Office of Inspector General | United States Postal Service

Management Alert

Protection of Personally Identifiable Information on Internal Systems

Report Number 21-034-R21 | April 1, 2021

Table of Contents

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

April 1, 2021

MEMORANDUM FOR: SIMON M. STOREY
VICE PRESIDENT, HUMAN RESOURCES

JENNIFER D. UTTERBACK
VICE PRESIDENT, ORGANIZATION DEVELOPMENT

JANINE CASTORINA
CHIEF PRIVACY & RECORDS OFFICER

for

FROM: Jason M. Yovich
Deputy Assistant Inspector General for Supply Management and Human Resources

SUBJECT: Management Alert – Protection of Personally Identifiable Information on Internal Systems (Report Number 21-034-R21)

This management alert presents issues identified in the Protection of Personally Identifiable Information on Internal Systems. These issues came to our attention during our ongoing audit of Peak Season Hiring (Project Number 20-316). The objective of this management alert is to provide U.S. Postal Service officials notification of these issues which require immediate attention and remediation.

We identified these issues while conducting our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient evidence to provide a reasonable basis for our finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on our audit objective.

We appreciate the cooperation and courtesies provided by your staff. If you have questions or need additional information, please contact John E. Cihota, Director, Human Resources and Support, or me at 703-248-2100.

Attachment

cc: Postmaster General
Vice President, Chief Information Security Officer
Corporate Audit Response Management

Results

Introduction

During the Peak Season Hiring audit (Project Number 20-316), we found that the U.S. Postal Service mishandled personally identifiable information (PII) for veteran employees on an internal system. The purpose of this management alert is to bring these issues to management's attention and make recommendations for corrective action.

PII is any information about an individual maintained by an agency, including information that can be used to distinguish or trace an individual's identity. The Postal Service is responsible for safeguarding PII for over 630,000 employees nationwide. Management is responsible for ensuring employees safeguard PII through restricting employee access and using the required storing and handling methods to protect sensitive information.

On October 21, 2020, two computer-generated files containing PII were uploaded to the Postal Service's internal website. Specifically, the files included the names, home addresses, employee identification numbers, and work locations of 89,070 Postal Service veterans. The first file contained information for headquarters veterans and the second file included information for area and district veterans.

The Postal Service created the files to aid in identifying employees for recognition on Veterans Day 2020. Sharing the files on the internal website allowed district Human Resources (HR) representatives, veteran coordinators, and Postal Service Learning Development and Diversity[1] managers to access the data for veteran employees. Both files were accessible to over 380,000 employees and contractors with access to the internal website.

On October 22, 2020, we discovered and accessed the unsecured files on the internal website and notified the Postal Service on October 23, 2020. Subsequently, the Postal Service Chief Privacy and Records Officer (Privacy Officer) coordinated with the Corporate Information Security Office (CISO) to identify and remove the PII files from the internal website on October 23, 2020.

Conclusion

Opportunities exist for the Postal Service to improve the handling and safeguarding of PII when posting on an internal website. Management approved and an employee posted the unsecured files containing the PII of 89,070 veterans to the organization's internal website without reviewing the files to ensure they were encrypted or password protected to prevent unauthorized access.

After our notification and the Postal Service's removal of the files from the internal website, the CISO determined that the data were only posted internally; however, they were unable to verify whether the files were shared outside of the Postal Service. Because the data did not contain social security information, management determined that the severity of this PII incident was a low risk and [redacted]. However, the Postal Service took 71 days to notify affected veterans of the exposure of their PII. Postal Service policy does not clearly define the t[redacted] when the release of PII has occurred.

We also determined the employee who posted the veterans' PII to the internal website completed the required cybersecurity training courses. However, the employee did not apply the training by reviewing the two files to ensure they did not contain PII prior to posting on the internal website.

The Postal Service maintains extensive data on employees for business purposes. The organization has a responsibility to protect sensitive information from loss, misuse, and unauthorized access within and outside of its organization. Incidents involving PII can cause financial harm to an individual and may lead to identity theft or other fraudulent use of the information. Additionally, when an organization does not protect its employees from security incidents, it can experience a loss of public trust, legal liability, or remediation costs. We identified $1,431,938 in associated costs[2] that can be attributed to the vulnerability of inappropriate or unauthorized disclosure of sensitive data.

1 Supports, develops, and helps Postal Service human resources reach their full potential, positioning the organization to achieve organizational continuous improvement.
2 Associated cost is other impact categorized as IT security. IT security is computer software, networks, and data that are vulnerable or at risk of loss because of fraud, inappropriate or unauthorized disclosure of sensitive data, or disruption of critical Postal Service operations and services.

Management Oversight

Postal Service management did not provide adequate oversight to safeguard and protect sensitive information for 89,070 Postal Service veterans. Management stated that they did not review the data files containing the PII prior to posting the files on the internal website to ensure files were password protected or encrypted. Rather, they relied on the employee to securely post the files to the internal website.

Postal Service policy[3] outlines that all managers and supervisors, regardless of functional area, are responsible for implementing information security policies. All managers must ensure compliance with information security policies by organizations and information resources under their direction and provide the personnel, financial, and physical resources required to appropriately protect information resources.

According to policy, all personnel must implement the protection requirements when handling sensitive information.[4] Additionally, the policy[5] requires that managers ensure employees do not store sensitive information on their computers without written permission from the manager. If permission is granted, managers must ensure that the employee is aware of their responsibility to safeguard the data through encryption and the potential employee personal liability should the data be compromised. Further, the managers responsible for those files must approve all access to existing employee and customer files.

After our notification and the Postal Service's removal of the files from the internal website, the Postal Service took swift action to address the incident. The Postal Service's Privacy and Records Management Office activated the *Response Plan for Information Breaches Involving Personal Information* (response plan)[6] and, in doing so, coordinated with the CISO to investigate the incident and provide instructions to HR on corrective actions. The Privacy Officer, in coordination with the CISO, assigned the PII incident as low risk because the data elements disclosed were considered minimal, which generally would not allow for misuse.[7] Additionally, the Postal Service determined the incident was internal and did not constitute an external breach, requiring further remediation by the CISO. The Postal Service's initial risk assessment was consistent with guidance provided in the response plan.

To address the security incident, the Postal Service:

- Activated the response plan and initiated an internal investigation.
- Issued a standard operating procedure for PII, which includes instructions for requesting and handling veterans' data containing PII for internal and external use. Management issued the document to the headquarters' Diversity and Talent Acquisition team,[8] which handled this information.
- Recommended cybersecurity training for all HR employees specifically related to PII. This training is currently being developed.

The Postal Service estimated that 176[9] employees had been provided a link to or accessed one or both data files. However, based on our analysis, we determined that 373 HR employees were provided a direct link to the veterans PII data uploaded on the internal website October 21, 2020. These 373 employees were authorized to have access to the file. The Postal Service conducted a systems data scan to determine if the files were viewed or downloaded by those not authorized to view or access the files. The Postal Service determined that 75

3 Handbook AS-805, *Information Security*, Section 2-1, dated November 2019.
4 Handbook AS-805, Section 3-1. These requirements include the protection of sensitive information in transit and in storage.
5 The Postmaster General's letter to all employees - *Securing Sensitive Business and Personal Information*, dated January 2007.
6 This plan, dated February 19, 2016, describes the Postal Service's Privacy and Records Management Office's roles and responsibilities, along with its response plan with regard to actual or suspected information security data breaches. The Privacy and Records Management Office works cooperatively with other internal stakeholders within the Law Department, and with CISO, the Inspection Service, and the Office of the Treasurer, as needed, to assure that data breach incidents are properly addressed and to ensure that appropriate actions to mitigate risk are carried out. Additionally, remedial actions may be taken to prevent future occurrences of a reported data breach incident.
7 These incidents are categorized on a case-by-case basis for severity and associated response times. The severity of the incident will determine the appropriate notification process. A severity level 4 was categorized for this incident, which was identified as low or no impact.
8 A division of HR which recruits, engages, and retains diverse talent to build and sustain the workforce of the present and future.
9 The Postal Service provided an initial list of 182 individuals that downloaded PII files. Six of the 182 were identified as duplicates.

employees with ACE login accounts[10] accessed the files on the internal website; however, they were unable to verify whether the files were shared externally.

Recommendation #1

We recommend the **Vice President, Human Resources**, reiterate policies and procedures to all Human Resources managers and employees with access to personally identifiable information (PII) to protect and safeguard PII from unauthorized access.

Employee Notifications

The Postal Service did not inform all 89,070 veterans until 71 days[11] after the incident. Management knew immediately who was affected by this incident and had determined that it was necessary to notify the employees.

[redacted] are outlined in both the Privacy Office's response plan and CISO's *Cybersecurity Incident Response Plan* (CSIRP).[12] Although Postal Service officials informed us that the Privacy Office's policy [redacted]

[redacted]

[redacted]

These guidelines also note [redacted].[14] The policy also notes that the [redacted]

Similarly, the CSIRP states the Postal Service is required to notify affected persons and relevant parties, including regulatory agencies, governmental agencies, and law enforcement, as required.[16] Further the Postal Service is required to identify the affected population across the states or geographical regions in which the affected persons are located and follow relevant notification statutes.[17]

However, neither policy clearly defined the [redacted] for [redacted] based on the severity level. We recognize that every cybersecurity incident is different, but [redacted] would help management effectively handle the incident response.

State laws have been enacted to define [redacted] affected individuals of unauthorized access and/or acquisition of their unencrypted or unsecured personal information. While many states, [redacted], require [redacted]

10 Provides access to the Postal Service infrastructure, its resources, and/or applications (Advanced Computing Environment). Once approval is granted, the individual is given a unique logon ID and password.
11 The Postal Service uploaded the files of veterans' PII to the internal website on October 21, 2020, and alerted veterans of the incident on December 31, 2020.
12 This plan, [redacted]
13 [redacted]
14 [redacted]
15 [redacted]
16 *Cybersecurity Incident Response Plan*, Section 5.1.
17 *Cybersecurity Incident Response Plan*, Section 7.8.3.

[redacted]

The 89,070 affected veterans reside in every state of the country. Although the Postal Service does not have to follow state laws, we believe this information could serve as a guide for the Postal Service to follow when determining [redacted] to help affected Postal Service employees reduce the risk of financial harm. At a minimum, clarification as to where to obtain [redacted] would assist those implementing the response plan understand their [redacted] responsibilities. Without [redacted] of PII exposure, Postal Service veterans were at an increased risk of financial harm, identity theft, or other malicious activity.

Recommendation #2

We recommend the **Chief Privacy & Records Management Officer**, in coordination with the **Vice President, Chief Information Security Officer**, as applicable, develop [redacted] affected by cybersecurity incidents and ensure both the Privacy & Records Management Office's *Response Plan for Information Breaches Involving Personal Information* and Corporate Information Security Office's *Cybersecurity Incident Response Plan* are updated accordingly.

Training

We found that Postal Service HR employees with access to the unsecured files generally complied with cybersecurity training requirements. Additionally, we reviewed the mandatory Postal Service cybersecurity training provided to employees and determined that courses developed contained the guidance necessary to help prevent this PII incident. As part of the Postal Service's information security program, policy requires that all officers, managers, and supervisors ensure personnel receive annual information security training.[18] This annual training provides cybersecurity awareness and procedures for handling, protecting, and sharing sensitive information.

We reviewed training records for 176[19] employees identified as having access to the unsecured files containing PII. Upon reviewing fiscal year 2020 cybersecurity training records for those employees, we found that 171 of the 176 (97.2 percent) completed the required two courses for cybersecurity training. For the remaining five employees (2.8 percent),[20] we noted:

- One of the five employees did not complete the Cybersafe Fundamentals for Employees course, which discusses protecting Postal Service equipment and data.
- All five employees did not complete the Cybersafe Data Protection for Employees course. This training describes sensitive and non-sensitive information, procedures for protecting critical digital and hard copy data, how to handle sensitive information, and procedures for sharing and disposing of sensitive and sensitive enhanced information.

We determined the employee who posted veterans' PII to the internal website completed both required cybersecurity training courses in August and September 2020. However, the employee did not apply that knowledge by reviewing the two files to ensure they did not contain PII prior to posting on the internal website. In response to the security incident and because of our audit, the employee re-took the Cybersafe Data Protection for Employees course.

While this incident occurred internally, opportunities exist for the Postal Service to communicate to key personnel the importance of handling, protecting, and sharing sensitive information.

Recommendation #3

We recommend the **Vice President, Organization Development**, verify employees with access to personally identifiable or sensitive information complete mandatory cybersecurity training courses.

18 Handbook AS-805, Section 2-2.5.

19 For our training analysis, we judgmentally selected 176 Postal Service HR employees based on the fact that they were initially invited to the planning meeting to celebrate veterans. These employees were provided the location of the files containing veterans PII on the internal website. During the audit, we identified 197 additional HR managers (373 total) that were provided the link to the veterans' files on October 22, 2020. Because the link to the internal website was taken down on October 23, 2020, one day later, we did not review these additional 197 HR managers' training records.

20 One employee was required to take both training courses.

Management's Comments

Management generally agreed with all the recommendations in this report.

Regarding recommendation 1, management stated that they are currently in compliance with the reiteration of policies and procedures to all HR managers and employees with access to PII. Management also stated that information security policies and procedures are reiterated yearly, through training and other methods. In subsequent correspondence, the Postal Service provided a memorandum issued March 30, 2021, to all HR regional and area directors and district managers to reiterate local HR responsibility for safeguarding PII.

Regarding recommendation 2, the CISO and Privacy Officer did not feel that [redacted] are appropriate as all investigations and/or incidents are different and [redacted]. These investigations/incidents could adversely affect ongoing analysis and create misinformation for parties involved. However, the Privacy Officer will provide [redacted] in an updated Privacy & Records Management Information Breach plan. These guidelines will reflect that notification will be required from the Privacy Officer to involved parties [redacted] after completing its investigation into the incident. Further, management stated that CISO would [redacted] from its processes, as prescriptions are made by the Privacy Officer. The target implementation date is September 30, 2021.

Regarding recommendation 3, management stated that any user that has access to sensitive or sensitive enhanced systems, is automatically assigned the Cybersecurity 201 Data Protection. Employees who do not complete the required training are placed in a limited system access state. In subsequent correspondence, management provided documentation confirming that four of five employees completed the training. For the remaining employee who has not yet completed the training, the Postal Service placed the employee's system access account in a suspended status as of February 5, 2021.

Management also noted that the incident did not occur during our ongoing Peak Season Hiring audit (Project Number 20-316). Rather, they cited that this incident was identified when an HR individual provided the link to an OIG employee working with HR on recognizing Postal Service veterans.

See Appendix A for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report. Regarding identification of the incident, we acknowledge that an OIG HR employee, who had a business need to view the files, initially identified this issue. However, our Peak Season audit team, who did not have a business need to view the unprotected files, independently and without knowledge of the OIG HR employee's identification found the files while searching the Postal Service intranet in support of the Peak Season audit.

All recommendations require OIG concurrence before closure. The OIG requests written confirmation when corrective actions are completed. Recommendation 2 should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed. We consider recommendations 1 and 3 closed with the issuance of this report.

Appendix A: Management's Comments

UNITED STATES POSTAL SERVICE

March 18, 2021

JOSEPH WOLSKI
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Management Alert – Protection of Veterans' Personally Identifiable Information on Internal Systems (Project Number 21-034-DRAFT)

Thank you for the opportunity to review and comment on the above referenced audit. The Postal Service either already has or will implemented two of the recommendations resulting from this audit, and partially agrees to implement the third. However, as more fully set forth below, the Postal Service wanted to clarify the factual circumstances that led to this audit.

Specifically, the Postal Service acknowledges that a spreadsheet containing names and addresses of veteran employees that was posted on the Postal Service's internal website Blue. The link to this spreadsheet was sent to employees who were authorized to use this information. However, due to location, the information was accessible to more than those with a need to know and the information was not properly secured. Once it was brought to management's attention, the information was removed from the website immediately and extensive efforts were made to eliminate any copies. Fortunately, neither the OIG nor the Postal Service found any evidence the information was transmitted outside the Postal Service.

However, contrary to what is noted in the audit, the incident did not occur during the Peak Season Hiring audit (Project Number 20-316). Instead, a Human Resources individual, while engaging coordinators to properly recognize Postal Service veterans, including the coordinator working for OIG, provided the link to the veterans' information on Blue to OIG personnel. That individual provided the link to ensure that all OIG personnel were properly recognized. After distributing that link, on October 23, 2020, OIG personnel raised the existence of the veterans file on the Blue page with superiors. Those superiors raised the issue with the Chief Privacy Officer of the Postal Service, who after a brief review of the document and location, determined that the document must be removed.

Therefore, while it acknowledges the mistake made by one of its Human Resources employees in this case, the Postal Service believes it already has a strong program in place to protect personally identifiable information. That is evidenced by its prompt response to the situation that led to this audit, as well as the fact that it is already in compliance with two of the three recommendations below.

475 L'Enfant Plaza SW
Washington DC 20260-4201

Recommendation #1: We recommend the **Vice President, Human Resources,** reiterate policies and procedures to all Human Resources managers and employees with access to personally identifiable information (PII) to protect and safeguard PII from unauthorized access.

Management Response/Action Plan:

Management agrees with this recommendation and is already in compliance with it. Information security policies and procedures are reiterated on a yearly basis, through training and other methods.

Recommendation #2: We recommend the **Vice President, Chief Information Security Officer (CISO),** in coordination with the **Chief Privacy & Records Management Officer (CPO),** update the Cybersecurity Incident Response Plan with [redacted] affected by cybersecurity incidents.

Management Response/Action Plan:

Management partially agrees with this recommendation. While the CISO and CPO do not feel [redacted] are appropriate as all investigations/incidents are different and [redacted] could adversely affect ongoing analysis and create misinformation for parties involved, the CPO will provide [redacted] in an updated Privacy & Records Management information breach plan. These guidelines will reflect that the CPO will require that notification be made to involved parties [redacted] after completing its investigation into the incident. CISO will [redacted] from its processes, as prescriptions are made by CPO.

Target Implementation Date:
September 30, 2021

Responsible Official:
Chief Privacy Officer and VP, Chief Information Security Officer (CISO)

Recommendation #3: We recommend the **Vice President, Organization Development** verify employees with access to personally identifiable or sensitive information complete mandatory cybersecurity training courses.

Management Response/Action Plan:

Management agrees with this recommendation, and believes it is already in compliance with it. Any user that has access to sensitive or sensitive enhanced systems, is automatically assigned the Cybersecurity 201 Data Protection Employees who do not complete the required training are placed in a limited ACE system access state.

Simon Storey
Simon Storey
Vice President, Human Resources

Janine Castorina
Digitally signed by Janine Castorina
Date: 2021.03.18 12:37:19 -04'00'
Janine Castorina
Chief Privacy & Records Officer

Jennifer D Utterback
Jenny D. Utterback
Vice President, Organization Development

cc: VP, Chief Information Security Officer, (CISO)
Mgr. Corporate Audit and Response

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100