Highlights
Table of Contents
Findings
Recommendations
Appendices

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Information Technology Continuity of Operations Plans

Audit Report

Report Number
IT-AR-17-002

March 29, 2017

Print

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

To support the Postal Service's overarching COOP plan, IT management developed their own COOP plans, referred to as Functional Workgroup Annex (FWGA) plans. These FWGA plans address essential information technology functions.

Background

The U.S. Postal Service is the center of a $1.4 trillion mailing industry. To meet its mail delivery mandate, the Postal Service has developed an overarching Continuity of Operations (COOP) plan to continue essential business functions when there is a disruption of normal operations.

To support the Postal Service's overarching COOP plan, Information Technology (IT) management developed their own COOP plans, referred to as Functional Workgroup Annex (FWGA) plans. These FWGA plans address essential information technology functions.

Federal directives require the Postal Service to develop and maintain COOP plans. Most recently, Presidential Policy Directive 40, issued in July 2016, reiterates COOP plan requirements and the need to include information technology systems, processes, and resources in plan development. In addition, Postal Service policy requires FWGA plans for all computer solution and service centers.

Our objective was to determine whether the Postal Service's IT division has viable FWGA capabilities to support essential business functions.

What the OIG Found

We found that the Postal Service is unable to meet its essential business functions because its FWGA plans are not current at [redacted] Postal Service IT locations we selected: [redacted], the [redacted] and the [redacted] centers.

We found that Postal Service management did not annually review, update, and test FWGA plans. For example, they had not updated [redacted] of the [redacted] plans in over [redacted] years. The plans were also incomplete and missing key requirements such as identifying critical information system assets, alternative telecommunications services, and procedures for using alternative processing sites that are not susceptible to the same threats as the primary location. Additionally, Postal Service management did not train personnel who execute the existing FWGA plans.

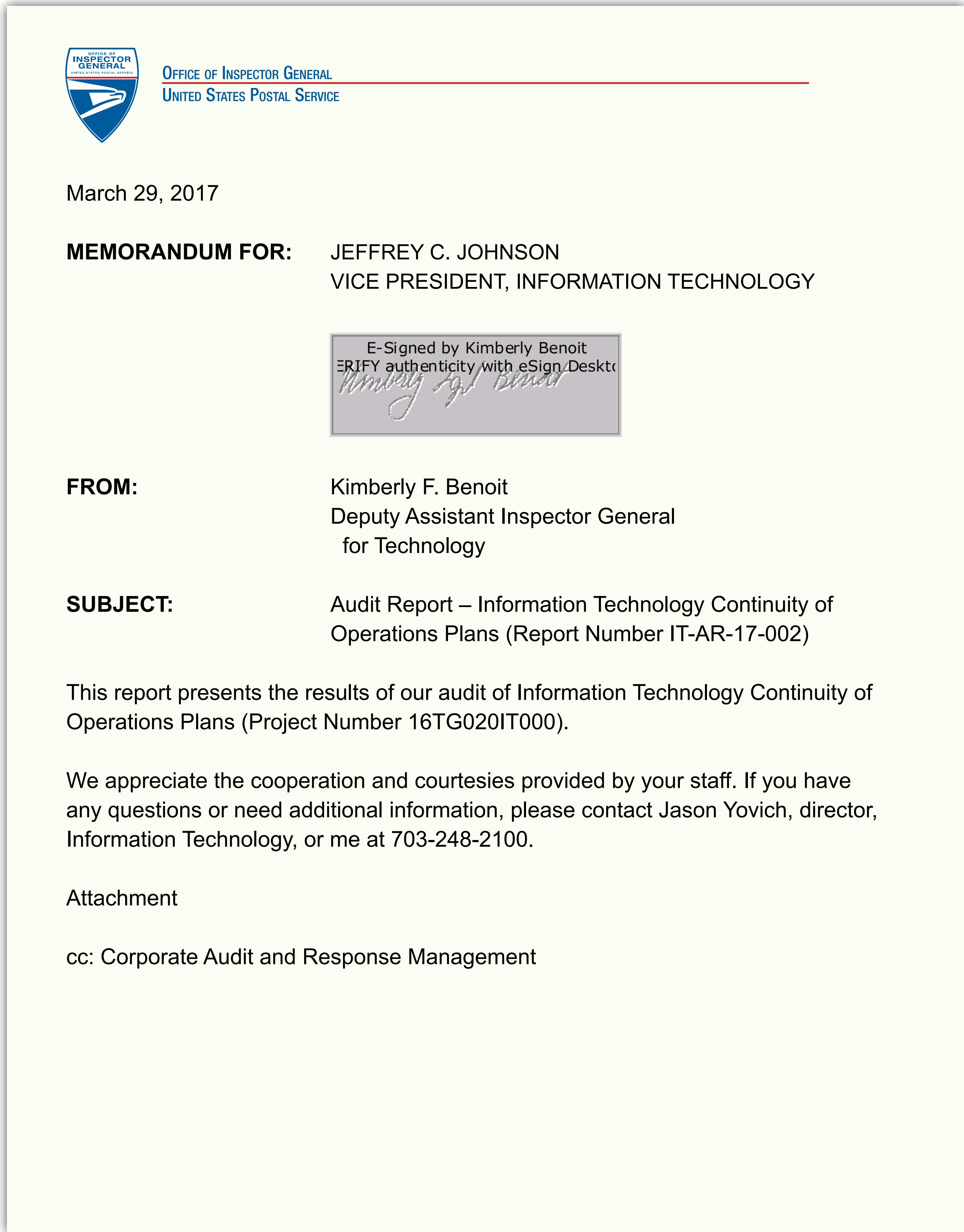
These issues occurred because Postal Service management did not have a policy that defined requirements for managing FWGA plans.

Without current, complete, and tested FWGA plans, the Postal Service will not be able to effectively support essential information system resources and services during an event that disrupts normal operations. In addition, a lack of training would result in Postal Service personnel not having the skills required to support essential functions during a continuity event.

What the OIG Recommended

We recommended Postal Service management create a policy for managing FWGA plans based on federal directives and industry best practices; review, update, and test FWGA plans annually; and require annual training for all personnel with FWGA plan responsibilities.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 29, 2017

MEMORANDUM FOR: JEFFREY C. JOHNSON
VICE PRESIDENT, INFORMATION TECHNOLOGY

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Deskto

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

SUBJECT: Audit Report – Information Technology Continuity of Operations Plans (Report Number IT-AR-17-002)

This report presents the results of our audit of Information Technology Continuity of Operations Plans (Project Number 16TG020IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Highlights
Table of Contents
Findings
Recommendations
Appendices

Findings

Postal Service policy requires FWGA plans for all computer solution and service centers.

We found that the Postal Service is unable to meet its essential business functions because its FWGA plans are not current at [redacted] Postal Service IT locations we selected: the [redacted] centers, the [redacted] Center, and the [redacted] centers.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's Information Technology (IT) Continuity of Operations Plans (Project Number 16TG020IT000). Our objective was to determine whether the Postal Service's IT division has viable Functional Workgroup Annex (FWGA) capabilities to support essential business functions. See Appendix A for additional information about this audit.

The Postal Service is the center of a $1.4 trillion mailing industry. To ensure it can meet its mail delivery mandate, the Postal Service has developed a Continuity of Operations (COOP) plan[1] for essential business functions to continue when there is disruption of normal operations.

To support the Postal Service's overarching COOP plan, IT management developed their own COOP plans — referred to as FWGA plans — to address essential information technology functions and act as auxiliary plans to the Postal Service Headquarters COOP plan.

Federal directives require the Postal Service to develop and maintain COOP plans. The Department of Homeland Security (DHS), in coordination with interagency partners, developed two guidelines — Federal Continuity Directive (FCD) 1[2] and FCD 2[3] — to assist government agencies in developing and implementing COOP plans. FCD 1 provides direction for developing COOP plans and programs, while FCD 2 implements the requirements of FCD 1 and provides guidance for validating and updating an agency's essential functions. Most recently, Presidential Policy Directive (PPD) 40,[4] issued in July 2016, reiterates COOP plan requirements and the need to include information technology systems, processes, and resources in plan developments. In addition, Postal Service policy requires FWGA plans for all computer solution and service centers.

Summary

We found that the Postal Service is unable to meet its essential business functions because its FWGA plans are not current at [redacted] Postal Service IT locations we selected: the [redacted] Centers, the [redacted] Center, and the [redacted] Centers. We found that Postal Service management did not annually review, update, and test the FWGA plans. For example, they had not updated [redacted] of the [redacted] plans in over [redacted] years. The plans were also incomplete and missing key requirements such as identifying critical information system assets, alternative telecommunications services, and procedures for using alternative processing sites that are not susceptible to the same threats as the primary location. Additionally, Postal Service management did not train personnel who execute the existing FWGA plans. These issues occurred because Postal Service management did not have a policy that defined requirements for managing FWGA plans.

Without current, complete, and tested FWGA plans, the Postal Service will not be able to effectively support essential information system resources and services during an event that disrupts normal operations. In addition, a lack of training would result in Postal Service personnel not having the skills required to support essential functions during a continuity event.

[1] Postal Service Headquarters, Continuity of Operations Plan, June 2016.
[2] Federal Continuity Directive 1, *Federal Executive Branch National Continuity Program and Requirements,* October 2012.
[3] Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, July 2013.
[4] Presidential Policy Directive 40, *National Continuity Policy*, July 15, 2016.

Highlights
Table of Contents
Findings
Recommendations
Appendices

Functional Workgroup Annex Maintenance and Testing

Postal Service management does not have functional IT FWGA plans for continuing essential IT functions in the event that normal operations are disrupted. Specifically, Postal Service management does not annually review, update, and test existing FWGA plans. For example, management had not updated [redacted] of the [redacted] plans we reviewed in over [redacted] years and all of the plans had [redacted] former employees listed as points of contact. Table 1 summarizes our analysis of the plans at each site.

Without current, complete, and tested FWGA plans, the Postal Service will not be able to effectively support essential information system resources and services during an event that disrupts normal service operations.

Table 1. Summary of FWGA Plan Review Results

[redacted]

Source: FWGAs provided by the manager, IT centers and Infrastructures.

In addition, these plans were incomplete and missing key requirements such as identifying critical information system assets that support essential business functions, alternative telecommunications services, and procedures for using alternative processing sites that are not susceptible to the same threats as the primary location. According to FCD 1 and National Institute of Standards and Technology Special Publication 800-34r1 (NIST SP 800-34r1),[5] Postal Service management should review FWGA plans annually — and when significant changes are made — to ensure they are complete and accurate. Management should also test the plans annually.

These issues occurred because Postal Service management did not have a policy that defined requirements for managing FWGA plans. Handbook AS-805[6] references a non-existent management instruction policy — Postal Service Continuity Policy (AS-280-2009-1) — that was never finalized or published. Furthermore, Handbook AS-805 refers to an outdated federal directive for developing, implementing, testing, and maintaining plans.

Without current, complete, and tested FWGA plans, the Postal Service will not be able to effectively support essential information system resources and services during an event that disrupts normal service operations. For example, having outdated personnel listed in the plans results in current staff not knowing whom to contact during a disruptive event.

In September 2016, management started reviewing existing FWGA plans. Management stated that efforts are underway to determine which Postal Service business and IT functions are essential, and they will update the FWGA plans accordingly.

[5] *NIST SP 800-*34r1, *Contingency Planning Guide for Federal Information Systems*, May 2010.
[6] Handbook AS-805, *Information Security* – Section 12-1, November 2016

Print

During our audit, Postal Service management took corrective action and started COOP training for personnel with FWGA responsibilities.

Functional Workgroup Annex Training

Postal Service management did not provide annual training for personnel who are responsible for executing the existing FWGA plans. We requested training records for individuals responsible for FWGA plans; however, management did not make it a priority to provide COOP training to personnel responsible for executing the plans.

According to FCD 1, an organization's training program must include and document annual training on the roles and responsibilities for personnel who activate, support, and sustain the continuity program. Annual training would include activities such as activating continuity plans, conducting essential functions from a telework site, and the capabilities of communications and IT systems used during an event. Furthermore, industry best practices[7] state that an organization should provide contingency training to users consistent with their assigned roles and responsibilities.

This occurred because Postal Service management did not fully develop a policy defining requirements for managing FWGA plans. Without annual continuity program training, Postal Service personnel may not have the skills required to support essential functions during a continuity event.

During our audit, Postal Service management took corrective action and started COOP training for personnel with FWGA responsibilities. For example, on September 29, 2016, two individuals completed the Federal Emergency Management Agency's COOP Awareness Course training.

[7] NIST Special Publication 800-53A r4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans*, December 18, 2014.

Recommendations

We recommend management develop and implement a policy, which includes annual reviews, updates, and testing for managing the FWA plans based on federal directives and industry best practices.

We recommend the vice president, Information Technology:

1. Develop and implement a policy, which includes annual reviews, updates, and testing for managing the Functional Workgroup Annex plans based on federal directives and industry best practices.

2. Require annual training for all personnel with Functional Workgroup Annex responsibilities in accordance with requirements outlined in Federal Continuity Directive 1.

Management's Comments

Management generally agreed with the findings and recommendations in the report and stated that they have begun to take corrective action.

Regarding recommendation 1, management will develop and distribute a policy across IT and the impacted sites. The policy will include the process for annually reviewing, updating, and testing COOP/FWGA plans. Managers throughout the Postal Service will discuss the decision to use federal directives as the standard to determine whether conforming to these directives is mandatory or voluntary. Management plans to develop and distribute the policy by September 30, 2017.

Regarding recommendation 2, management will train personnel who have FWGA responsibilities. However, managers throughout the Postal Service will discuss the decision to use the requirements outlined in the Federal Continuity Directive 1 to determine whether conforming to this directive is mandatory or voluntary. Management plans to have this completed by September 30, 2017.

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

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendations in the report and the corrective action proposed should resolve the issues identified.

Concerning both recommendations, it is the OIG's position that the Postal Service is required to follow all of the federal directives mentioned in the report.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action(s) are completed. No recommendations should be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation(s) can be closed.

Appendices

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

Appendix A: Additional Information

Our objective was to determine whether the Postal Service's IT division has viable FWGA capabilities to support essential business functions.

Background

The Postal Service is the center of a $1.4 trillion mailing industry that employs more than 7.5 million people. The Postal Service uses one of the world's largest computer networks — linking nearly 32,000 facilities and making possible communication among thousands of employees and hundreds of systems for the efficient processing and delivery of mail to everyone in the U.S. and its territories. To meet its mail delivery mandate, the Postal Service developed an overarching COOP plan to ensure that essential business functions continue when there is a disruption of normal operations.

Continuity planning is an accepted good business practice. Current threats such as acts of nature, accidents, technological emergencies, and military or terrorist-related incidents have increased the need for robust continuity capabilities and planning that enable organizations to continue their essential functions across a broad spectrum of emergencies.

The evolution of the COOP plan began in 1988 with an executive order[8] requiring the head of each federal agency to ensure the continuity of essential functions in any national security emergency. In 1998 and 2007, presidential directives[9] were issued to enhance this requirement by mandating a comprehensive and effective national continuity capability. The DHS, in coordination with interagency partners, developed FCDs 1 and 2 to help government agencies develop and implement COOP plans. FCD 1 provides direction for developing continuity plans and programs, while FCD 2 implements the requirements of FCD 1 and provides guidance for validating and updating an agency's essential functions.

In July 2016, PPD 40 was issued to require the inclusion of IT systems, processes, and resources into COOP plans. This directive requires the identification and inclusion of all essential IT systems in COOP planning. Additionally, Handbook AS-805[10] requires each installation head to implement and manage COOP plans for their facility or organization. Facilities include, but are not limited to, computer service centers, mail processing facilities, and other postal installations.

Objective, Scope, and Methodology

Our objective was to determine whether the Postal Service's IT division has viable FWGA capabilities to support essential business functions.

The scope of our audit was the IT FWGA plans from the following [redacted] Postal Service locations: the [redacted] [redacted] Centers, the [redacted] Center, and the [redacted] Centers.

We compared FWGAs at these locations to see if they adhered to federal requirements, Postal Service policies, and best practices for supporting the Postal Service's essential business functions. We also interviewed Postal Service personnel responsible for executing the FWGAs.

We requested training records to determine if Postal Service management trained personnel with FWGA responsibilities. In addition, we interviewed key officials regarding the training program; and training topics, policies, and practices.

We conducted this performance audit from September 2016 through March 2017, in accordance with generally accepted government auditing standards and included such tests of internal controls, as we considered necessary under the circumstances.

[8] Executive Order 12656, November 18, 1988.
[9] Presidential Decision Directive 67, October 21, 1988, and Homeland Security Presidential Directive 20/National Security Presidential Directive 51, May 9, 2007.
[10] Handbook AS-805, *Information Security,* Section 2-2.15, November 2016.

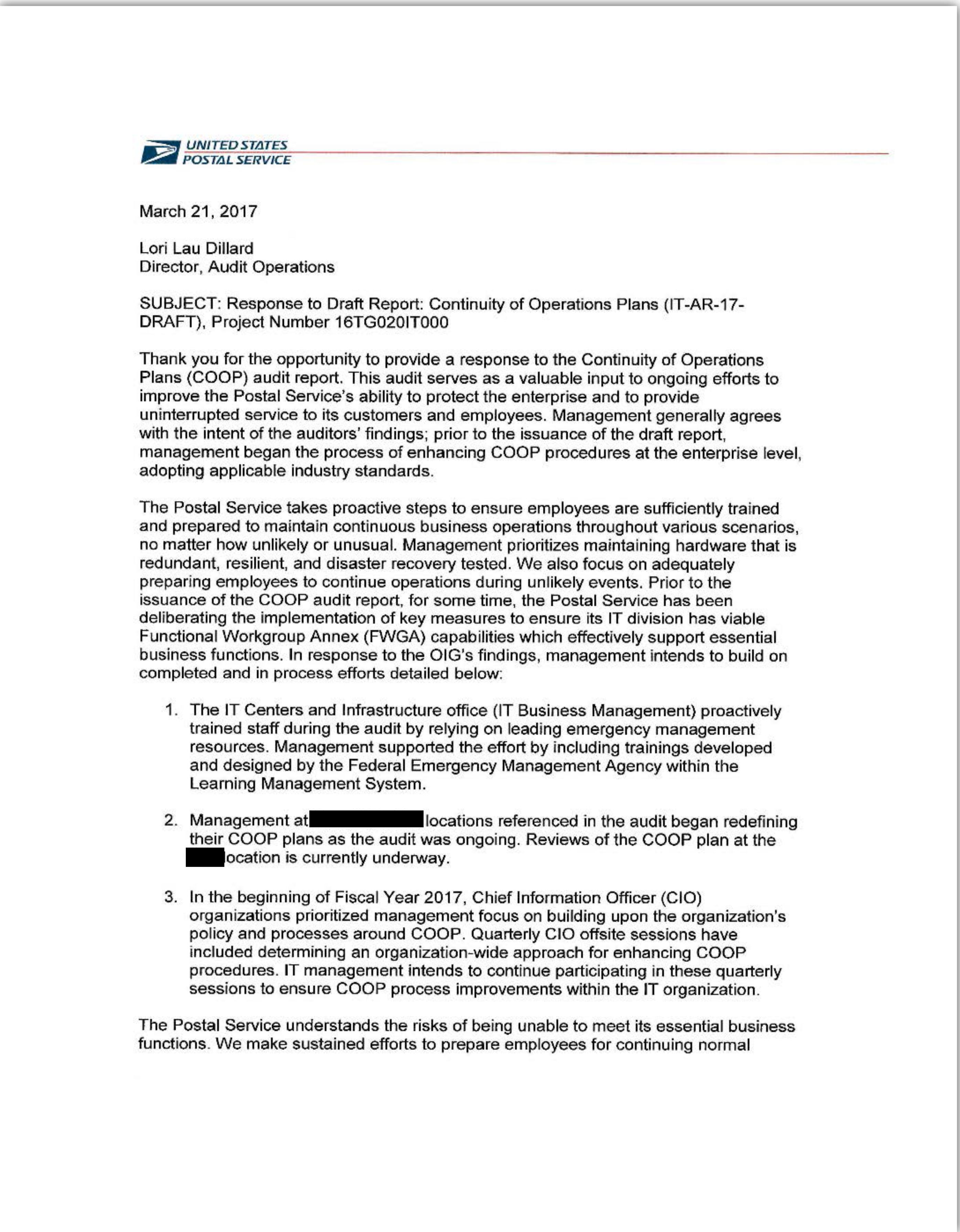
Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on March 2, 2017, 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.

Highlights
Table of Contents
Findings
Recommendations
Appendices

Appendix B: Management's Comments



UNITED STATES POSTAL SERVICE

March 21, 2017

Lori Lau Dillard
Director, Audit Operations

SUBJECT: Response to Draft Report: Continuity of Operations Plans (IT-AR-17-DRAFT), Project Number 16TG020IT000

Thank you for the opportunity to provide a response to the Continuity of Operations Plans (COOP) audit report. This audit serves as a valuable input to ongoing efforts to improve the Postal Service's ability to protect the enterprise and to provide uninterrupted service to its customers and employees. Management generally agrees with the intent of the auditors' findings; prior to the issuance of the draft report, management began the process of enhancing COOP procedures at the enterprise level, adopting applicable industry standards.

The Postal Service takes proactive steps to ensure employees are sufficiently trained and prepared to maintain continuous business operations throughout various scenarios, no matter how unlikely or unusual. Management prioritizes maintaining hardware that is redundant, resilient, and disaster recovery tested. We also focus on adequately preparing employees to continue operations during unlikely events. Prior to the issuance of the COOP audit report, for some time, the Postal Service has been deliberating the implementation of key measures to ensure its IT division has viable Functional Workgroup Annex (FWGA) capabilities which effectively support essential business functions. In response to the OIG's findings, management intends to build on completed and in process efforts detailed below:

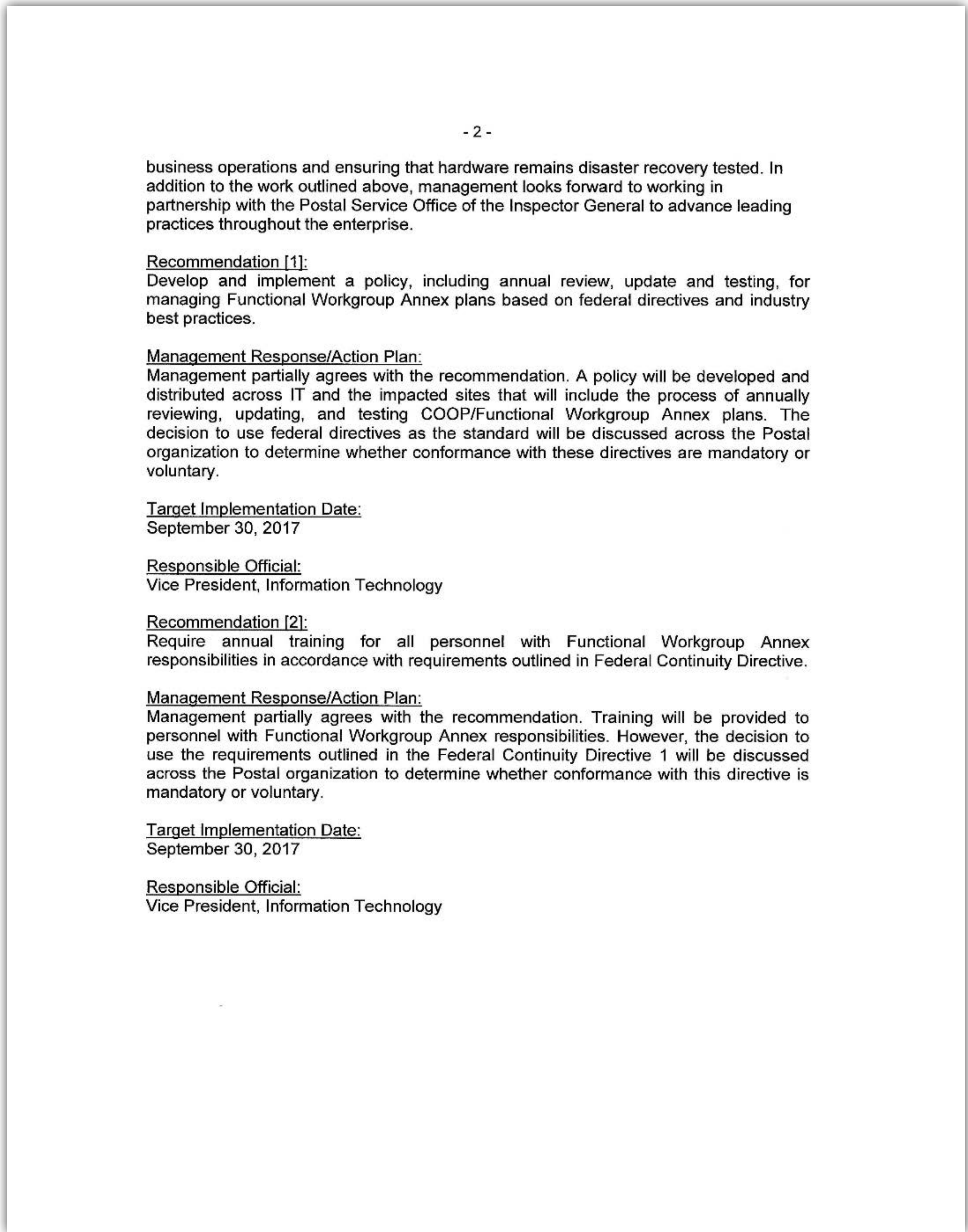
1. The IT Centers and Infrastructure office (IT Business Management) proactively trained staff during the audit by relying on leading emergency management resources. Management supported the effort by including trainings developed and designed by the Federal Emergency Management Agency within the Learning Management System.

2. Management at [redacted] locations referenced in the audit began redefining their COOP plans as the audit was ongoing. Reviews of the COOP plan at the [redacted] ocation is currently underway.

3. In the beginning of Fiscal Year 2017, Chief Information Officer (CIO) organizations prioritized management focus on building upon the organization's policy and processes around COOP. Quarterly CIO offsite sessions have included determining an organization-wide approach for enhancing COOP procedures. IT management intends to continue participating in these quarterly sessions to ensure COOP process improvements within the IT organization.

The Postal Service understands the risks of being unable to meet its essential business functions. We make sustained efforts to prepare employees for continuing normal

Highlights
Table of Contents
Findings
Recommendations
Appendices



business operations and ensuring that hardware remains disaster recovery tested. In addition to the work outlined above, management looks forward to working in partnership with the Postal Service Office of the Inspector General to advance leading practices throughout the enterprise.

Recommendation [1]:
Develop and implement a policy, including annual review, update and testing, for managing Functional Workgroup Annex plans based on federal directives and industry best practices.

Management Response/Action Plan:
Management partially agrees with the recommendation. A policy will be developed and distributed across IT and the impacted sites that will include the process of annually reviewing, updating, and testing COOP/Functional Workgroup Annex plans. The decision to use federal directives as the standard will be discussed across the Postal organization to determine whether conformance with these directives are mandatory or voluntary.

Target Implementation Date:
September 30, 2017

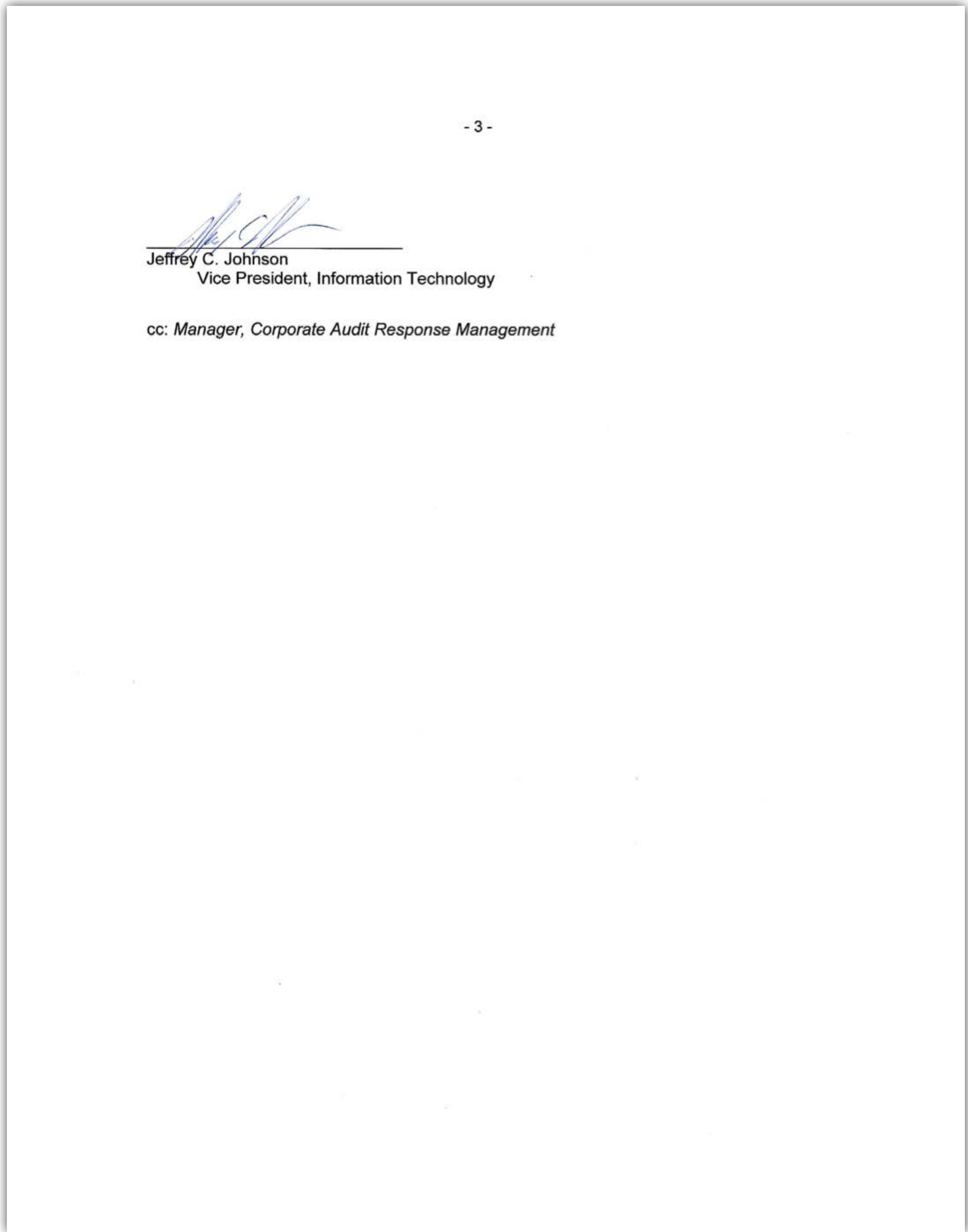
Responsible Official:
Vice President, Information Technology

Recommendation [2]:
Require annual training for all personnel with Functional Workgroup Annex responsibilities in accordance with requirements outlined in Federal Continuity Directive.

Management Response/Action Plan:
Management partially agrees with the recommendation. Training will be provided to personnel with Functional Workgroup Annex responsibilities. However, the decision to use the requirements outlined in the Federal Continuity Directive 1 will be discussed across the Postal organization to determine whether conformance with this directive is mandatory or voluntary.

Target Implementation Date:
September 30, 2017

Responsible Official:
Vice President, Information Technology



- 3 -

Jeffrey C. Johnson
Vice President, Information Technology

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