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

IMPLEMENTATION REVIEW OF CORRECTIVE ACTION PLAN

Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015 Report Number A160028/O/T/F16003 September 28, 2016

Assignment Number A180001
October 19, 2018

Table of Contents

Introduction

We have completed an implementation review of the management actions taken in response to the recommendations contained in our September 2016 audit report, *Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015*, Report Number A160028/O/T/F16003 (see ***Appendix A***).

Objective

The objective of our review was to determine whether the Office of GSA IT (GSA IT) has taken the actions as outlined in the corrective action plan for *Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015*. To accomplish our objective we:

1. Examined documentation submitted by GSA IT supporting the completion of the action plan steps;
2. Performed testing of the corrective actions outlined in GSA IT's action plan; and
3. Interviewed Agency personnel responsible for GSA's Privacy Program and personnel from the Office of the Deputy Chief Information Officer.

Background

On September 18, 2015, a GSA employee transmitted an unencrypted file to the Agency's independent external financial 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 employees. The external auditor determined that the file contained PII that it did not need to know and promptly notified GSA. GSA's Initial Agency Response Team (Response Team) subsequently determined that a breach occurred.[1]

On September 28, 2016, we issued an audit report, *Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015*, to GSA IT. GSA IT oversees the Agency's breach response process and notification procedures. The objective of the audit 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.

Our audit found that GSA failed to notify individuals affected by the PII breach as required by GSA policy, due to a breakdown in its breach response process.

[1] The Initial Agency Response Team is composed of the program manager of the program experiencing or responsible for the breach, the Chief Information Security Officer, the Chief Privacy Officer, and a member of the Office of General Counsel.

To address the finding identified in our report, we recommended that 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.

The Deputy Chief Information Officer concurred with our report finding and recommendations.

Results

Our implementation review determined that GSA IT did not satisfactorily implement the following corrective actions:

1. Evaluate whether every reasonable attempt has been made to identify/notify any individuals not previously identified/notified. If not, attempt to do so.
2. Review all relevant policies dealing with breach of Personally Identifiable Information; identify strengths and/or weaknesses; amend policy(ies) as appropriate; and provide information regarding and updates to roles and responsibilities to response team members prior to the first annual training and/or test.

See ***Appendix A*** for highlighted steps that were not fully implemented.

Finding 1 – GSA IT did not issue timely breach notifications.

Our original audit found that GSA failed to notify over 8,200 individuals affected by the PII breach within 30 days as required by its *GSA Information Breach Notification Policy* (Breach Notification Policy).[2] In its action plan, GSA IT stated that it would evaluate whether every reasonable attempt was made to notify those individuals that had not been previously notified. If not, GSA IT asserted that it would attempt to notify these individuals. GSA IT stated that it would provide evidence of these notifications to our office by January 2017. However, GSA IT did not notify 20 of the remaining 26 individuals affected by the PII breach until December 2017, more than two years after the initial breach occurred. Without timely and effective notice of the breach, the affected individuals could not take prompt action to protect themselves against the possibility of harm resulting from the exposure of their PII.

GSA's Chief Privacy Officer conducted a review in January 2017 and determined that the Agency had not notified 26 individuals affected by the PII breach. GSA management could not find contact information for 6 of the affected individuals. In February 2017, the Chief Privacy Officer provided the program office responsible for the breach with the names and addresses of the remaining 20 affected individuals and authorized the responsible program office to mail breach notifications to these individuals. We inquired about the status of these notifications in November 2017 and learned that the responsible program office still had not mailed the notifications to the affected individuals. After our inquiry, the responsible program office mailed the notifications to the remaining 20 individuals on December 5, 2017 – 809 days after the initial breach occurred.

[2] GSA Order CIO 9297.2B, dated March 31, 2015, required GSA to notify affected individuals within thirty (30) calendar days from the date it was reported to the United States Computer Emergency Readiness Team (US-CERT). During our implementation review, GSA issued GSA Order CIO 9297.2C, dated July 31, 2017, changing the notification timeframe to 60 calendar days from the date the incident was determined to be a breach. This change is discussed further in *Finding 2*.

Although the breach notifications were not issued in a timely manner, the responsible program office ultimately notified the remaining 20 individuals. In accordance with GSA's Breach Notification Policy, the responsible program office also provided confirmation to the Chief Privacy Officer that the notices were sent. As a result, no further action is needed by GSA IT to address this recommendation. GSA should, however, assess the factors that led to the excessive delay in issuing the notifications to the affected individuals and consider additional controls to ensure future notifications are sent in accordance with the timeframes set forth by its Breach Notification Policy.

Finding 2 – GSA IT's revised Breach Notification Policy could hinder the timeliness of future PII breach notifications.

Our original audit found that lapses in GSA's breach response process led to untimely notifications. In its action plan, GSA IT stated that it would review, improve, and amend its PII policies as appropriate. GSA IT also stated that it would assess gaps and weaknesses of relevant policies and provide us with amended policies by July 2017. On July 31, 2017, GSA issued its revised Breach Notification Policy. However, we found that the policy changes allow for an unreasonable delay in GSA's timeframe for determining that a breach has occurred and notifying affected individuals. This could prevent affected individuals from taking prompt and appropriate measures to protect themselves from potential harm, identity theft, embarrassment, harassment, or inconvenience stemming from the unauthorized exposure of their PII.

Under GSA's previous Breach Notification Policy, the timeframe to notify individuals affected by a PII breach started from the date the incident was reported to US-CERT.[3] The previous policy further required GSA to identify and notify individuals affected by the breach within 30 days of reporting the incident to US-CERT. In its revised Breach Notification Policy, GSA IT adjusted the notification timeframe to begin when GSA's Response Team determines that a breach has occurred. However, the policy does not specify the amount of time the Response Team has to make its determination which could indefinitely extend the notification timeframe. GSA further extended the notification timeframe by increasing the amount of time the Agency has to identify and notify those affected by the breach to 60 days from the date the Response Team determined that a breach occurred. The Chief Privacy Officer stated that these changes allow GSA more time to investigate the breach and correctly understand all of the facts before attempting to notify those affected. Nonetheless, the changes place affected individuals at risk because they increase GSA's timeframe to notify these individuals that their PII was exposed.

We assessed the effect of these revisions on four confirmed breaches that were remediated in Fiscal Year 2017. We found that GSA's Response Team took an average of 70 days to determine

[3] The Federal Information Security Modernization Act of 2014 requires agencies to notify US-CERT regarding information security incidents within one hour of being identified. Security incidents are those where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised.

if a breach occurred from the date of the incident. As the policy now allows up to 60 days after the Response Team's breach determination to notify affected individuals of the unauthorized exposure of their PII, these individuals may not be notified of a breach for 130 days – or more than 4 months – after a breach has occurred. In one incident involving PII related to background investigations, the Response Team did not determine that a breach occurred until 181 days after it became aware that PII was exposed. Thus, GSA had a total of 241 days (approximately 8 months) to make a determination and to issue notifications.

GSA's revisions to its Breach Notification Policy provide limited assurance that the Agency's breach response process and procedures will enable it to respond to future PII breaches in a timely manner and without unreasonable delay. Therefore, we conclude that GSA IT did not satisfactorily complete this action step.

Conclusion

Our implementation review determined that GSA IT did not successfully implement corrective actions for audit recommendations 1 and 4. Specifically, GSA IT did not notify remaining individuals who were affected by the September 18, 2015, breach that their PII was exposed until more than 2 years after the breach occurred. GSA has since issued notices to these individuals. While no further notifications are required, GSA should assess the factors that led to the excessive delay in notifying affected individuals and consider additional controls to ensure timely notifications in the future. Additionally, although GSA IT assessed and revised its Breach Notification Policy in accordance with its corrective action plan, the revisions made hinder its ability to notify affected individuals without unreasonable delay in the future. Therefore, GSA IT's revisions to its Breach Notification Policy hinder the Agency's ability to notify affected individuals without unreasonable delay and could significantly extend breach notification timeframes. These revisions did not meet the spirit of our recommendation, which was aimed at improving the Agency's policies for responding to PII breaches.

As a result, GSA IT must submit a revised corrective action plan addressing this outstanding recommendation by November 19, 2018, to this office and the Audit Management Division (H1EB).

Audit Team

This review was managed out of the Acquisition and Information Technology Audit Office and conducted by the individuals listed below:

Sonya D. Panzo	Associate Deputy Assistant Inspector General for Auditing
Kyle D. Plum	Audit Manager
Bruce E. McLean	Auditor-In-Charge

Appendix A – Corrective Action Plan for Report Number A160028/O/T/F16003

Designated Responding Official: **REDACTED**
Contact Person: **REDACTED**
Telephone Number: **REDACTED**
Date: 11/25/2016

Audit: A160028/O/T/F16003 Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015	Recommendation Number: 001	Proposed Recommendation Completion Date: 01/31/2017

Recommendation 001: 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.

Action to be Taken Step by Step	**Supporting Documentation to be sent to H1G**	**Documentation will be sent the last day of**
001 The Chief Privacy Officer will: a. review records of: individuals affected by the breach; b. individuals notified; c. list any individuals who may not have been identified and/or notified; and d. Evaluate whether every reasonable attempt has been made to identify/notify any individuals not previously identified/notified. If not, attempt to do so.	Documentation with names of individuals, contact date and means of contact, evidence of notification to the affected individuals (e.g. email logs and posted letters, to the extent these exist), and cover letter affirming Chief Privacy Officer's review.	January 2017

Appendix A – Corrective Action Plan for Report Number A160028/O/T/F16003 (cont.)

Audit: A160028/O/T/F16003 Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015	Recommendation Number: 002	Proposed Recommendation Completion Date: 04/30/3017

Recommendation 002: Develop and implement a training program for Agency Response Team members regarding their specific roles and responsibilities.

Action to be Taken Step by Step	**Supporting Documentation to be sent to H1G**	**Documentation will be sent the last day of**
002. Develop: a) training course curriculum; b) recommend training method (e.g. classroom, online) c) target audience (e.g. Agency Response Teams and any back-ups) d) Conduct the training prior to the annual test (see below)	a) Outline of proposed training curriculum; b) recommended method; c) target audience; d) attendance record	February 2017 February 2017 February 2017 April 2017

Appendix A – Corrective Action Plan for Report Number A160028/O/T/F16003 (cont.)

Audit: A160028/O/T/F16003 Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015	Recommendation Number: 003	Proposed Recommendation Completion Date: 07/31/2017

Recommendation 003: Evaluate the Agency's breach response capability by:

a. Assessing the technical tools that are 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.

Action to be Taken Step by Step	**Supporting Documentation to be sent to H1G**	**Documentation will be sent the last day of**
003: Evaluate breach response capability: a. Assess for effectiveness technical tools used to identify and notify individuals potentially affected by a breach; b. Develop annual test schedule to: ● review roles and responsibilities with Agency Response Teams prior to the test; ● allow time for Agency Response Teams to ask questions about their roles and responsibilities during and after test; ● solicit Agency Response Teams' feedback to assess whether the test was effective/realistic, and incorporate lessons learned into any subsequent tests; and provide role and responsibility	a) Analysis of technical tools available for use to identify and notify potentially affected individuals b) Copy of schedule c) Execute at least one breach test and provide documentation of lessons learned	a) February 2017 b) February 2017 c) July 2017

training materials to any response team member who joins after the annual training and/or test; request that the departing response team member provide on-the-job training and answer any questions the new member may have; and require the new member to provide a confirmation, e.g. email confirming receipt and review of training materials. c. Run at least one test of Agency action teams by 06/30/2017		

Appendix A – Corrective Action Plan for Report Number A160028/O/T/F16003 (cont.)

Audit: A160028/O/T/F16003 Audit of GSA's Response to the Personally Identifiable Information Breach of September 18, 2015	Recommendation Number: 004	Proposed Recommendation Completion Date: 07/31/2017

Recommendation 004: 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.

Action to be Taken Step by Step	**Supporting Documentation to be sent to H1G**	**Documentation will be sent the last day of**
Review all relevant policies dealing with breach of Personally Identifiable Information; identify strengths and/or weaknesses; amend policy(ies) as appropriate; and provide information regarding and updates to roles and responsibilities to response team members prior to the first annual training and/or test.	Gap analysis of relevant policies that identifies gaps and weaknesses. Mitigation plan and/or copies of proposed amended policies	July 2017

Appendix B – 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)

Chief Privacy Officer (ISP)

Chief Administrative Services Officer (H)

Audit Management Division (H1EB)

Audit Liaison, GSA IT (IDRGS)

Assistant Inspector General for Auditing (JA)

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