OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 29, 2010

MICHAEL J. AMATO
MANAGER, ENGINEERING SOFTWARE MANAGEMENT

SUBJECT: Audit Report – Access Controls Over the Electronic Data Distribution Infrastructure (Report Number IS-AR-10-011)

This report presents the results of our audit of the Electronic Data Distribution Infrastructure (EDDI) (Project Number 10RG016IT000). Our objective was to determine whether EDDI access controls are effective. We performed the audit to supplement a U.S. Postal Service Office of Inspector General (OIG) investigation associated with alleged unauthorized access to and modification of EDDI servers and files. This audit addresses operational risk. See Appendix A for additional details about this audit.

EDDI servers – essentially workstations that share files – facilitate the automated delivery of address data, mail sort programs, and application software updates required to maintain current mail processing and handling equipment nationwide. Infrastructure access controls help prevent unauthorized modification to, or unavailability of, the data or systems that provide the Postal Service with the capability to deliver mail efficiently.

Conclusion

EDDI access controls are not effective. Management can improve preventive access controls and preserve the U.S. Postal Service brand by [redacted]

Access Controls

[redacted]

Administrators did [redacted] but rather, relied on automated scripts[1] to gather [redacted][2] only, which they believed to be an adequate

[1] A script is a list of commands executed to automate processes on a computer.
[2] [redacted].

control. Comprehensive [redacted] Additionally, administrators did not [redacted] because management did not emphasize information security policy. Moreover, administrators did not obtain formal approval through eAccess[3] to utilize shared user accounts because they were not aware of the requirement.[4]

[redacted] mitigates the risk of unauthorized access or undetected malicious activity occurring on the EDDI servers that might render the data or servers unavailable, which would affect the Postal Service's ability to deliver mail efficiently. [redacted] also enables forensic analysis in the event of a compromise; thus, improving the probability the Postal Service can identify the cause of any unauthorized activity that poses a threat to mail processing operations. [redacted] makes it difficult for administrators to identify individuals who perform unauthorized modifications to servers or its data. See Appendix B for our detailed analysis of this topic.

We recommend the manager, Engineering Software Management, direct the manager, Software Development, to:

1. Enable [redacted] on Electronic Data Distribution Infrastructure servers.

2. Manage [redacted] according to Handbook AS-805, *Information Security,* requirements.

3. Obtain approval through eAccess to use shared user accounts within the Electronic Data Distribution Infrastructure environment.

Management's Comments

Management agreed with the recommendations. In response to recommendation 1, management will implement [redacted] on all EDDI servers. Management stated that while they agree to implement recommendation 1, they believe that [redacted] does not mitigate the [redacted] or undetected malicious activity. To address recommendation 2, management will create individual user accounts for all EDDI support personnel and set password expiration dates to 45 days. Additionally, in response to recommendation 3, management will eliminate [redacted] on the EDDI servers.

[3] The Postal Service implemented the eAccess application to manage access to its information resources.
[4] Handbook AS-805, *Information Security,* dated November 2009, Section 9-4.2.4, Shared Accounts.

The target completion date for all three recommendations is October 2010. See Appendix C for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and management's corrective actions should resolve the issues identified in the report. Regarding recommendation 1, we believe that while [redacted] may not mitigate the risk [redacted] or malicious activity so that appropriate actions can be taken to mitigate future occurrences.

The OIG considers all recommendations significant, and therefore requires 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.

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

E-Signed by Darrell E. Benjamin, Jr
VERIFY authenticity with ApproveIt

Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Steven J. Forte
Kelly M. Sigmon
Shahpour Ashaari
Corporate Audit Response Management

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

EDDI is an Information Technology (IT) infrastructure managed by the Engineering Software Management group in [redacted]. The infrastructure consists of over [redacted] stand-alone servers that that receive data via [redacted] and transfer the data to [redacted] [redacted][5] which interface with mail processing and handling equipment. The EDDI servers – essentially workstations that share files – facilitate the automated delivery of address data, mail sort programs, and application software updates required to maintain current mail processing and handling equipment nationwide. Access controls to the infrastructure help prevent unauthorized modification to or unavailability of the data or systems and maintain the Postal Service's capability to deliver mail efficiently.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether EDDI access controls are effective. To achieve our objective, we interviewed key officials and reviewed applicable Postal Service policy, standards, and procedures. We limited our review to access and [redacted] controls on [redacted] EDDI servers using custom scripts and automated industry-accepted software tools.

We conducted this performance audit from March through July 2010 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on our audit objective. In addition, we used manual and automated techniques to analyze computer-processed data and concluded the data were sufficiently reliable to meet the report objective. We discussed our observations and conclusions with management officials on June 30, 2010, and included their comments where appropriate.

PRIOR AUDIT COVERAGE

The OIG did not identify any prior audits or reviews related to the objective of this audit.

[5] [redacted] servers connect to automated mail processing systems and enable file transfers, directory downloads, and terminal connections.

APPENDIX B: DETAILED ANALYSIS

Access Controls

We assessed [redacted] EDDI servers and identified that administrators did not:

- [redacted]

- [redacted]

- [redacted]

- [redacted].

- [redacted]

Information security policy requires that:

- [redacted].[6]

- Personnel authenticate[7] to information resources before performing any other action. One method of authentication is to require passwords.[8]

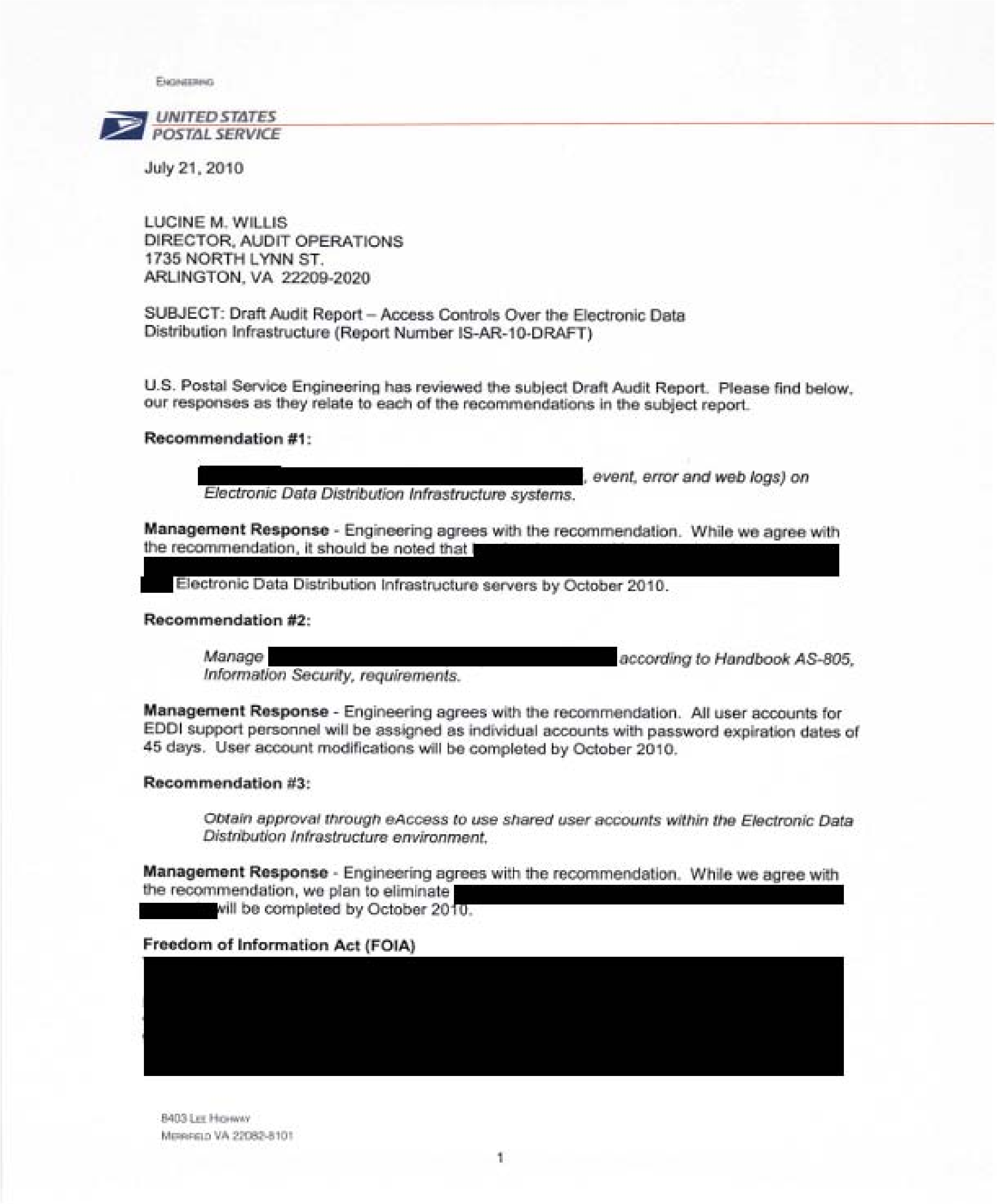
- Passwords for privileged or sensitive accounts expire at least every 30 days and passwords for all other accounts expire at least every 90 days. Management must make a request, in writing, to the manager, Corporate Information Security, for use of non-expiring passwords and document their use in eAccess.[9]

- Management delete logon identifications for user accounts not used within 1 year.[10]

- Management obtain approval to utilize shared user accounts via eAccess.[11]

[6] Handbook AS-805, [redacted].
[7] Authentication verifies the claimed identity of an individual or workstation.
[8] Handbook AS-805, Section 9-6, Authentication.
[9] Handbook AS-805, Section 9-6.1, Passwords.
[10] Handbook AS-805, Section 9-5.5, Terminating Logon Identification.
[11] Handbook AS-805, Section 9-4.2.4, Shared Accounts.

APPENDIX C: MANAGEMENT'S COMMENTS



ENGINEERING

UNITED STATES
POSTAL SERVICE

July 21, 2010

LUCINE M. WILLIS
DIRECTOR, AUDIT OPERATIONS
1735 NORTH LYNN ST.
ARLINGTON, VA 22209-2020

SUBJECT: Draft Audit Report – Access Controls Over the Electronic Data Distribution Infrastructure (Report Number IS-AR-10-DRAFT)

U.S. Postal Service Engineering has reviewed the subject Draft Audit Report. Please find below, our responses as they relate to each of the recommendations in the subject report.

Recommendation #1:

> [redacted], *event, error and web logs) on Electronic Data Distribution Infrastructure systems.*

Management Response - Engineering agrees with the recommendation. While we agree with the recommendation, it should be noted that [redacted] Electronic Data Distribution Infrastructure servers by October 2010.

Recommendation #2:

> *Manage* [redacted] *according to Handbook AS-805, Information Security, requirements.*

Management Response - Engineering agrees with the recommendation. All user accounts for EDDI support personnel will be assigned as individual accounts with password expiration dates of 45 days. User account modifications will be completed by October 2010.

Recommendation #3:

> *Obtain approval through eAccess to use shared user accounts within the Electronic Data Distribution Infrastructure environment.*

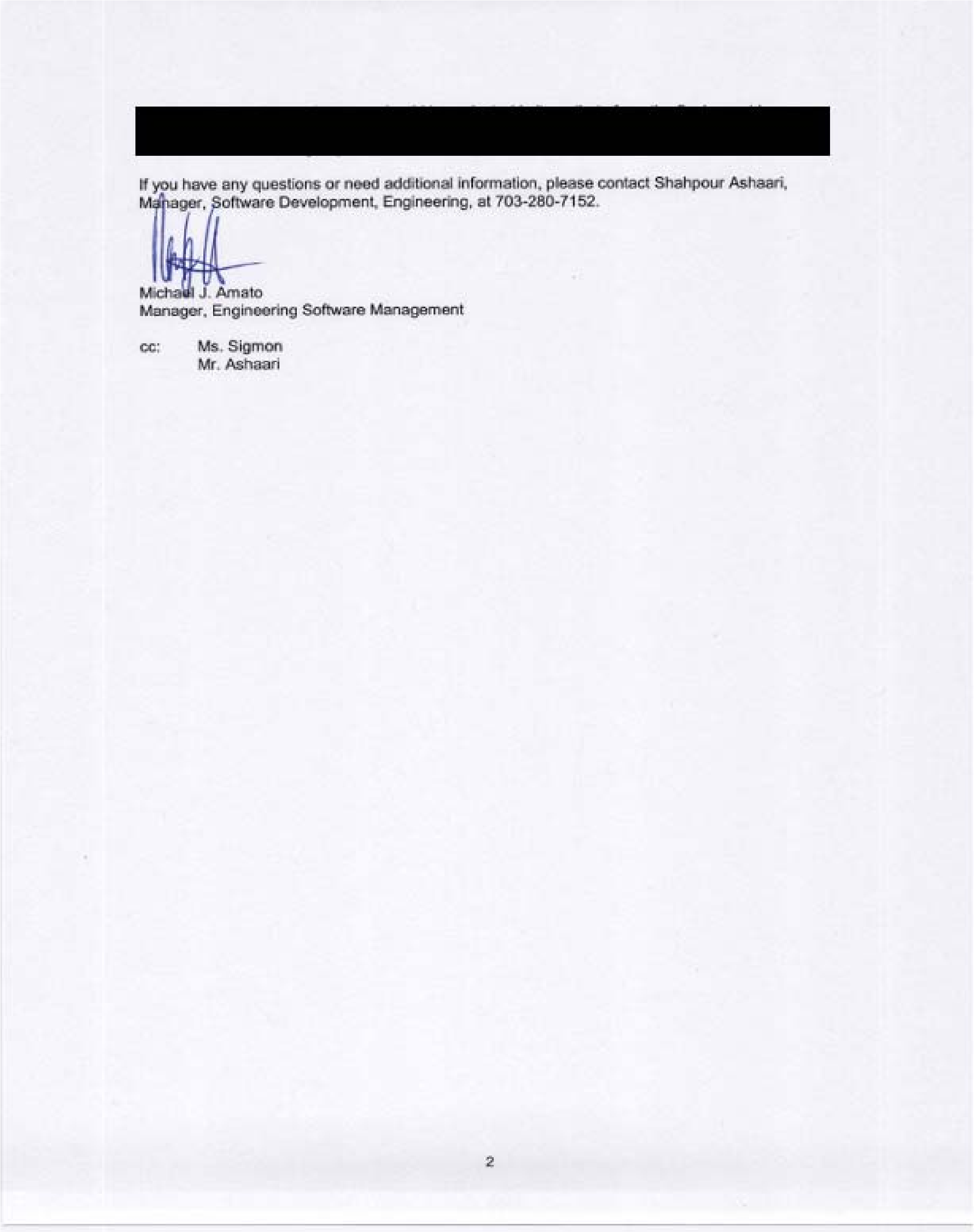
Management Response - Engineering agrees with the recommendation. While we agree with the recommendation, we plan to eliminate [redacted] will be completed by October 2010.

Freedom of Information Act (FOIA)

[redacted]

8403 LEE HIGHWAY
MERRIFIELD VA 22082-8101

1



[redacted]

If you have any questions or need additional information, please contact Shahpour Ashaari, Manager, Software Development, Engineering, at 703-280-7152.

Michael J. Amato
Manager, Engineering Software Management

cc: Ms. Sigmon
Mr. Ashaari