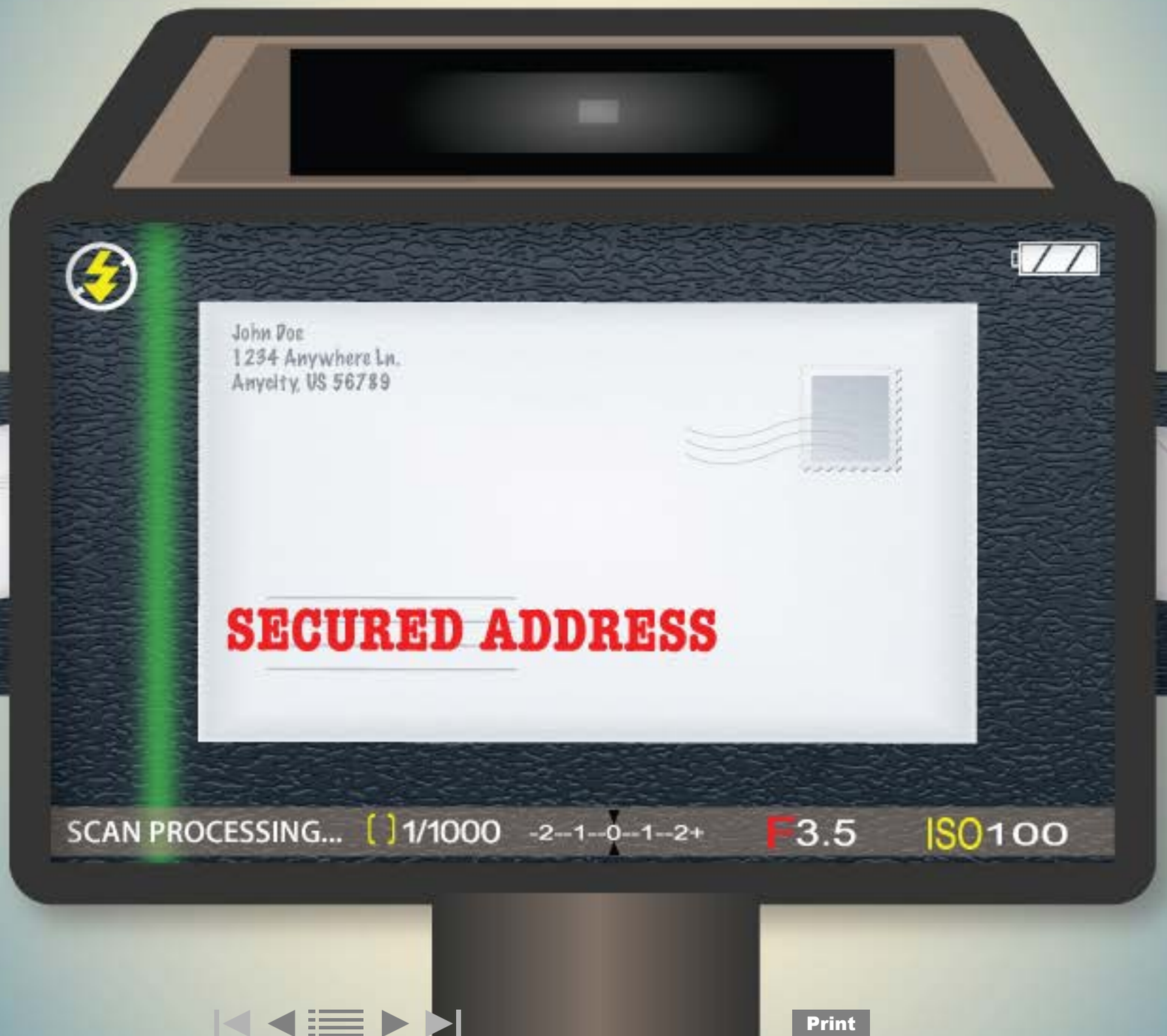
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Access Controls Over Mail Imaging Systems

Audit Report

Report Number
IT-AR-16-004

January 14, 2016



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

We found no issues with the established practice of mail image retention; however, management could improve access controls over systems that store mail images to ensure unauthorized users cannot access the images or other parts of the Postal Service network.

Background

The U.S. Postal Service has over 270 mail processing centers across the nation with more than 6,600 pieces of mail processing equipment that capture mailpiece images. The mail processing equipment maintains these images for between 4 seconds and 120 days depending on the type of processing equipment. These images enable the tracking of mailpieces from receipt to delivery.

The Postal Service has different types of facilities that process mail, such as the Merrifield, VA, Processing and Distribution Center. When mail processing machines are unable to read addresses on mailpieces, their images are forwarded to the Remote Encoding Center (REC) in Salt Lake City, UT.

The Postal Service uses one set of security standards for its administrative network, Handbook AS-805, *Information Security* (AS-805), and another for account management and password controls governing the mail processing infrastructure network, Handbook AS-805-G, *Information Security for Mail Processing/ Mail Handling Equipment* (AS-805-G).

Our objective was to determine the effectiveness of access controls over mail imaging systems.

What The OIG Found

We found no issues with the established practice of mail image retention; however, management could improve access controls over systems that store mail images to ensure unauthorized users cannot access the images or other parts of the Postal Service network.

Engineering Systems management said they used AS-805-G to determine account management and password configuration criteria; however, they should have used the stricter standards of AS-805 because the six mail imaging systems we tested are connected to both the mail processing infrastructure and administrative networks. We identified the following instances where AS-805 was not followed:

- Thirteen shared administrative accounts allowed multiple users to apply the same username and password to access three mail imaging systems.
- Eight active user accounts had administrative privileges on three systems that did not require passwords.
- Access to eight shared accounts with administrative privileges that had not been used in more than a year should have been terminated.

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

- Thirty-seven administrative accounts did not require password changes at least every 30 days and 11 non-administrative accounts did not require password changes at least every 90 days.
- Five active guest accounts were enabled without passwords.
- Engineering Systems and Corporate Information Security Office management did not conduct security documentatio updates, known as business impact assessments, for 11 mail imaging systems.

Finally, during our visit to the REC, we observed that a maintenance employee left a laminated note card with administrator and user login credentials in the REC server room that another employee could have used to access eight pieces of mail imaging equipment. The REC manager acted promptly to remove the visible password list and notified the staff of the importance of securing this type of information. As a result, we are not making a recommendation on this issue.

During the last 4 years, Engineering Systems and Corporate Information Security Office management have updated business impact assessments for sensitive mail imaging systems and have not finished updating the non-sensitive documentation. They have no date for completion.

Without proper security and access controls, the Postal Service is at risk of unauthorized access and theft of data, including mail images.

What The OIG Recommended

We recommended management, in accordance with Handbook AS-805, update account management, revise password settings for mail imaging systems, and establish a plan to ensure the required business impact assessments comply with Postal Service standards.

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

What the OIG Found

We identified the following instances where AS-805 was not followed:

Click On The Icons Below To Reveal Findings

13 shared administrative accounts allowed multiple users to apply the same username and password to access three mail imaging systems.

8 active user accounts had administrative privileges on three systems that did not require passwords.

8 shared accounts with administrative privileges that had not been used in more than a year should have been terminated.

37 administrative accounts did not require password changes at least every 30 days and 11 non-administrative accounts did not require password changes at least every 90 days.

5 active guest accounts were enabled without passwords.

11 mail imaging systems did not have security documentation updates, known as business impact assessments, conducted by the Engineering Systems and Corporate Information Security Office management.

Click Here to Reset.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 14, 2016

MEMORANDUM FOR: MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

GREGORY S. CRABB
ACTING CHIEF INFORMATION SECURITY OFFICER AND
DIGITAL SOLUTIONS VICE PRESIDENT

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskt

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – Access Controls Over Mail Imaging Systems
(Report Number IT-AR-16-004)

This report presents the results of our audit of the Access Controls over Mail Imaging Systems (Project Number 15TG026IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean Balduff, acting director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

The U.S. Postal Service has over 270 mail processing centers across the nation with more than 6,600 pieces of mail processing equipment that capture images of address information on mailpieces.

Introduction

This report presents the results of our self-initiated audit of the Access Controls over Mail Imaging Systems (Project Number 15TG026IT000). Our objective was to determine the effectiveness of access controls over mail imaging systems. See Appendix A for additional information about this audit.

The U.S. Postal Service has over 270 mail processing centers across the nation with more than 6,600 pieces of mail processing equipment that capture images of address information on mailpieces. The mail processing equipment maintains these mail images for between 4 seconds and 120 days depending on the type of processing equipment. These images are retained to enable the tracking of mailpieces from receipt to delivery.

The Postal Service has different types of facilities that process mail such as the Merrifield, A, Processing and Distribution Center (P&DC) and one Remote Encoding Center (REC) in Salt Lake City, UT. The Merrifield P&DC contains more than 40 pieces of mail processing equipment, similar to those used throughout the Postal Service. This equipment performs such functions as positioning mailpieces for scanning, reading addresses, and applying barcodes. Mailpieces are then moved to other equipment where they are sorted and packaged for transport to other facilities.

When mail processing machines are unable to read address information they forward images of the mailpieces to the REC. This center, which is the only one of its kind, has seven types of mail processing equipment used to read addresses.

We reviewed six mail imaging systems[1] that are connected to both the administrative network and the mail processing infrastructure (MPI) network. We also tested account management and password controls at the Merrifield, A, P&DC for two mail imaging systems that receive data from the following five types of mail processing equipment

- Delivery Barcode Sorter
- Delivery Barcode Sorter Input /Output Subsystem
- Combined Input /Output Subsystem
- Automated Package Processing System
- Automated Parcel Bundle Sorter

In addition, we tested account management and password controls at the REC for four mail imaging systems; however, we do not know how many employees have access to the images. Engineering Systems personnel stated that it would take them a minimum of 60 days to provide us with user information for all mail imaging systems nationwide (see Appendix B for details on the systems we tested).

1 We identified the six mail imaging systems for review based on our site visits and interviews with Posta Service Engineering Systems, Maintenance Technical Support Center, Network Operations, and In-Plant Support management. The systems are listing in Appendix B.

Due to RMN's reliance on MICS, the account management and password configuration issues for MICS also apply to RMN.

The Postal Service uses one set of security standards for its administrative network, Handbook AS-805, *Information Security*, and another for account management and password controls governing the MPI network, Handbook AS-805-G, *Information Security for Mail Processing/Mail Handling Equipment*. Engineering Systems leveraged Handbook AS-805-G guidance for mail processing equipment because the mail imaging systems are on the MPI network.

As part of our review, we looked at the Mail Image Controller Server (MICS), which provides mail images for the Postal Service's ongoing Real Mail Notification (RMN) pilot. This pilot provides customers who sign up for the service with a daily email that shows images of the mailpieces delivered to their mailboxes that day. Due to RMN's reliance on MICS, the account management and password configuration issues for MICS also apply to RMN.

Summary

We did not find issues with the established practice for retaining images of mailpieces; howeve , we determined the Postal Service could improve access controls over the mail images.

During the audit, the Engineering Systems Audit Response Coordination (ARC) liaison confirme that the mail imaging systems we tested have access to both the MPI and administrative networks. However, access controls protecting mail images did not comply with the stricter Handbook AS-805 information security requirements that govern the administrative network. Engineering Systems and Corporate Information Security Office (CISO) management also did not comply with information security requirements when updating security documentation, a process known as Business Impact Assessments (BIA),[2] for mail imaging systems as required by Handbook AS-805.

Finally, during our visit to the REC, we observed that a maintenance employee left their laminated note card with administrator and user login credentials in the REC server room where another employee could have used them to gain access to eight pieces of mail imaging equipment. The REC manager acted promptly to remove the visible password list and notified the sta f of the importance of securing this type of information. As a result, we are not making a recommendation on this issue.

Engineering Systems management said they used Handbook AS-805-G to determine account management and password configuration criteria. Howeve , the stricter standards of Handbook AS-805 apply because mail imaging systems are connected to both the MPI and administrative networks. As a result, Engineering Systems management did not follow Handbook AS-805's requirement to establish proper access controls for the six systems containing mail images and the password settings we reviewed.

According to Engineering Systems and the CISO, BIAs were not updated because the system security process changed in 2011, requiring mail imaging systems to have updated business impact assessments. During the last 4 years, Engineering Systems and CISO management have updated BIAs for sensitive mail imaging systems and have not finished updating the non-sensitive documentation. They have no date for completion.

Without proper security and access controls, the Postal Service is at risk for unauthorized access and theft of data, including mail images.

2 A BIA is a process for determining how to categorize Postal Service information resources. A BIA must be completed for all information resources, whether they are developed in house, outsourced, or hosted in non-Postal Service facilities.

Handbook AS-805-G allows for shared accounts with multiple users and limited password controls within the MPI network, under the condition its network does not connect to the administrative network.

Account Management

Handbook AS-805-G allows for shared accounts with multiple users and limited password controls within the MPI network, under the condition its network does not connect to the administrative network. However, the systems we tested were connected to the administrative network, which must be secured as directed by Handbook AS-805. Management did not properly control access to systems that contain mail images in accordance with Handbook AS-805 (see Table 1 for details). Specifically

- Engineering Systems did not properly manage shared administrative accounts. We identified 13 shared administrativ accounts that allow multiple users to apply the same username and password to access three of the mail imaging systems. Handbook AS-805 requires assigning individual users to administrative accounts.
- Engineering Systems enabled full access to systems without a password. We identified eight active user accounts wit administrative privileges on three systems that were not required to have passwords. Handbook AS-805[3] requires that these accounts use two-factor authentication.[4]
- Engineering Systems did not appropriately terminate administrative access to the mail imaging systems we reviewed. We identified eight shared accounts that were not assigned to individuals, granted administrative privileges, and had not been use in more than 365 days. Handbook AS-805[5] requires management to delete accounts not used in the last 365 days.
- Engineering Systems did not require account passwords to be changed in accordance with policy.[6] We identified 3 administrative accounts that did not change passwords at least every 30 days and 11 non-administrative accounts that did not change passwords at least every 90 days. Handbook AS-805 requires administrative passwords to be changed every 30 days and non-administrative passwords to be changed every 90 days.
- Engineering Systems did not delete or disable guest accounts.[7] We identified five active guest accounts that were enabl without passwords. Handbook AS-805[8] requires guest accounts to be deleted or disabled.

Table 1 shows the number of active accounts that do not comply with Handbook AS-805 policy.

3 Handbook AS-805, Section 9-7.2.2.
4 Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card, and the other is typically something memorized, such as a password.
5 Handbook AS-805, Section 9-5.5.
6 Handbook AS-805, Section 9-6.1.6.
7 A guest account provides access to the computer for any user who does not have a user account on the computer.
8 Handbook AS-805, Section 9-4.2.6.

The Engineering Systems ARC liaison stated that Handbook AS-805 does not apply to systems that are on the MPI network and that Handbook AS-805-G authorizes discretionary implementation of access controls, which limits individual accountability.

Table 1 – User Account Management

	Number of Accounts With Issues					
System	Shared Accounts With Administrative Privileges	Privileged Accounts Without a Password	Administrative Accounts Not Used in 365 Days	Administrative Passwords Not Changed Every 30 Days	Non-Administrative Passwords Not Changed Every 90 Days	Guest Accounts Not Disabled or Deleted
[redacted]	0	2	4	10	0	2
[redacted]	4	0	1	4	7	1
[redacted]	0	0	0	6	2	0
[redacted]	0	2	2	8	0	2
[redacted]	5	4	1	5	1	0
[redacted]	4	0	0	4	1	0
Total	**13**	**8**	**8**	**37**	**11**	**5**

Source: U.S. Postal Service Office of Inspector General (OIG) analysis.

Engineering Systems management agreed there was a lack of management oversight. In addition, the systems were configured for local authentication and installed with accounts created by a standard system configuration template used throughout the mail processing environment. The Engineering Systems ARC liaison stated that Handbook AS-805 does not apply to systems that are on the MPI network and that Handbook AS-805-G authorizes discretionary implementation of access controls, which limits individual accountability. However, Engineering Systems confirmed the mail imaging systems are connected to both the MPI and administrative networks. Therefore, they must comply with the information security policy in Handbook AS-805. By not properly controlling account management, the Postal Service exposes the mail imaging systems to potential data theft.

Password Configurations

According to Handbook AS-805-G, Engineering Systems determines the password settings for systems that cannot accommodate the password criteria defined in Handboo AS-805. However, both the manager, CISO, and the vice president, Engineering Systems, must review and approve these exceptions to Handbook AS-805 password criteria. Engineering Systems was unable to provide any documentation that such approval was given. Management did not properly configure password settings for six of the mail imaging systems, composed of 12 subsystems[9] that are connected to the administrative network in accordance with Handbook AS-805 (see Table 2 for details). Specificall , we identified the following

- Engineering Systems did not configure the systems to require the creation of passwords for four subsystems. It permitte minimum password lengths to be set to zero, so no passwords were required. Handbook AS-805[10] states that systems must deny access if a user does not have a password.

9 A subsystem is a group of interconnected and interactive parts that performs an important job or task as a component of a larger system.
10 Handbook AS-805, Section 9-6.1.12.

Both the manager, CISO, and the vice president, Engineering Systems, must review and approve exceptions to Handbook AS-805 password criteria.

- Engineering Systems did not configure 10 subsystems to follow the Handboo AS-805[11] requirement that systems require password changes every 90 days. Instead, it permitted users to keep the same passwords.

- Engineering Systems did not configure 10 subsystems to enable password complexit . The password complexity was set to a status of disabled, meaning that any password entered would be acceptable. Handbook AS-805[12] requires passwords to contain characters of various categories that create complexity, such as upper/lowercase characters, numbers, and special characters.

- Engineering Systems did not configure 1 subsystems to enforce the minimum password length. It only required minimum password lengths of zero to eight characters, while Handbook AS-805[13] states account passwords must be at least 15 characters.

- Engineering Systems did not configure nine subsystems to enforce the minimum number of reused passwords and had n limitation for repeated passwords. However, Handbook AS-805[14] states that passwords must not be repeated for at least five generations

According to the Engineering Systems ARC liaison, these issues occurred because Handbook AS-805-G allows for discretionary implementation of password configuration settings, which resulted in no security for eight administrator accounts used on three mail imaging systems. However, these systems are connected to both the MPI and administrative networks and, consequently, must meet the stricter password settings required by Handbook AS-805. Because Engineering did not use Handbook AS-805, these password settings were incorrectly set up in the program code[15] used on the six systems.

Table 2 details the password issues associated with systems tested during our audit.

11 Handbook AS-805, Section 9-6.1.12.
12 Handbook AS-805, Sections 9-6.1.12 and 9-6.1.
13 Handbook AS-805, Sections 9-6.1.12 and 9-6.1.1.
14 Handbook AS-805, Sections 9-6.1.12 and 9-6.1.
15 Program code is a set of computer instructions written in a programming language.

The BIAs for 11 systems, designated as non-sensitive, were last updated between 7 and 12 years ago instead of every 3 years.

Policy states that written passwords should be stored in a tamper-resistant manner.

Table 2 – System Password Settings

System	Number of Subsystems With Password Configuration Issues: Minimum Password Length is Zero; No Password Required	Password Not Changed After 90 Days	Password Complexity Disabled	Minimum Password Length Less Than 15 Characters	Password History Less Than Five Generations
[redacted]	0	2	2	2	2
[redacted]	1	1	1	1	1
[redacted]	3	4	4	4	3
[redacted]	0	2	2	2	2
[redacted]	0	1	1	1	1
[redacted]	0	0	0	1	0
Total	4	10	10	11	9

Source: OIG analysis.

Business Impact Assessments Need to be Updated

Engineering Systems and CISO management did not update BIAs as required.[16] The BIAs for 11 systems, designated as non-sensitive, were last updated between 7 and 12 years ago instead of every 3 years. According to Engineering Systems and the CISO, BIAs were not updated because the system security process changed in 2011, requiring mail imaging systems to have updated BIAs. During the last 4 years, Engineering Systems and CISO management have updated BIAs for sensitive mail imaging systems and have not finished updating the non-sensitive documentation. They have no date for completion. Because the BIAs have not been updated, system changes that affect the security of mail are not reviewed and updated regularly, which could lead to the exposure of customer information. See Appendix C for the list of the BIAs needing updates.

Visible Username and Passwords

Policy states that written passwords should be stored in a tamper-resistant manner.[17] However, a REC maintenance employee left his laminated note card with administrator and user login credentials in the REC server room where any of 35 managers and staff could have used them to gain access to eight pieces of mail imaging equipment.

The REC manager acted promptly when informed of the employee's negligence. Management removed all visible login credentials and reminded staff of the importance of securing user names and passwords. As a result, we are not making a recommendation on this issue.

16 Handbook AS-805-A, *Information Resource Certification and Accreditation Process*, Section 6-2, March 2015.
17 Handbook AS-805-C, *Information Security for General Users,* Section 2, November 2014.

Recommendations

We recommend the vice president, Engineering Systems, direct the manager, Engineering Software Management, and the manager, Technology Development and Applications, in accordance with Handbook AS-805, *Information Security,* policy for mail imaging systems connected to the administrative network, to:

1. Remove administrative privileges for shared accounts on all mail imaging systems.

2. Require passwords for all mail imaging systems accounts in accordance with Handbook AS-805.

3. Delete all accounts that have not been used in more than 365 days and all guest accounts on the mail imaging systems.

4. Require users to change passwords for all administrative accounts at least every 30 days and for all non-administrative accounts at least every 90 days for the mail imaging systems.

We recommend the vice president, Engineering Systems, and the acting chief information security officer and vice president, Digital Solutions, direct the manager, Technology Development and Applications, and the manager, Information Systems Security, to:

5. Establish a plan to update past due business impact assessments for the mail imaging systems to ensure compliance with Handbook AS-805 no later than September 30, 2016.

Management's Comments

Management generally agreed with the findings. Management also agreed with recommendations 1, 2, 3, and 4, and partially agreed with recommendation 5. See Appendix D for management's comments in their entirety.

Regarding recommendation 1, management will conduct a full review of administrative privileges for shared accounts on the mail imaging systems and remove the administrative privileges where appropriate. The target implementation date is September 30, 2016.

Regarding recommendation 2, management will conduct a business needs assessment of all mail imaging systems and update the systems wherever possible, subject to business needs and system limitations. The target implementation date is September 30, 2016.

Regarding recommendation 3, management will assess all accounts on the mail imaging systems to determine which have been in use for more than 365 days and which are guest accounts. Following this assessment, management will remove accounts where appropriate. The target implementation date is September 30, 2016.

Regarding recommendation 4, management will conduct a business needs assessment of all mail imaging systems and update the systems to require password changes wherever possible, subject to business needs and system limitations. The target implementation date is September 30, 2016.

Regarding recommendation 5, management agreed to conduct a BIA or an Infrastructure Impact Assessment (IAA) for eight of the mail imaging systems. Management also stated that they conducted IAAs for two of the identified systems [redacted]) in an appropriate time frame and retired one system[redacted] The target implementation date is September 30, 2016.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1 through 4, and corrective actions should resolve the issues identified in the report. The OIG considers management's comments to recommendation 5 to be partially responsive.

Regarding recommendation 5, for an Infrastructure Impact Assessment (IIA) to be accepted in place of a BIA, a risk assessment and risk acceptance letter approved by the vice president, Information Technology, and the vice president, Engineering Systems must be completed. As such, for these two systems management should either complete the BIAs as required by Handbook AS-805, or provide the approved risk assessments and risk acceptance letters along with the IIAs. In addition, the [redacted]system was an active production system at the locations where we performed our testing; therefore, management will need to provide support that the Postal Service has retired its [redacted]system before we close this recommendation.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information

Background

Mail images are processed locally at mail processing centers throughout the nation and remotely at the REC in Salt Lake City. The Postal Service has a complex network of automation equipment and administrative workstations that are managed and supported by a variety of organizational units: Engineering Systems, Maintenance Technical Support Center (MTSC), Network Operations, In-Plant Support, Information Technology, and the REC. Management controls over systems that use mail images fall under multiple Postal Service vice presidents and the vice president, Western Area Operations. See Appendix B for details about the systems.

The Postal Service used optical character recognition technology on more than 8,500 pieces of automated processing equipment to sort 98 percent of all hand-addressed letter mail and 99.5 percent of machine-printed mail in 2014. Throughout the agency, mail is processed at rates of 363,300 mailpieces per minute and 6,050 mailpieces per second. To accomplish this level of proficienc , the Postal Service scans the mailpieces to capture mail images and read the address information for sorting, distribution, and delivery.

According to In-Plant Support, Maintenance, and Engineering Systems, the majority of mail images are discarded within 4 seconds during mail processing; however, under specific circumstances some images may be kept for up to 120 days. Most mail image files are identified by a number that is not associated with customer information and cannot be used to retrieve that information however, one system[18] has mail images that are retrievable by customer information and are used to handle customer inquiries. Also, employees can copy mail images in the performance of their duties. These image files are required to be deleted within 60 days[19] of the date they were downloaded.

Objective, Scope, and Methodology

The overall objective of this audit was to determine the effectiveness of access controls over mail imaging systems. To answer this objective, we:

- Assessed management controls that affect mail images;
- Researched Privacy Act criteria;
- Reviewed signed BIAs to evaluate the privacy assessment information; and
- Evaluated access controls on six systems that store mail images.

We also requested asset management information, such as system identification, system location, authorized users, BIAs, and relevant policies at the beginning of the audit. Challenges prevented the Engineering Systems ARC liaison from completing our requests promptly.

Our audit fieldwork resulted in information retrieved from six systems at the Merrifield P&DC and the REC, composed o 12 subsystems. We discovered that Postal Service access controls include physical security; user groups; user accounts; passwords; folder and file permissions; limited storage; and first-in first-out deletion of image

We did not find issues with the privacy or the established practice of mail image retention; howeve , we determined the

18 [redacted]

19 The [redacted] non-disclosure agreement states that mail images must be deleted within 60 days. This statement appears every time an employee logs on to view images.

Postal Service could improve access controls over the mail images. The Postal Service is complying with the Privacy Act by placing the public on notice of how it is collecting, maintaining, disclosing, and discarding customer information.

We conducted this performance audit from March 2015 through January 2016, in accordance with generally accepted government auditing standards and included such tests of internal controls, as we considered necessary under the circumstances. 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 objective. e believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. e discussed our observations and conclusions with management on October 28, 2015, and included their comments where appropriate.

We did not assess the reliability of any computer-generated data for the purposes of this report and did not identify any databases containing mail images during this audit.

Prior Audit Coverage

The OIG issued the *Mail Isolation, Control, and Tracking* management alert (Report Number HR-MA-14-002, dated December 3, 2013) but did not claim any monetary impact in the alert.

Appendix B: Systems Tested

We reviewed six systems, which are composed of 12 subsystems we tested at the Merrifield P&DC and the REC. Table 3 lists the systems, subsystems, and Postal Service facilities that we examined.

Table 3 – Tested Systems

System	Subsystem	Information Resource Name	Postal Service Facility
[redacted]	[redacted]	[redacted]	REC
	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	Merrifield P&DC
[redacted]	[redacted]	[redacted]	REC
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	
	[redacted]	[redacted]	REC
	[redacted]	[redacted]	
	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	REC
	[redacted]	[redacted]	
	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	REC
[redacted]	[redacted]	[redacted]	Merrifield P&DC
6	12		

Source: OIG analysis.

Appendix C: Privacy and Business Impact Assessments

Table 4 lists the BIAs that were past-due as of June 1, 2015. Our review of BIAs identified 1 non-sensitive systems needing updates. The BIAs, on average, were past due 6.6 years.

Table 4 – Business Impact Assessments as of June 1, 2015

System Name	Document Date	Due Date (3 Years After Issuance)	Years Past Due
[redacted]	7/2/2008	7/2/2011	3.9
[redacted]	8/17/2004	8/17/2007	7.8
[redacted]	11/23/2004	11/23/2007	7.5
[redacted]	8/5/2008	8/5/2011	3.8
[redacted]	8/3/2007	8/2/2010	4.8
[redacted]	9/9/2004	9/9/2007	7.7
[redacted]	7/15/2003	7/14/2006	8.9
[redacted]	9/9/2004	9/9/2007	7.7
[redacted]	9/9/2004	9/9/2007	7.7
[redacted]	7/13/2003	7/12/2006	8.9
[redacted]	7/2/2008	7/2/2011	3.9
Total of Outdated BIAs	**11**		

Source: OIG analysis.

Appendix D: Managment's Comments

UNITED STATES POSTAL SERVICE

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Access Controls over Mail Imaging Systems (IT-AR-16-DRAFT), Project Number 15TG026IT000

Thank you for the opportunity to review and comment on the subject draft audit report. Management understands the intent of the draft report to help improve the overall posture and capabilities of the Postal Service to defeat and otherwise mitigate cybersecurity risks.

Management agrees with the findings in this report with the exception of 3 systems listed in Table 4 (Business Impact Assessments as of June 1, 2015) of this report. As of November 19, 2015 for two of the systems identified in the report [redacted], management already conducted Infrastructure Impact Assessments (IIA) within an appropriate timeframe and prior to the date identified by the OIG. Additionally, one system ([redacted]) has been retired.

Protecting the privacy of customer, employee, supplier and the Postal Service information has been and always will be a priority for the Postal Service. USPS has developed and is executing a multi phased cybersecurity improvement strategy to meet its security objectives and to further protect information and assets across the enterprise. The response to the recommendations in the report fall under the Cybersecurity Program Development project and the Identity and Access Management project, which are 2 of the 15 major project initiatives within the cybersecurity improvement strategy. The focus of the Cybersecurity Program Development strengthens the USPS enterprise-wide cybersecurity strategy, policies, governance structure, compliance program, and risk management framework. The focus of the Identity and Access Management project is to revise and develop policies and processes related to the creation, maintenance, and deactivation of identities with access to USPS information assets. The on-going implementation of these 2 strategic projects will help ensure the mitigation of the vulnerabilities identified in this report.

In addition to these 2 strategic projects management has already conducted a review of privileged access and has:

- Removed local administrative rights for many users, users requiring local rights are not allowed to operate on the main user domain
- Reduced the number of users with high-level access. (Since the breach, the number of privileged system administrators has decreased from 1500 down to 50)
- Removed 20,000 inactive devices

These actions are part of the ongoing improvement to the USPS Cybersecurity posture and will greatly assist in the Privacy and Protection of Mail Images.

In regards to recommendation #5, as of November 19, 2015 for two of the systems identified in the report ([redacted], management already conducted Infrastructure Impact Assessments (IIA) within an appropriate timeframe and prior to the date identified by the OIG. Additionally, one system ([redacted]) has been retired.

475 L'Enfant Plaza SW
Washington DC 20260-5000
www.usps.com

Recommendation [1]:
Remove administrative privileges for shared accounts on all mail imaging systems.

Management Response/Action Plan:
Management agrees with the intent of the recommendation and will conduct a full review of administrative privileges for shared accounts on mail imaging systems by the target date and remove the administrative privileges where appropriate.

Target Implementation Date:
September 30, 2016

Responsible Official:
Manager, Engineering Software Management

Recommendation [2]:
Require passwords for all mail imaging systems accounts in accordance with AS-805.

Management Response/Action Plan:
Management agrees with the intent of the recommendation and will conduct a thorough business needs assessment of all mail imaging systems by the target date and will update the systems wherever possible, subject to business needs and system limitations.

Target Implementation Date:
September 30, 2016

Responsible Official:
Manager, Engineering Software Management

Recommendation [3]:
Delete all accounts that have not been used in more than 365 days and all guest accounts on the mail imaging systems.

Management Response/Action Plan:
Management agrees with the intent of the recommendation and will conduct a thorough assessment of all accounts that have not been in use for more than 365 days and of all guest accounts on mail imaging systems by the target date. Following this assessment, management will remove accounts where appropriate.

Target Implementation Date:
September 30, 2016

Responsible Official:
Manager, Engineering Software Management

Recommendation [4]: Require users to change passwords for all administrative accounts at least every 30 days and for all non-administrative accounts at least every 90 days for the mail imaging systems.

Management Response/Action Plan:
Management agrees with the intent of the recommendation and will conduct a thorough business needs assessment of all mail imaging systems by the target date and will update the systems wherever possible, subject to business needs and system limitations.

Target Implementation Date:
September 30, 2016

Responsible Official:
Manager, Engineering Software Management

Recommendation [5]:
Establish a plan to update past-due business impact assessments for the mail imaging systems to ensure compliance with Handbook AS-805 no later than September 30, 2016.

Management Response/Action Plan:
Management partially agrees with the recommendation. For two of the systems identified in the report [redacted], management already conducted Infrastructure Impact Assessments (IIA) within an appropriate timeframe and prior to the date identified by the OIG. Additionally, one system [redacted] has been retired. Management agrees to conduct a Business Impact Assessment or Infrastructure Impact Assessment for the remaining 8 systems identified in the report by the target date.

Target Implementation Date:
September 30, 2016

Responsible Officials:
Manager, Technology Development and Applications (Engineering)
Manager, Corporate Information Security Office (CISO)

Michael J. Amato
Vice President, Engineering Systems

Gregory S. Crabb
(A) Chief Information Security Officer & Digital Solutions, Vice President

cc: *Manager, Corporate Audit Response Management*

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