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

Audit of the Migration of Legacy GSA Human Resource Systems to HR Links

Report Number A190056/C/T/F21004
July 16, 2021

Executive Summary

Audit of the Migration of Legacy GSA Human Resource Systems to HR Links
Report Number A190056/C/T/F21004
July 16, 2021

Why We Performed This Audit

This audit was included in our *Fiscal Year 2019 Audit Plan* after the launch of HR Links resulted in the exposure of sensitive information. HR Links is a major software application that provides human resource services to approximately 21,000 federal employees, including 11,000 who work for GSA. Our objective was to determine whether GSA appropriately managed risks associated with migrating its legacy human resource systems to HR Links, which launched on June 4, 2018.

What We Found

GSA did not sufficiently manage risks associated with migrating its legacy human resource systems to HR Links. We found that GSA did not adequately test HR Links or fully address problems identified during system testing. As a result, HR Links had a series of significant system weaknesses upon deployment. These weaknesses caused the exposure of sensitive information (including personally identifiable information), incomplete and inaccurate employee information, and functional deficiencies. Although GSA has addressed these deficiencies, it should apply lessons learned from the HR Links deployment to ensure that appropriate testing is conducted to identify and mitigate risks for future system deployments.

What We Recommend

We recommend that GSA's Chief Human Capital Officer and Chief Information Officer, prior to the deployment of future systems, design and implement appropriate system testing to ensure that:

a. Required system security controls, including those governing user roles and data permissions, are operating effectively;
b. Data is complete and accurately migrated from legacy systems, if applicable; and
c. System testing verifies that all functional requirements are met.

The GSA Chief Human Capital Officer and Chief Information Officer agreed with our finding and recommendation. GSA's response is included in its entirety in ***Appendix B*** – GSA Comments.

Table of Contents

Introduction

We performed an audit of HR Links, a human resource (HR) and time and attendance (TA) software application that supports approximately 21,000 federal employees, including 11,000 who work for GSA.

Purpose

This audit was included in our *Fiscal Year 2019 Audit Plan* after end users experienced multiple issues when GSA deployed HR Links. As the shared service provider for HR and payroll services, GSA migrated its 11,000 federal employees' information, as well as 32 other federal client agencies' information, to HR Links. Due to the issues end users experienced when HR Links launched, we sought to determine if deficiencies existed in GSA's system migration process.

Objective

Our objective was to determine whether GSA appropriately managed risks associated with migrating its legacy HR systems to HR Links. Specifically, we assessed whether GSA planned for the migration, assessed risks, and performed adequate and appropriate testing on HR Links prior to making the system available to end users in accordance with system requirements and other applicable federal standards.

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

Background

GSA provides HR and payroll services for GSA and 32 other federal agencies, supporting approximately 21,000 federal employees. In November 2016, GSA awarded a 10-year, $149 million contract to International Business Machines (IBM) for HR Links, a commercial-off-the-shelf product used for human capital management. GSA's migration to HR Links replaced the following legacy systems:

- The Comprehensive Human Resources Integrated System (CHRIS), which was used to manage HR transactions, such as performance appraisals;
- The Electronic Time and Attendance Management System (ETAMS), which was used to manage employee timesheets; and
- The Authorized Leave and Overtime Help Application (ALOHA), which was used to manage employee leave requests.

Prior to HR Links, GSA managed its HR and TA transactions in these separate legacy systems. HR Links combined the management of HR and TA transactions.

GSA's migration to HR Links. The HR Links migration occurred from November 2016 to June 2018. IBM configured HR Links to meet the requirements of GSA and its client agencies. GSA's

Office of Human Resources Management and Office of GSA IT worked collaboratively with IBM to design, build, and test HR Links.

HR Links system security. In HR Links, system security consists of two attributes assigned to a user's profile: user roles and data permissions. These attributes are designed to work together to define the actions a user may take in the system and the scope of information they are able to access. HR Links user roles and data permissions are described below.

- **User roles** in the system are assigned to a user's profile depending on their day-to-day responsibilities at GSA, such as time administrator or HR administrator. Users with the time administrator role perform higher-level TA tasks, such as reviewing timesheets and approving leave if no other user is available. Users with the HR administrator role are able to approve employee promotions and raises. However, user roles alone do not grant the ability to access other employees' information or requests.

- **Users' data permissions** control the specific employee information and requests they are able to view. For example, an HR administrator may have data permissions to view only the employees they support. A time administrator with data permissions to an entire department can view the TA information and requests for all employees in the department. Accordingly, HR Links must be configured to manage data permissions to protect employee information from unauthorized disclosure.

Results

Finding – GSA did not adequately test HR Links or fully address problems identified during testing prior to system deployment, resulting in sensitive information exposures, incomplete and inaccurate data, and functional deficiencies.

GSA did not sufficiently manage risks associated with migrating its legacy HR systems to HR Links. We found that GSA did not adequately test HR Links or fully address problems identified during system testing. As a result, HR Links had a series of significant system weaknesses upon deployment. As described below, these weaknesses caused the exposure of sensitive information (including personally identifiable information [PII]), incomplete and inaccurate employee information, and functional deficiencies. According to GSA personnel, the system testing was challenged by project delays that affected the test data and testing schedule. Although GSA has since addressed the deployment issues, it should apply lessons learned from the HR Links deployment to ensure that appropriate testing is conducted to identify and mitigate risks for future system deployments.

Inappropriate Information Access Resulted in the Exposure of Sensitive Information

The Federal Information Security Modernization Act of 2014 requires that information systems limit users' access to only the information for which they are authorized.[1] To meet this requirement and protect the confidentiality and integrity of system information, it is critical that agencies thoroughly test a system's access controls prior to deployment to verify that users can only access the information necessary to fulfill their job responsibilities. However, we found that GSA's testing of HR Links did not identify system security weaknesses that resulted in sensitive information exposures and inappropriate access.

Exposure of sensitive information. As described below, GSA's HR Links testing failed to identify access control deficiencies that resulted in the exposure of sensitive information, such as PII and employment-sensitive information, for 92 users.

- *Help desk ticket exposure.* GSA's HR Links testing failed to identify misconfigured access controls that enabled a user to view other users' help desk tickets, as well as any sensitive information or attachments included with the tickets. As a result, HR Links exposed PII and employment-sensitive information for at least six individuals, including a birth certificate, college transcript, performance appraisal, and insurance application. HR Links testing did not verify that users were limited to viewing only their own help desk tickets. GSA determined that two individuals' PII was accessed in this incident.

- *Address change requests.* GSA's testing of access controls governing address change requests in HR Links was not comprehensive. When a user changes their home address

[1] The Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283, requires federal agencies to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency.

in HR Links, the system automatically sends a confirmation email. These emails include hyperlinks that, when opened, should take the user to their specific address change request in HR Links. GSA's testing verified that notification emails were sent to users as required, but failed to identify an access control weakness that enabled users to view all address change requests when opening the hyperlink. As a result, the names and home addresses for 68 employees were accessible to other employees through an address change self-service page. GSA determined that 19 individuals' PII was accessed in this incident.

- *Shared unique identifier.* GSA's testing was insufficient to ensure that each user was limited to accessing their own user account. In configuring the system, GSA did not use a unique identifier to create each employee's user account. Consequently, individuals who shared the same first and last name were not uniquely identified and signed into an account that was not their own. GSA did not detect this problem during testing, which resulted in the exposure of individuals' names, social security numbers, and home addresses. GSA determined that 18 individuals' PII was accessed in this incident.

On June 7, 2018, 3 days after HR Links' launch, we notified GSA's Chief Human Capital Officer and Chief Information Officer of the PII exposures in HR Links caused by the access control weaknesses identified above. In response, GSA corrected these issues. GSA also conducted a review of the 92 individuals whose sensitive information was exposed in HR Links. GSA determined that 39 individuals' PII was accessed and assessed the risk of harm to these individuals. GSA determined that 21 of the 39 individuals should receive notification of their PII's exposure. For the remaining 18 individuals, GSA contacted the employees who were incorrectly granted access to another employee's profile to determine if PII had been stored or disseminated. These individuals attested that they did not store or disseminate PII. GSA concluded that the risk of harm to the affected 18 individuals was low and that notification of their PII's exposure was not required, in accordance with the Office of Management and Budget's M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* and the *GSA Information Breach Notification Policy*.

Inappropriate information access. HR Links testing also failed to identify misconfigured user roles and data permissions for time administration and HR personnel. The misconfigured user roles and data permissions resulted in excessive or inadequate access to information and, in some cases, prevented these users from performing their work.

- *Time administration personnel access.* Time administration personnel enter, adjust, or approve time requests for a group or groups of employees who they are assigned to support. However, GSA did not limit time administration personnel's access to their assigned employees and failed to detect the misconfiguration during testing.

  After the HR Links launch, 35 help desk tickets were submitted reporting that time administration personnel were able to view and approve employee TA information and requests for employees they were not assigned to support. In some cases, these time administration personnel were granted inappropriate access to TA information and requests for all GSA employees. Conversely, 94 help desk tickets were submitted reporting that time administration personnel could not view and approve TA information and requests for the departments they supported.

- *Excessive access to HR transactions.* GSA officials did not configure data permissions to limit HR personnel's access to only those employees they support and did not detect the potential problems arising from this misconfiguration through system testing. As a result, some HR personnel were unintentionally given access to view and process all HR transactions in HR Links instead of only transactions for the employees they support. In one instance, an administrator denied an employee promotion transaction they should not have been able to access, which disrupted the promotion process.

Taken together, the deficiencies described above demonstrate that GSA's testing was insufficient to identify system security weaknesses, which resulted in exposures of sensitive user information and inappropriate access. GSA should ensure that system roles and data permissions are accurately defined and sufficiently tested in advance of future system deployments to properly control employees' access to information.

Deficiencies in Data Migration Led to Incomplete and Inaccurate Information

GSA's testing did not ensure that all necessary legacy system information was migrated in accordance with mandatory system requirements. GSA's transition to HR Links required the migration of employee data from the three legacy HR systems to HR Links. Accordingly, thorough testing of migrated information was required to verify that mandatory system requirements were met and reduce the risk of business disruptions. However, as described below, GSA's testing of HR Links failed to identify missing and inaccurate employee data migrated from legacy systems.

- *Missing supervisor of record*. In HR Links, every position must contain a supervisor of record to enable the system to route HR and TA requests properly. However, GSA migrated incomplete supervisor of record information from legacy HR systems to HR Links; therefore, 517 employees were unable to route their HR and TA requests. Although similar problems were encountered during testing, GSA did not take corrective action to ensure that all employee positions identified a supervisor of record prior to the deployment of HR Links.

- *Invalid department identification (ID)*. HR Links uses department IDs to assign data permissions to groups of employees in an office or organization. An employee must be assigned to a department ID in HR Links or they will not be visible within the system to other appropriate users, including time administration and HR personnel, and will have limited use of the system. However, GSA's testing did not verify that all employees were assigned to a valid department ID. As a result, some employees were not visible to other appropriate users and were unable to access any HR or TA functions because they were not assigned to a valid HR Links department ID. GSA officials stated that they were unable to provide the number of employees affected by this issue.

- *Incorrect accounting group*. In HR Links, some employees must be assigned to an accounting group that enables them to select specific labor codes for their timesheet. These labor codes allow employees to charge their time to various job duties, such as managing regional operations or legislative affairs. When GSA deployed HR Links, 170 employees were assigned to the wrong accounting group. Some of these employees were inappropriately required to select labor codes; others were unable to select their correct labor codes. When these employees attempted to submit their timesheets in HR Links, the system rejected their timesheets because they did not contain the expected labor codes.

  During testing, GSA did not verify that all employees were assigned to the correct accounting group and did not detect this problem before system deployment. According to GSA officials, this problem was caused by GSA developing incorrect instructions for assigning employees to accounting groups. GSA corrected this issue by updating the instructions and reassigning the affected employees to the correct accounting groups.

GSA's HR Links testing failed to identify missing and inaccurate employee data migrated from legacy HR systems. GSA officials informed us that they were aware that the data in legacy systems was imperfect, and the project could have benefitted from additional efforts to prepare the data for migration. Ultimately, GSA chose to migrate data from the legacy systems and fix issues as they arose after deploying HR Links. Although GSA has since addressed these data integrity issues, GSA should apply the lessons learned to future system deployments.

Functional Deficiencies

HR Links' testing failed to identify deficiencies in system functionality. Thorough functional testing verifies that the system meets user expectations, satisfies GSA business requirements, and reduces the risk of business disruptions during the system transition. However, as described below, we identified misconfigurations and functional limitations that caused errors in processing timesheets, automated approval of HR transactions, supervisory functions, and system-generated emails.

- *Timesheet processing*. Although GSA tested employee timesheet submission functionality, GSA officials stated that a business rule that validates employee leave balances was not properly configured. The misconfigured business rule did not compare the amount of leave requested against the employee's leave balance, causing many timesheets to generate error messages for employees with sufficient leave.

- *Automated approval of HR transactions*. GSA was unable to automate the end-to-end approval of HR transactions, such as employee promotions, within HR Links. GSA was unable to configure HR Links to route transactions to the appropriate HR personnel because it was unclear how approval responsibilities for HR user roles would transfer from legacy HR systems. Ultimately, GSA chose to abandon this HR Links functionality and conduct most of the approval process for personnel transactions outside of HR Links.

- *Supervisory functions*. HR Links did not satisfy GSA's mandatory system requirements in three supervisory functions:

    1. Supervisors were only able to delegate all of their employees or none of their employees to an alternate supervisor;
    2. Neither higher-level supervisors nor administrators were able to approve employee requests on behalf of supervisors who were unavailable; and
    3. Supervisors with employees detailed to their team were unable to manage their temporary employees' performance appraisals in HR Links.

    GSA officials stated that HR Links was unable to support the existing GSA business process without enhancements to the existing design. In November 2018, GSA deployed functionality in HR Links that fully resolved the above limitations. Tests related to this functionality appear to have failed during system testing, but deficiencies were not corrected prior to deployment.

- *System-generated emails*. The launch of HR Links experienced three email functionality issues that did not meet mandatory system requirements:

    1. GSA's email servers rejected HR Links notification emails or incorrectly categorized the notification emails as spam. HR Links generates notification emails that inform personnel that they have pending HR and TA requests requiring their approval. GSA email servers were not configured to properly route HR Links notification emails;
    2. Users were unable to view their TA requests because hyperlinks embedded in notification emails directed users to invalid webpages; and
    3. A misconfiguration caused employees to receive email notifications that stated their timesheet had been modified for "%5" instead of a valid pay period.

GSA could have detected the functionality deficiencies identified above through more robust testing. While GSA has either corrected the deficiencies or elected to move away from certain functionality, it should assess the limitations in its testing that failed to detect these errors to improve future system deployments.

In sum, GSA's HR Links testing was inadequate to meet its stated purpose of "validating business requirements and confirming business readiness." GSA's testing did not identify inaccuracies in employee data or functional deficiencies. In addition, GSA failed to address problems identified during testing prior to launching HR Links. While these problems did not have a catastrophic effect on HR Links, they resulted in exposures of sensitive information, incomplete and inaccurate information, and functional deficiencies.

Testing Challenges

During our audit, HR Links technical specialists and program management officials identified a number of challenges that contributed to GSA's inadequate testing. For example, the HR Links test plan called for the use of live employee data to test HR Links' interfaces with other GSA systems. However, live data was not available until after the completion of interface testing. GSA required an authorization to operate (ATO) for HR Links to exchange live data, but the ATO for HR Links came later than anticipated due to a lengthy security assessment process.[2] In one situation we identified, GSA chose to move forward with testing by using data that had employee PII removed because HR Links had not yet received an ATO. The lack of live data during interface testing likely limited GSA's ability to verify the accuracy of employee information migrated from legacy HR systems to HR Links.

The delay in the HR Links ATO also added challenges to the HR Links deployment. HR Links technical specialists stated that the deployment was completed under a compressed schedule due to the delayed ATO. Rather than complete test phases sequentially, in accordance with the HR Links test plan, technical specialists stated that test phases were overlapped to accommodate the compressed schedule. Technical specialists also asserted that the project would have benefited from gaps between the different test phases and extra time to conduct a thorough quality assurance process. HR Links program management officials stated that additional delays to the launch of HR Links would have resulted in additional cost, and that all HR Links tests were completed prior to deployment.

GSA should assess these challenges, along with our report finding, to identify opportunities for improvement in future system deployments. In particular, GSA should focus on enhancements to system testing to ensure that future system deployments are not adversely affected by system security weaknesses, incomplete and inaccurate data migration, and deficiencies in functionality encountered during the HR Links deployment.

[2] National Institute of Standards and Technology Special Publication 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*, requires federal information systems to undergo a security assessment and authorization process. An ATO is the successful end result of this process.

Conclusion

GSA did not sufficiently manage risks associated with migrating its legacy HR systems to HR Links. We found that GSA did not adequately test HR Links or fully address problems identified during system testing. As a result, HR Links had a series of significant system weaknesses upon deployment. These weaknesses caused the exposure of sensitive information (including PII), incomplete and inaccurate employee information, and functional deficiencies.

Although GSA has addressed these deficiencies, it should apply lessons learned from the HR Links deployment to ensure that appropriate testing is conducted to identify and mitigate risks for future system deployments, including GSA's government-wide payroll system, NewPay.

Recommendation

We recommend that GSA's Chief Human Capital Officer and Chief Information Officer, prior to the deployment of future systems, design and implement appropriate system testing to ensure that:

a. Required system security controls, including those governing user roles and data permissions, are operating effectively;
b. Data is complete and accurately migrated from legacy systems, if applicable; and
c. System testing verifies that all functional requirements are met.

GSA Comments

The GSA Chief Human Capital Officer and Chief Information Officer agreed with our finding and recommendation. GSA's response is included in its entirety in ***Appendix B*** – GSA Comments.

OIG Response

In its response to our draft report, GSA provided a technical comment related to the number of individuals notified of the PII exposure. GSA identified a transcription error in the data it provided during the audit and provided clarifying documentation. We have updated the report to reflect the additional information GSA provided.

Audit Team

This audit 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
Robert B. Fleming	Audit Manager
James N. Shreve	Auditor-In-Charge
Victor R. Pimentel	IT Specialist
Carla J. Humphrey	Management Analyst

Appendix A – Scope and Methodology

To evaluate the HR Links migration, we analyzed a number of information security incidents that occurred after the system launched. Our analysis covered the time period between November 2016 and February 2019.

To accomplish our objective, we:

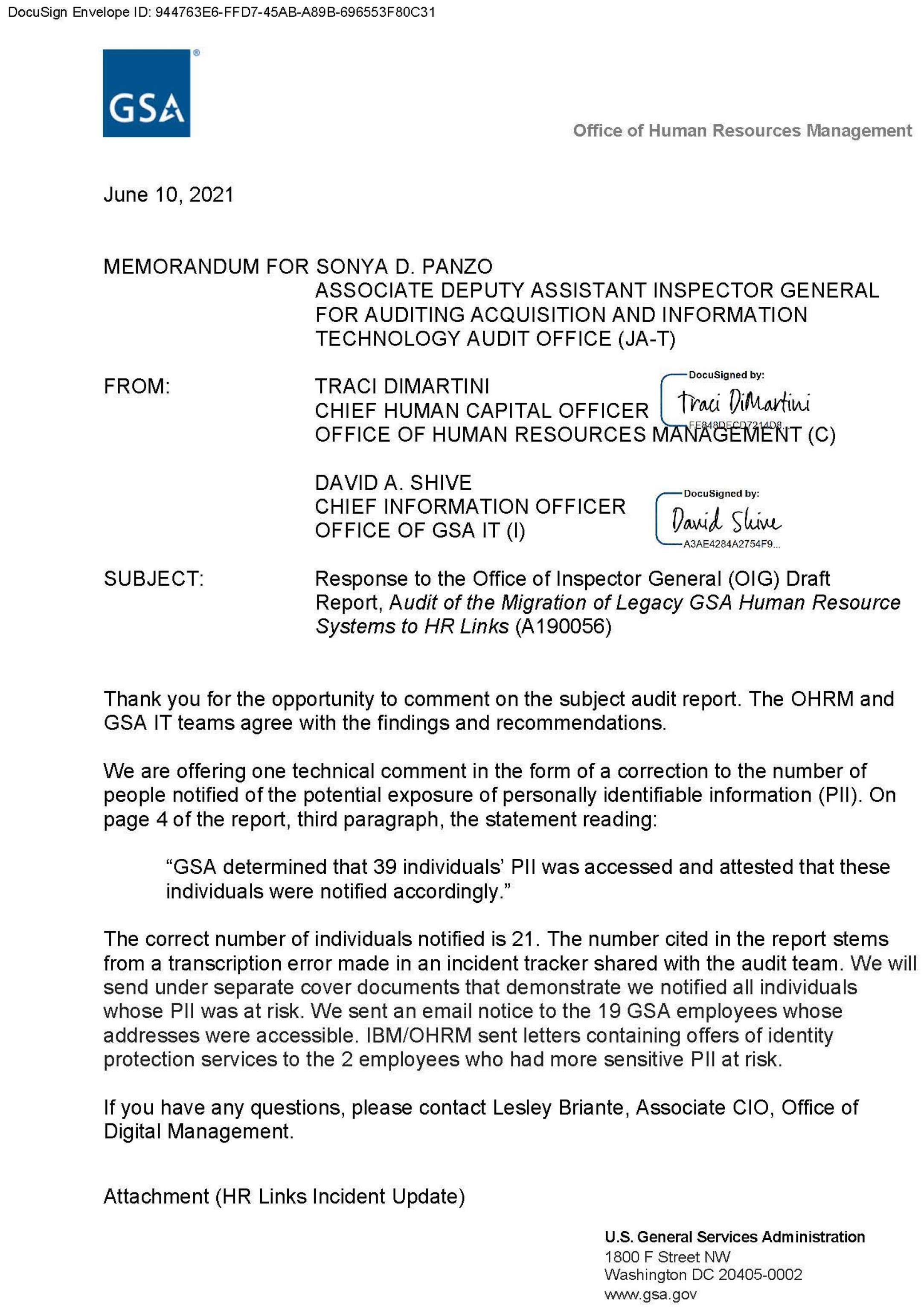
- Reviewed HR Links' system security and functional documentation;
- Reviewed the HR Links contract, system design documents, test plans and results, and actions taken to resolve HR Links issues;
- Gathered evidence related to HR Links' system security incidents;
- Reviewed 1,899 help desk tickets submitted in the 2 weeks after HR Links was launched on June 4, 2018;
- Evaluated HR Links system updates made in 2018 and how they affected HR Links system operation;
- Analyzed GSA's information technology security policy and federal information system standards; and
- Interviewed GSA and IBM personnel.

We conducted the audit between February 2019 and November 2020 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 finding and conclusions based on our audit objective.

Internal Controls

Our assessment of internal controls was limited to those necessary to address the objective of the audit.

Appendix B – GSA Comments



DocuSign Envelope ID: 944763E6-FFD7-45AB-A89B-696553F80C31

Office of Human Resources Management

June 10, 2021

MEMORANDUM FOR SONYA D. PANZO
ASSOCIATE DEPUTY ASSISTANT INSPECTOR GENERAL
FOR AUDITING ACQUISITION AND INFORMATION
TECHNOLOGY AUDIT OFFICE (JA-T)

FROM: TRACI DIMARTINI
CHIEF HUMAN CAPITAL OFFICER
OFFICE OF HUMAN RESOURCES MANAGEMENT (C)

DocuSigned by:
Traci DiMartini
FE848DECD7214D8...

DAVID A. SHIVE
CHIEF INFORMATION OFFICER
OFFICE OF GSA IT (I)

DocuSigned by:
David Shive
A3AE4284A2754F9...

SUBJECT: Response to the Office of Inspector General (OIG) Draft Report, *Audit of the Migration of Legacy GSA Human Resource Systems to HR Links* (A190056)

Thank you for the opportunity to comment on the subject audit report. The OHRM and GSA IT teams agree with the findings and recommendations.

We are offering one technical comment in the form of a correction to the number of people notified of the potential exposure of personally identifiable information (PII). On page 4 of the report, third paragraph, the statement reading:

> “GSA determined that 39 individuals’ PII was accessed and attested that these individuals were notified accordingly.”

The correct number of individuals notified is 21. The number cited in the report stems from a transcription error made in an incident tracker shared with the audit team. We will send under separate cover documents that demonstrate we notified all individuals whose PII was at risk. We sent an email notice to the 19 GSA employees whose addresses were accessible. IBM/OHRM sent letters containing offers of identity protection services to the 2 employees who had more sensitive PII at risk.

If you have any questions, please contact Lesley Briante, Associate CIO, Office of Digital Management.

Attachment (HR Links Incident Update)

U.S. General Services Administration
1800 F Street NW
Washington DC 20405-0002
www.gsa.gov

Appendix C – Report Distribution

GSA Administrator (A)

GSA Deputy Administrator (AD)

Chief Human Capital Officer (C)

Chief of Staff (C)

Deputy Chief Human Capital Officer (CS)

Director of Human Resources (CR)

Chief Information Officer (I)

Chief of Staff (I)

Deputy Chief Information Officer (ID)

Associate Chief Information Officer for Enterprise Planning and Governance (IDR)

Chief Information Security Officer (IS)

Chief Financial Officer (B)

Office of Audit Management and Accountability (BA)

Assistant Inspector General for Auditing (JA)

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