Highlights

Table of Contents

Findings

Recommendations

Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Software Change Management for Engineering Systems

Audit Report

Report Number
IT-AR-16-007

June 13, 2016

Print

Highlights
Table of Contents
Findings
Recommendations
Appendices

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Our objective was to evaluate the effectiveness of the software change management process for Engineering Systems.

Background

The U.S. Postal Service's Engineering Systems group uses the Serena Business Manager Team Track application (Serena) to track software change requests (SCRs) for over 80 Engineering Systems' applications. There were 391 user accounts in Serena. Changes occur when software problems are encountered or new functionality is added to a system. Serena tracks SCRs from submission through implementation of a software release. Also, Serena can manage the status of the SCRs and report on current and historical SCRs. There were 1,328 Engineering Systems SCRs in the Serena application between January 1 and December 16, 2015.

Our objective was to evaluate the effectiveness of the software change management process for Engineering Systems.

What The OIG Found

We found that Engineering Systems was not effectively administering their software change management process. Engineering Systems management did not perform risk assessments on any of the 190 SCRs in our random sample. We also found that 67 of the 190 SCRs (35 percent) were not properly managed in Serena. Specifically, we identified seven SCRs that bypassed the required approval process. We also found 32 SCRs pending without a management decision and 28 SCRs that were approved but not implemented and were over 3 years old, with the oldest one being open 8 years. In addition, the system administrator was not disabling or removing user accounts as required. Specifically, we determined that 72 of the 391 total user accounts in the Serena system (18 percent) were not disabled after 90 days of inactivity, and 107 of the 391 accounts (27 percent) were not terminated after 365 days of inactivity.

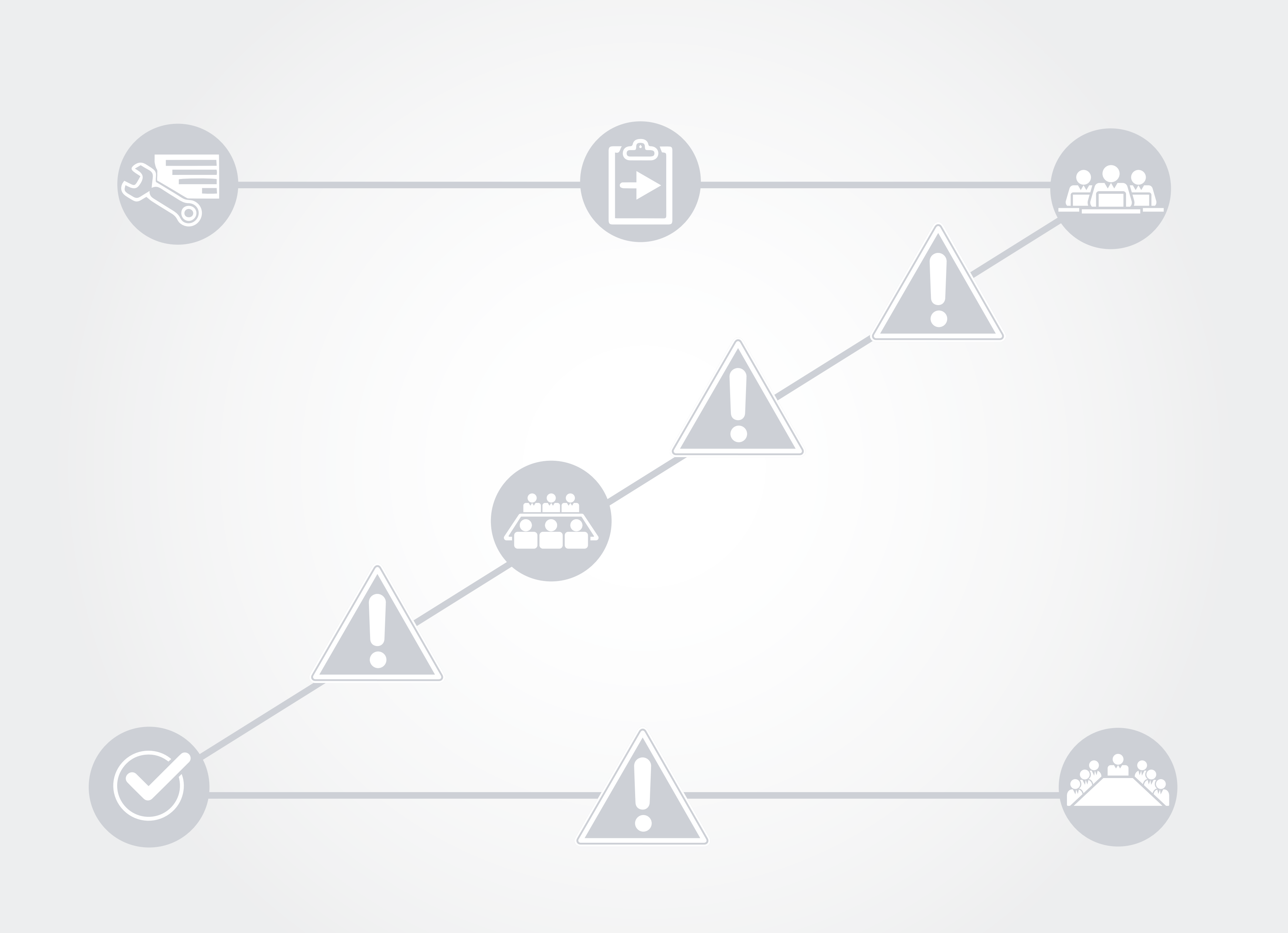
Risk assessments were not performed on any of the 190 SCRs we reviewed because management focused on higher priorities, such as deploying mail processing equipment. Also, there is no guidance for when management can bypass the approval process. In addition, management did not discuss in their monthly meetings the SCRs that were pending or not implemented. Finally, user accounts were not properly disabled or terminated because the system administrator was not aware that policies in Postal Service Handbook AS-805, *Information Security*, applied to Serena.

Without effective implementation of the software change management process, Engineering Systems applications could have unauthorized changes that result in system failure. In addition, without adequate account management, inappropriate user access could compromise data within Serena.

What The OIG Recommended

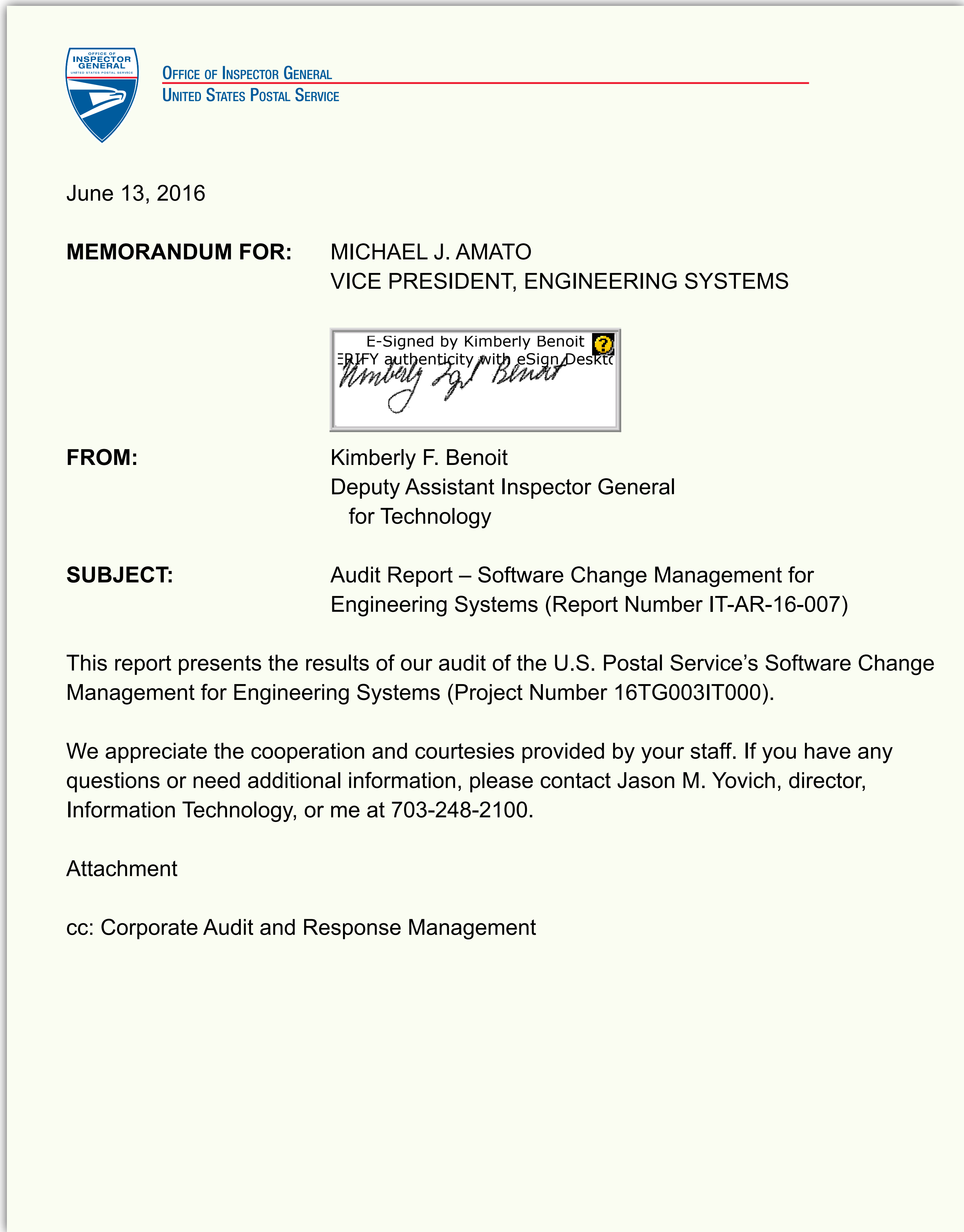
We recommended the vice president, Engineering Systems ensure staff perform risk assessments and document them in Serena, create guidance for SCRs that bypass approval, allocate time in monthly meetings to review SCRs that are pending or not implemented, and disable and terminate user accounts in accordance with Handbook AS-805.

Click On The Icons Below To Reveal The Steps In The Serena Software Change Management Process.



Click To Reset

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 13, 2016

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

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskto

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology

SUBJECT: Audit Report – Software Change Management for Engineering Systems (Report Number IT-AR-16-007)

This report presents the results of our audit of the U.S. Postal Service’s Software Change Management for Engineering Systems (Project Number 16TG003IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

Engineering Systems uses Serena to track and manage software change requests for over 80 Engineering Systems' applications.

Engineering Systems was not effectively administering their software change management process.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's Serena Business Manager Team Track application (Serena) to track software change requests for the Engineering Systems group (Project Number 16TG003IT000). Our objective was to evaluate the effectiveness of the software change management process for Engineering Systems. See Appendix A for additional information about this audit.

Engineering Systems uses Serena[1] to track and manage software change requests (SCR)[2] for over 80 Engineering Systems' applications. There were 391 user accounts in Serena. Changes occur due to software problems encountered or new functionality requirements needed in an application. Serena tracks SCRs from submission through implementation of a new software release.[3] Serena has various capabilities to manage the Product Change Board (PCB)[4] status of SCRs. The statuses are pending, deferred,[5] bypassed, and approved. Additionally, Serena can report on current and historical SCRs. There were 1,328 Engineering Systems SCRs in the application between January 1 and December 16, 2015.

Four groups are involved in the Engineering Systems software change management process:

- The Software Process Management group develops the software change management process guidance documentation, reviews the timeline for software releases, and acts as the administrator for Serena.
- Design Cognizant Organizations (DCO)[6] identify SCRs and determine the costs, impact, and risks associated with them.
- PCBs approve SCRs and consolidate them into software releases.
- The Executive Oversight Board (EOB)[7] authorizes software releases after SCRs are assigned to a release.

Summary

We found that Engineering Systems was not effectively administering their software change management process. Engineering Systems management did not perform risk assessments on any of the 190 SCRs in our random sample. We also found that 67 of the 190 (35 percent) SCRs were not properly managed. Specifically, we identified seven SCRs that bypassed the required approval process. We also found 32 SCRs pending without a management decision and 28 SCRs that were approved but not implemented that were over 3 years old, with the longest one being open 8 years. In addition, the system administrator was not disabling or removing user accounts as required.[8] Specifically, we determined that 72 of the 391 total user accounts in the system (18 percent) were not disabled after 90 days of inactivity and 107 of the 391 user accounts (27 percent) were not terminated after 365 days of inactivity.

[1] A web application that allows Engineering Systems to submit, track, and modify SCRs.
[2] Proposed enhancements or modifications to existing systems to improve performance.
[3] A group of SCRs approved by the EOB for a particular system.
[4] There are six Engineering Systems PCBs: Letters, Flats, Package, Material Handling, Delivery and Retail, and Support Systems.
[5] PCB items are typically deferred until a later date or for additional information.
[6] There are six DCOs within Engineering Systems: Software Development, Letter Mail Technology, Flat Mail Technology, Package Technology and Visibility, Material Handling, and Delivery and Retail Technology.
[7] The EOB has representatives from across Engineering Systems and Network Operations, including the following groups: Engineering Software Management, Technology Acquisition and Program Management, Technology Development and Applications, and Network Operations Technical Support.
[8] Handbook AS-805, *Information Security*, Section 9-5.3, Suspending Log-on IDs, and Section 9-5.5, Terminating Log-on IDs.

Highlights
Table of Contents
Findings
Recommendations
Appendices

Management did not perform risk assessments on the SCRs because they were focused on higher priorities, such as deploying mail processing equipment. Also, there is no guidance for when management can bypass the approval process. In addition, management did not discuss in their monthly meetings the SCRs that were pending or not implemented. Finally, user accounts were not properly disabled or terminated because the system administrator was not aware that policies in Handbook AS-805 applied to Serena.

> ***Risk assessments were not performed on the SCRs because management focused on higher priorities.***

Without effective implementation of the software change management process, Engineering Systems applications could have unauthorized changes that result in system failure. In addition, without adequate account management, inappropriate user access could compromise data.

We recommend management perform risk assessments and document them in Serena, create guidance for SCRs that bypass approval, allocate time in monthly meetings to review SCRs that are pending or not implemented, and disable and terminate user accounts in accordance with Handbook AS-805.

Missing Risk Assessments

DCOs did not perform risk assessments[9] on any of 190 SCRs in our sample between January 1 and December 16, 2015. According to the software process management guidance document,[10] DCOs assigned to the SCRs are required to assess the risk associated with the SCR and document those results in Serena. As a best practice,[11] management should identify risks to the business and the likelihood they will occur as part of the change management process. Risk assessments were not performed on the SCRs because management focused on higher priorities, such as deploying mail processing equipment. If SCRs are implemented without appropriate consideration and evaluation of risk, then inappropriate changes could be introduced to production systems,[12] resulting in system failures.

Software Change Requests are not Properly Managed

In our random sample we identified 67 of the 190 SCRs with changes that were not properly managed (35 percent):

- Seven bypassed the required PCB approval process.
- Thirty-two were pending without a PCB decision for over 3 years.
- Twenty-eight were PCB-approved but not implemented for over 3 years, with the longest one being open 8 years.

According to the Engineering Systems PCB charter,[13] SCRs should be analyzed, approved, and implemented in a consistent and timely manner. This occurred because there is no guidance for when management can bypass the PCB approval process. In addition, management did not allocate time in their monthly meetings to review the status of their SCRs. As a result, changes may not be implemented rapidly enough to meet Engineering Systems' new business needs.

[9] Analyzing threat and vulnerability information to determine the likelihood that a specified negative event will occur.
[10] Software Process Management's *Software Change Request Preliminary Review Process,* dated April 29, 2014.
[11] Information Technology Infrastructure Library, *Service Transition Processes*, dated 2011.
[12] Engineering Systems applications included in our sample of SCRs were Combined Input Output Subsystem, Flats Sequencing System, Automated Flats Sorting Machine 100, Passive Adaptive Scanning System, Integrated Data System, and Delivery Bar Code Sorter.
[13] Defines Engineering Systems' responsibilities to ensure that software changes for all systems across all platforms are considered in a consistent manner.

During our audit, the DCO for Flat Mail Technology took corrective action by updating the status of 14 SCRs from pending without a management decision to being approved, disapproved, or deferred in Serena.

Serena User Accounts not Disabled or Terminated

Serena system administrator was not disabling or removing user accounts as required.

We determined 72 of the 391 total user accounts in the Serena system (18 percent) were not disabled after 90 days of inactivity, and 107 of the 391 (27 percent) user accounts were not terminated after 365 days of inactivity. According to Handbook AS-805,[14] management must disable user accounts that have not been accessed within the past 90 days and terminate those that have not been used in the last 365 days. User accounts were not correctly disabled and terminated because the system administrator was not aware that Handbook AS-805 policies applied to Serena.[15] Without adequate account management, inappropriate user access could compromise data.

[14] Handbook AS-805, Section 9-5.3, Suspending Log-on IDs, and Section 9-5.5, Terminating Log-on IDs.

[15] The Serena system resides in the Information Technology environment and must adhere to Handbook AS-805.

Recommendations

We recommend management perform risk assessments and document them in Serena, create guidance for software change requests that bypass approval, allocate time in monthly meetings to review software change requests that are pending or not implemented, and disable and terminate user accounts in accordance with Handbook AS-805.

We recommend the vice president, Engineering Systems:

1. Require Design Cognizant Organizations to perform risk assessments for software change requests and document the results in Serena Business Manager Team Track prior to the implementation of software change requests into production.

2. Direct the Software Process Management group to create guidance for when the Design Cognizant Organizations are allowed to bypass Product Change Board approval.

3. Require the Design Cognizant Organizations and the Product Change Boards to allocate time in their monthly meetings to review software change requests that are pending without a management decision or approved but not implemented; and, document the results of these discussions in Serena Business Manager Team Track.

4. Disable Serena Business Manager Team Track user accounts that have not been accessed in over 90 days in accordance with Postal Service Handbook AS-805, *Information Security*.

5. Terminate Serena Business Manager Team Track user accounts that have not been used in over 365 days in accordance with Postal Service Handbook AS-805, *Information Security*.

Management's Comments

Management agreed with the findings and recommendations in the report. Management stated that all recommendations were implemented in May 2016.

Regarding recommendation 1, management stated that a risk assessment field has been added to the Software PCB workflow that is required to be completed for all PCB approval decisions.

Regarding recommendation 2, management stated they established a new PCB Chair Bypass Review process for all bypass items, with the PCB chair providing approval or disapproval.

Regarding recommendation 3, management stated Engineering Systems Software Process Management staff will be attending the PCB meetings to ensure that pending items are being reviewed timely.

Regarding recommendation 4, management stated that a system-generated email notification will be sent to inactive account users for all Engineering Systems Software Process group-managed user types. These accounts will be deactivated after 91 days of inactivity in accordance with Handbook AS-805, Section 9.4.3, *Account Management*.

Regarding recommendation 5, management stated Software Process Management is responsible for account management. User accounts will be managed as described in Recommendation 4 and accounts will be deleted in accordance with AS-805.

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

Evaluation of Management’s Comments

The OIG considers management’s comments generally responsive to all recommendations in the report and the corrective action proposed should resolve the issues identified.

Regarding recommendations 1, 2 and 3, we generally agree with management’s response. However, documentation should also be maintained for their risk assessments, the guidance for when the DCOs are allowed to bypass the PCB, and the results of monthly meeting discussions regarding requests that are pending or approved but not implemented.

Management has not provided the OIG supporting documentation to verify that corrective actions were taken in May, 2016. Therefore, all recommendations will remain open until management provides this documentation.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All recommendations 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.

Appendices

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

Appendix A: Additional Information

The scope of this audit was software change requests within Serena and access controls over Serena Business Manager Team Track between January 1 and December 16, 2015.

Background

The change management process is the sequence of steps or activities followed by a change management team or project. The purpose of software change management is to process and review software changes in a consistent and timely manner following structured practices. Software change management practices consider the impact, costs, benefits, and risks associated with proposed changes.

Four groups are involved in the Engineering Systems software change management process:

- The Software Process Management group develops the software change management process guidance documentation, reviews the timeline for software releases, and acts as the administrator for Serena.
- DCOs[16] identify SCRs and determine the costs, impact, and risks associated with them.
- PCBs approve SCRs and consolidate them into software releases.
- EOBs authorize software releases after SCRs are assigned to a release.

There were 1,328 Engineering Systems SCRs in the Serena application between January 1 and December 16, 2015.

Each of the six PCBs must be composed of enough individuals to ensure that all critical perspectives are represented without diminishing the PCB's ability to make timely decisions. Each PCB has a charter that describes the roles of the PCB and the EOB when making modifications to specific systems. These PCB charters recommend holding monthly meetings to review SCRs. When the PCB makes a decision, it assigns approved SCRs to a software release.

Objective, Scope, and Methodology

Our objective was to evaluate the effectiveness of the software change management process for Engineering Systems. The scope of this audit was SCRs within Serena and access controls over Serena between January 1 and December 16, 2015.

To accomplish our objective, we:

- Reviewed current policies and guidance related to software change management and interviewed Engineering Systems personnel to evaluate the effectiveness of the software change management process.
- Interviewed Engineering Systems personnel to identify SCRs and determine if changes were appropriately managed.
- Analyzed a random sample of 190 of the 1,328 SCRs within Serena to determine if required approvals were obtained and requirements were followed.
- Interviewed the Serena administrator to determine how user access and log-in requirements are established. We also examined access control data to evaluate if user accounts were authorized and up-to-date.

[16] There are six DCOs within Engineering Systems: Software Development, Letter Mail Technology, Flat Mail Technology, Package Technology and Visibility, Material Handling, and Delivery and Retail Technology.

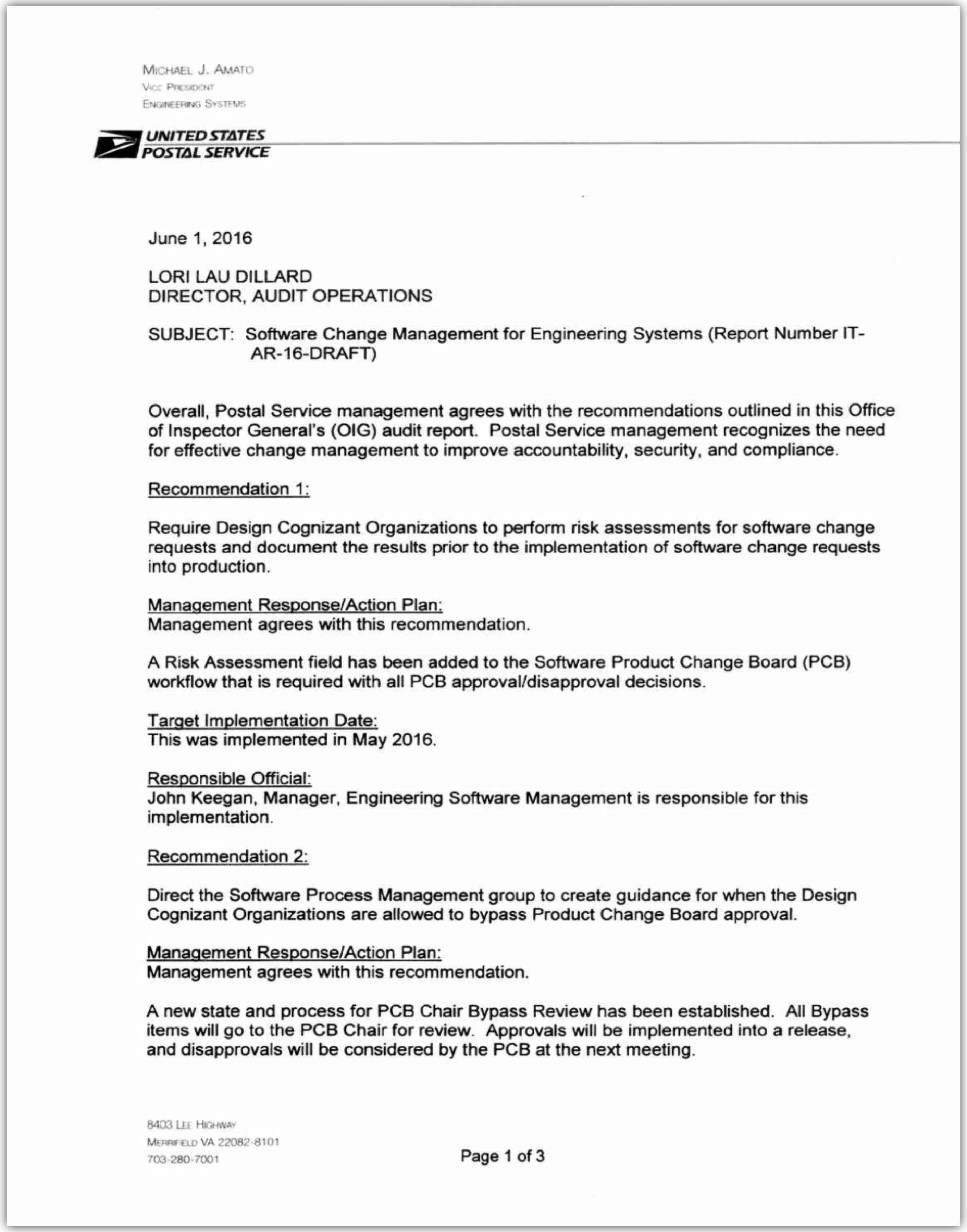
We conducted this performance audit from November 2015 through June 2016, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on May 11, 2016, and included their comments where appropriate.

We assessed the reliability of SCR data by verifying our results with the DCOs and PCBs, as well as the Software Process Management group. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The U.S. Postal Service Office of Inspector General did not identify any prior audits or review related to the scope of this audit.

Appendix B: Management's Comments



MICHAEL J. AMATO
VICE PRESIDENT
ENGINEERING SYSTEMS

UNITED STATES
POSTAL SERVICE

June 1, 2016

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Software Change Management for Engineering Systems (Report Number IT-AR-16-DRAFT)

Overall, Postal Service management agrees with the recommendations outlined in this Office of Inspector General's (OIG) audit report. Postal Service management recognizes the need for effective change management to improve accountability, security, and compliance.

Recommendation 1:

Require Design Cognizant Organizations to perform risk assessments for software change requests and document the results prior to the implementation of software change requests into production.

Management Response/Action Plan:
Management agrees with this recommendation.

A Risk Assessment field has been added to the Software Product Change Board (PCB) workflow that is required with all PCB approval/disapproval decisions.

Target Implementation Date:
This was implemented in May 2016.

Responsible Official:
John Keegan, Manager, Engineering Software Management is responsible for this implementation.

Recommendation 2:

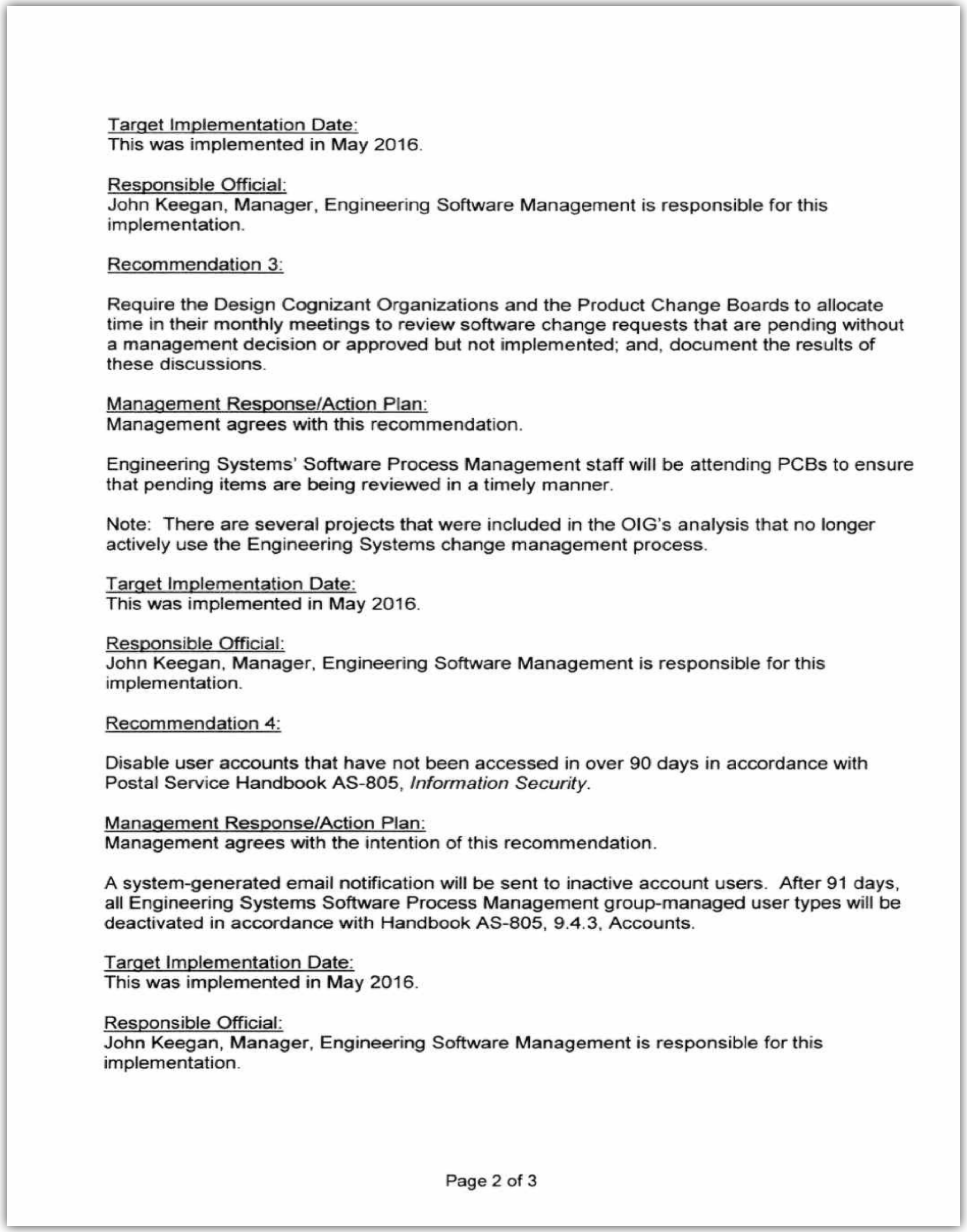
Direct the Software Process Management group to create guidance for when the Design Cognizant Organizations are allowed to bypass Product Change Board approval.

Management Response/Action Plan:
Management agrees with this recommendation.

A new state and process for PCB Chair Bypass Review has been established. All Bypass items will go to the PCB Chair for review. Approvals will be implemented into a release, and disapprovals will be considered by the PCB at the next meeting.

8403 LEE HIGHWAY
MERRIFIELD VA 22082-8101
703-280-7001

Page 1 of 3



Target Implementation Date:
This was implemented in May 2016.

Responsible Official:
John Keegan, Manager, Engineering Software Management is responsible for this implementation.

Recommendation 3:

Require the Design Cognizant Organizations and the Product Change Boards to allocate time in their monthly meetings to review software change requests that are pending without a management decision or approved but not implemented; and, document the results of these discussions.

Management Response/Action Plan:
Management agrees with this recommendation.

Engineering Systems' Software Process Management staff will be attending PCBs to ensure that pending items are being reviewed in a timely manner.

Note: There are several projects that were included in the OIG's analysis that no longer actively use the Engineering Systems change management process.

Target Implementation Date:
This was implemented in May 2016.

Responsible Official:
John Keegan, Manager, Engineering Software Management is responsible for this implementation.

Recommendation 4:

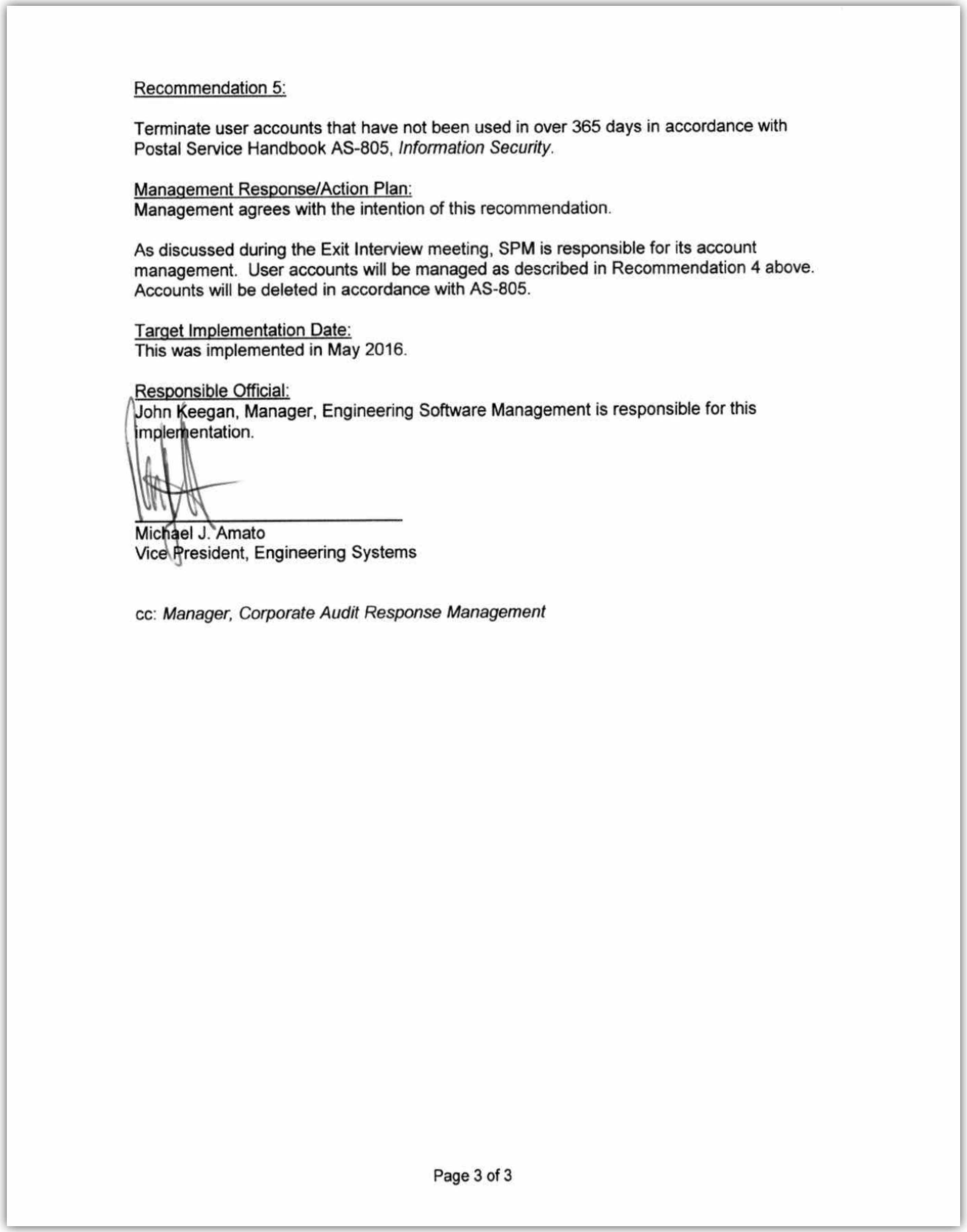
Disable user accounts that have not been accessed in over 90 days in accordance with Postal Service Handbook AS-805, *Information Security*.

Management Response/Action Plan:
Management agrees with the intention of this recommendation.

A system-generated email notification will be sent to inactive account users. After 91 days, all Engineering Systems Software Process Management group-managed user types will be deactivated in accordance with Handbook AS-805, 9.4.3, Accounts.

Target Implementation Date:
This was implemented in May 2016.

Responsible Official:
John Keegan, Manager, Engineering Software Management is responsible for this implementation.



Recommendation 5:

Terminate user accounts that have not been used in over 365 days in accordance with Postal Service Handbook AS-805, *Information Security*.

Management Response/Action Plan:
Management agrees with the intention of this recommendation.

As discussed during the Exit Interview meeting, SPM is responsible for its account management. User accounts will be managed as described in Recommendation 4 above. Accounts will be deleted in accordance with AS-805.

Target Implementation Date:
This was implemented in May 2016.

Responsible Official:
John Keegan, Manager, Engineering Software Management is responsible for this implementation.

Michael J. Amato
Vice President, Engineering Systems

cc: *Manager, Corporate Audit Response Management*

Page 3 of 3

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