected individuals had not been notified – GSA sent another email to affected individuals. Although generally successful, this too did not reach all intended recipients. Based on the evidence provided by GSA, we estimate that this attempt reached approximately 5,300 affected individuals (61.7 percent).

GSA issued another email on December 17, 2015, which also was not entirely successful. Specifically, based on evidence provided by GSA, this email did not reach over 500 individuals (more than 6 percent) affected by the breach. As a result, on December 24, 2015, we issued a memorandum informing the GSA CIO that the

Agency's previous attempts to notify individuals had not been fully successful. We recommended that the GSA CIO take immediate action to fulfill its responsibility to identify and notify the affected individuals regarding the exposure of their PII. GSA subsequently made two notification attempts via first-class mail on December 29, 2015, and January 6, 2016, after which the Agency believed all affected individuals had been contacted. See *Figure 1* for a timeline of events related to GSA's response to the September 18, 2015, PII breach.

Figure 1 – Timeline of Events



GSA's notifications to affected individuals were not timely. Although GSA considers its notification efforts to be complete, it has not been able to show that those efforts were fully successful. As we discuss in detail below, these failures are the result of ineffective Agency Response Team processes, overreliance on email to notify affected individuals, and insufficient oversight of the breach response process.

II. Limited input from Agency Response Team members led to an ineffective breach response plan

GSA determined that it was necessary to convene the Full Agency Response Team because the breach affected over 1,000 individuals. The Full Agency Response Team consists of eight members and is responsible for determining how to respond to a breach and the best method for notifying affected individuals. Each member of the

team is selected for their expertise to ensure adequate coverage and implementation of the Agency's breach response plan.

We asked GSA for all records of discussion related to its response plan, to determine what information was shared for decision-making purposes. The emails GSA produced to us reflect that the GSA Privacy Officer proposed a response to the breach, but no detailed dialogue occurred among the Full Agency Response Team members about other potential approaches and related risks. For example, we found no evidence of any discussion to ensure that GSA obtained accurate contact information or used the most efficient method to notify affected individuals. This hampered GSA's ability to effectively respond to the breach.

Furthermore, at least two of the eight Full Agency Response Team members did not understand their obligations under GSA's breach response process or respond to requests for concurrence with the Privacy Officer's proposal. For example, the representative from the Office of Communications and Marketing responded to the Privacy Officer's proposal by stating,

> …we didn't recall being a part of the internal agency response team previously and thought we were included for notification purposes. If there is something that requires signoff, can we get an understanding of what we should be assessing? Otherwise I think I would defer to the others with expertise who have already concurred.

Another member of the team never responded to the Privacy Officer's request for concurrence. Despite not receiving direct input from two members of the eight member team, the Agency proceeded to move forward with its notification efforts.

III. Reliance on email over other forms of communication to notify affected individuals

Although the home addresses of the affected individuals were readily available, GSA chose to use email as the notification method to reach them. This approach conflicts with OMB Memorandum M-07-16*,* which states, "first-class mail notification to the last known mailing address of the individual in your agency's records should be the primary means notification is provided." Further, OMB has described email notification as "problematic," because individuals' email addresses often change. Rather than following OMB's guidance, GSA relied on email three times before using first-class mail to notify the remaining affected individuals, even though the file included a significant number of missing or inaccurate email addresses.

A. Lack of reliable or verified email addresses

GSA's initial attempt to create a contact list relied upon information contained in the breached file. When we reviewed the file, we determined email addresses were not included for 26.4 percent of the individuals listed. Additionally, the file contained

information for individuals who are no longer employed by GSA; therefore, the email addresses for those individuals (generally, @gsa.gov email addresses) were no longer valid. Further, some of the email addresses contained syntax errors that were only identified when GSA attempted to upload the list of email addresses into the bulk email software. These errors were identified when the software rejected the email addresses. However, GSA officials did not request help with notification efforts from GSA's Office of Human Resource Management until more than three months after the breach, when the Full Agency Response Team decided to provide notification via first-class mail.

B. Creation of unverified email addresses

The Program Office created an email address for individuals who did not have one included in the file. These email addresses were created by inserting a period (".") between the "first name" and "last name" fields in the file, and appending "@gsa.gov" to the end. For example, the email address created for an employee named John Doe would have been: "john.doe@gsa.gov."

In some instances, this process resulted in the creation of invalid email addresses. This further impaired GSA's efforts to notify the affected individuals. Factors that led to the creation of these invalid email addresses included:

- Incorrect Names. When a name in the file was incorrect (*e.g.*, due to a misspelling, former name, etc.), the erroneous information was incorporated into the email address.

- Blank Spaces. When a blank space was included in the "first name" or "last name" field, the blank space was incorporated into the email address. However, blank spaces are not permitted for email addresses.

IV. Insufficient oversight of the PII breach response process

GSA did not have effective processes in place to monitor the results of its breach notification efforts. As a result, GSA had no assurance whether its efforts to notify those affected by the breach were effective.

A. Lack of an effective confirmation process for email notification

GSA relied on the receipt of delivery error messages, or bounce backs, to determine the success of its initial notification attempt. When no delivery error messages were received, the Agency assumed its notification attempt was successful. This approach was problematic in this instance because delivery error messages were not generated when GSA's spam filter prevented the bulk email process from continuing. When asked why this occurred, employees with GSA IT's Platform Operations and Management Division could not explain why the spam filter incorrectly flagged and quarantined any email as containing sensitive information. In addition, an email notification to a valid

email address – but to the wrong individual – would not have resulted in a delivery error message.

B. Lack of clear guidance on actions needed to confirm notification

GSA's Breach Notification Policy requires that the Program Office responsible for the breach "provide evidence that notification was provided to impacted individuals…." However, the policy does not clearly define what evidence is necessary to confirm notification and to whom this evidence should be provided. Further, the policy does not require the Privacy Officer or the Agency Response Teams to seek confirmation from the Program Office that the notification attempt was successful. In this case, GSA's Travel & Purchase Card Program Division within the Office of Administrative Services did not provide evidence that affected individuals received notification. Additionally, neither the Privacy Officer nor the Full Agency Response Team sought confirmation that affected individuals received notification.

C. Inadequate tracking of notification efforts

We provided GSA with a random sample of 368 individuals selected from the original file subject to the breach. We then asked GSA to identify if, when, and how each individual was notified. For purposes of our audit, we considered notification to be complete if GSA provided evidence to support that an email or notification letter had been delivered to the intended recipient.

GSA was unable to provide evidence that 100 individuals in our sample (27.2 percent) were notified that they were affected by the breach. After we expressed concerns that we could not locate supporting evidence for nearly a third of the individuals in our sample, we gave GSA another opportunity to provide evidence for the remaining individuals. GSA provided a second submission. When we reviewed this submission, we noticed that several of the notification claims made were contrary to the evidence provided. For example, we identified an instance where GSA claimed an individual received a notification via email; however, the materials GSA provided clearly show a delivery failure for the individual. Based on the evidence provided by GSA to date, we cannot confirm whether the Agency notified 100 of the sampled individuals (27.2 percent).

Conclusion

A breakdown in GSA's breach response process caused the Agency's failure to timely notify over 8,200 affected individuals of the unauthorized exposure of their PII. While GSA policy requires notification of a breach within 30 days of an incident, 110 days passed between the date of the breach and GSA's final notification attempt. In addition, although GSA considered its notification efforts complete as of January 6, 2016, it could not provide evidence to show that its efforts were fully successful. Accordingly, some affected individuals may remain unaware that their PII was inappropriately released.

GSA's failure to develop a well-defined action plan to respond to this incident, combined with management oversight failures, left affected individuals vulnerable to identity theft, substantial harm, embarrassment, and inconvenience. Additionally, the Agency exposed itself to significant reputational risk and potential litigation. GSA should conduct a comprehensive review of its breach notification policy and breach response process and implement necessary changes to better position the Agency to more effectively respond in the event of future breaches.

Recommendations

We recommend the Senior Agency Official for Privacy/Chief Information Officer:

1. Review and certify GSA's September 18, 2015, breach notification efforts and determine if any additional action is needed to ensure all affected individuals have been notified.
2. Develop and implement a training program for Agency Response Team members regarding their specific roles and responsibilities.
3. Evaluate the Agency's breach response capability by:
    a. Assessing the technical tools that will be used to identify and notify the individuals affected by a potential breach to ensure they are operating as intended;
    b. Requiring periodic testing of the Agency Response Teams to ensure members understand their roles and responsibilities, training is effective, and lessons learned are identified and incorporated; and
    c. Requiring an after action assessment of Agency Response Teams' response to actual breach incidents to identify and incorporate lessons learned.
4. Assess policies to ensure objectives are clear, roles and responsibilities are detailed, and comprehensive procedures are established for Agency Response Teams to communicate and document relevant information necessary for making decisions and taking action in response to a PII breach. Take appropriate actions to address and correct those areas identified as deficient.

GSA Comments

The Deputy Chief Information Officer concurred with the audit report finding and recommendations. GSA's written comments to the draft report are included in their entirety as ***Appendix B***.

Audit Team

This audit was conducted by the individuals listed below:

Sonya Panzo	Audit Manager
Daniel Riggs	Auditor-In-Charge
Reynaldo Gonzales	Auditor

On their behalf, we thank you and your staff for your assistance during this audit.

Appendix A – Scope and Methodology

Scope and Methodology

We initiated an audit of GSA's response to the PII breach that occurred on September 18, 2015, to assess the Agency's ability to efficiently notify affected individuals regarding an information breach, in accordance with applicable guidance and policy.

To accomplish our objectives, we:

- Reviewed the related US-CERT Summary Report, to develop our understanding of the incident;
- Reviewed GSA's June 2015 active travel cardholder file subject to the PII breach, to evaluate the nature and scope of the information breached;
- Interviewed Agency management responsible for GSA's Privacy Program and personnel responsible for executing the information breach notification process;
- Interviewed GSA employees and GSA OIG staff regarding receipt of the initial Agency breach notification on October 9, 2015;
- Researched applicable federal guidance and reports and GSA policy related to information breach handling and incident response management;
- Reviewed user manuals and process diagrams for applicable software and applications;
- Reviewed email correspondence between members of GSA's Initial Agency Response Team and Full Agency Response Team, to ascertain the Agency's initial assessment of and planned response to the incident;
- Obtained email addressee lists for each email notification attempt, copies of the breach notifications sent via email, and all copies of correspondence sent via first-class mail to affected individuals;
- Reviewed email log reports to determine message delivery status to affected individuals;
- Used a random sample of 368 affected individuals, to determine the completeness of GSA's notification attempt, based on supporting documentation; and
- Compared the Agency's notification claims against its supporting documentation to identify and resolve any discrepancies and estimate the effectiveness of its notification attempts.

We conducted the audit between November 2015 and March 2016 in accordance with generally accepted government auditing standards. Those standards require that 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A – Scope and Methodology (cont.)

Internal Controls

Our assessment of internal controls was limited to those necessary to address the objective of our audit. Identified internal control issues are discussed in the Results section of this report.

Appendix B – GSA Comments

GSA

GSA Office of the Chief Information Officer

September 22, 2016

Mr. Brian J. Gibson
Associate Deputy Assistant Inspector General for Auditing
Acquisition and Information Technology Audit Office (JA-T)
General Services Administration
Office of Inspector General
Washington, DC 20405

Dear Mr. Gibson,

GSA IT appreciates the opportunity to review and comment on the Office of the Inspector General Draft final report entitled, *Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015* (A160028).

In the report, the Office of Inspector General recommends:

The Senior Agency Official for Privacy/Chief Information Officer:

1. Review and certify GSA's September 18, 2015, breach notification efforts and determine if any additional action is needed to ensure all affected individuals have been notified.
2. Develop and implement a training program for Agency Response Team members regarding their specific roles and responsibilities.
3. Evaluate the Agency's breach response capability by:
    a. Assessing the technical tools that will be used to identify and notify the individuals affected by a potential breach to ensure they are operating as intended;
    b. Requiring periodic testing of the Agency Response Teams to ensure members understand their roles and responsibilities, training is effective, and lessons learned are identified and incorporated; and
    c. Requiring an after action assessment of Agency Response Teams' response to actual breach incidents to identify and incorporate lessons learned.
4. Assess policies to ensure objectives are clear, roles and responsibilities are detailed, and comprehensive procedures are established for Agency Response Teams to communicate and document relevant information necessary for making decisions and taking action in response to a PII breach. Take appropriate actions to address and correct those areas identified as deficient.

U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
www.gsa.gov

GSA IT concurs with all the findings and recommendations cited in the draft report.

If you have any questions or concerns regarding this matter please contact me at 202-501-1000, or Lesley Briante, Associate CIO, at (202) 501-0797.

Sincerely,

Steve Grewal
Deputy Chief Information Officer (I)

U.S. General Services Administration
Comments for OIG Draft Report
***Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015* (A160028)**

Appendix C – Report Distribution

GSA Administrator (A)

Deputy Administrator (AD)

Chief of Staff (AC)

Deputy Chief of Staff (AC)

Senior Agency Official for Privacy/Chief Information Officer (I)

Deputy Chief Information Officer (ID)

Privacy Officer (ISP)

Chief Administrative Services Officer (H)

GAO/IG Audit Management Division (H1G)

Audit Liaison, GSA IT (IDRP)

Assistant Inspector General for Auditing (JA)

Director, Audit Planning, Policy, and Operations Staff (JAO)