OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Engineering Systems and Network Operations Disaster Recovery Plan – [redacted]

Audit Report

September 24, 2013

Report Number IT-AR-13-007

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

September 24, 2013

Engineering Systems and Network Operations Disaster Recovery Plan – [redacted]

Report Number IT-AR-13-007

BACKGROUND:

U.S. Postal Service policy requires management to develop and test disaster recovery plans (DRPs) and perform business or infrastructure impact assessments for all applications. These plans assist in relocating and restoring applications at an alternative location following a disaster. The alternative location should be far enough from the main site so it is not affected by the same disaster. The impact assessments assist management in prioritizing the site's disaster recovery strategies.

In addition, the Continuity of Operations Plan provides for sustaining mission essential functions at an alternative site. Management supports 71 applications at the [redacted] and at sites nationwide.

Our objective was to determine whether the [redacted] has a DRP and whether the plan complies with Postal Service policies, industry standards, and best practices.

WHAT THE OIG FOUND:

Engineering Systems and Network Operations management did not establish or periodically test a DRP for the [redacted] that prioritized the applications that should be restored or described how those prioritized applications could be restored. An outdated Continuity of Operations Plan listed alternative sites in case of a disaster; however, no plan exists that describes how those sites would become operational in a disaster. The primary alternative site is on the [redacted] and could be impacted by the same disaster. Management believed their recovery procedures for the primary site were a viable DRP. Without a plan and testing, Postal Service operations and its brand — valued at about $102.4 million — are at risk.

Further, business or infrastructure impact assessments were not completed or updated for 57 of the 71 supported applications. Without placing a priority on completing these assessments, management would not be able to develop an effective DRP. As a result of our audit, management created or updated 24 of 71 assessments and developed an action plan to complete the remaining 33 assessments.

WHAT THE OIG RECOMMENDED:

We recommended management create and test a DRP at an alternative site that is a sufficient distance from the [redacted] so that it will not be affected by the same disaster and to complete impact assessments for the supported applications.

Link to review the entire report

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 24, 2013

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

DAVID E. WILLIAMS, JR.
VICE PRESIDENT, NETWORK OPERATIONS

FROM: John E. Cihota
Deputy Assistant Inspector General
for Financial and Systems Accountability

SUBJECT: Audit Report – Engineering Systems and Network Operations Disaster Recovery Plan – [redacted] (Report Number IT-AR-13-007)

This report presents the results of our audit of the Engineering Systems and Network Operations Disaster Recovery Plan at the [redacted] (Project Number 13BG002IT000).

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

Attachment

cc: Corporate Audit and Response Management

TABLE OF CONTENTS

Introduction

This report presents the results of our self-initiated audit of the Engineering Systems and Network Operations Disaster Recovery Plan (DRP) – [redacted] (Project Number 13BG002IT000). Our objective was to determine whether Engineering Systems and Network Operations at the [redacted] has a DRP and whether the DRP complies with U.S. Postal Service policy, industry standards,[2] and best practices.[3] See Appendix A for additional information about this audit.

Postal Service policy requires all major information technology (IT) sites and organizations that use or support information resources[4] in the Postal Service to develop a DRP. The DRP identifies key personnel and priority procedures for relocating information systems operations to an alternative location following a major system disruption with long-term effects. A DRP is also an information system-focused plan for restoring the target system, applications, or computer facility infrastructure at an alternative site after a disaster. Best practices[5] and industry standards[6] suggest the alternative site be located far enough away from the primary site to reduce the likelihood of being affected by the same disaster. In addition, routine DRP testing helps assure an orderly transition to the alternative site. Postal Service policy tasks the installation head with developing, maintaining, and testing the DRP.

A Continuity of Operations Plan (COOP) provides guidance for sustaining an organization's mission essential functions at an alternative site and performing those functions for up to 30 days before returning to normal operations. The most recent COOP, prepared in 2010, lists [redacted].

Finally, Postal Service policy requires infrastructure impact assessments (IIAs) and business impact assessments (BIAs) to complete a DRP; determine the sensitivity[7] and criticality[8] of information infrastructure and applications, respectively; determine the appropriate security requirements needed to protect the resource; and assist management in prioritizing the recovery of these vital resources at the alternative site. DRP documentation is required for each application.

---

[1] [redacted]
[2] A mandatory requirement, code of practice or specification approved by a recognized external standards organization.
[3] A proven activity or process that has been successfully used by multiple enterprises.
[4] All Postal Service information assets, including information systems, hardware, software, data, applications, telecommunications networks, computer-controlled mail processing equipment, and related resources and the information they contain.
[5] Gartner, G00155016, *Toolkit Decision Framework: Best Data Center Locations for Disaster Recovery,* dated March 2008.
[6] National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, Section 3.4.3, dated May 2010.
[7] Sensitivity determines the need to protect the confidentiality and integrity of the information.
[8] Criticality determines the need for continuous availability of the information.

Engineering Systems and Network Operations at the [redacted] are system sponsors for 71 applications, 16 of which are at the [redacted] as noted in Appendix C, Table 1. The remaining 55 applications reside at other field units such as [redacted].

Conclusion

Engineering Systems and Network Operations' management did not have a DRP for the [redacted] or the planning documents to restore those specific applications on the [redacted] in the event of a disaster. Management also did not prepare BIAs or IIAs for 10 of the 16 applications at the [redacted] and six of the 55 applications hosted at other installations. For example, management did not create an IIA or a DRP for the Remote Computer Reader to determine how, when or even if the application should be recovered at an alternative site. Furthermore, BIAs or IIAs for 17 applications must be updated.[9] Without a BIA or IIA or timely recertification,[10] an effective DRP for the [redacted] cannot be developed. Without a DRP, a catastrophic event could place Postal Service operations, brand, and services — valued at about $102.4 million — at risk.[11]

Preparation and Testing of Disaster Recovery Plans

Engineering Systems and Network Operations management did not have a DRP for the [redacted] that prioritized the applications that should be restored or a viable disaster recovery testing program.[12] Additionally, management did not have all the planning documents that describe how to restore those prioritized applications at the [redacted]. Finally, management did not have DRPs describing how the secondary alternative site in [redacted] as described in the COOP, would become operational. Postal Service policy[13] requires management to prepare a DRP for all applications and base testing frequency on the level of criticality.

A facility security report[14] prepared in 2011 for the U.S. Postal Inspection Service reported completion of facility recovery plans, workgroup recovery plans, and application DRP. However, the IT Artifacts Library[15] and the Enterprise Information Repository (EIR) showed that no DRPs were completed for applications at [redacted] This occurred because management believed their recovery and back-up procedures for the primary COOP site constituted a viable DRP. While these procedures may

[9] As a result of our audit, management created or updated 24 assessments.
[10] Handbook AS-805, *Information Security,* Section 3.3-1, dated May 2013, states, "The BIA must be updated periodically as required (every 1, 3, or 5 years depending on its sensitivity designation), whenever a significant change is made to the information resource, or whenever the certification and accreditation (C&A) process is re-initiated."
[11] IT assets are at risk of disruption longer than necessary because a DRP (and all its supporting BIAs and IIAs) has not been developed and tested.
[12] Because a DRP did not exist, the U.S. Postal Service Office of Inspector General (OIG) could not perform testing.
[13] Handbook AS-805, Section 12.5.
[14] 2011 *Vulnerability Risk Assessment Tool* (VRAT) prepared for Engineering.
[15] A document repository that contains finalized project deliverables for all technology solutions.

protect against data loss in non-disaster conditions, they alone should not be considered a viable DRP.

According to the EIR,[16] management performed recovery testing for one of the 16 applications, the Electronic Maintenance Activity Reporting and Scheduling (eMARS) system,[17] in 2009. See Appendix C, Table 1 for a listing of the 16 applications at the [redacted].

During our review, management developed recovery and backup procedures [redacted] as a primary alternative site. However, this [redacted] and could be impacted by the same disaster.

Insufficient disaster recovery planning that does not include moving systems and application recovery to an alternative location outside of the [redacted] and testing the DRP commensurate with the criticality and sensitivity of the application places the Postal Service's operations, brand, and services at risk. Our analysis estimates the risk to be about $102.4 million. See Appendix B for details on the calculation of other impact.

Business and Infrastructure Impact Assessments

System sponsors[19] within Engineering Systems and Network Operations did not always ensure completion of BIAs or IIAs for their respective applications. These sponsors must complete the EIR registration; request Corporate Information Security Office (CISO) collaboration in completing the impact assessments; and document application characteristics such as production environment, high-level network architectural diagrams, and sensitive data elements needed to proceed with the impact assessment. Management did not prepare BIAs or IIAs for 10 of 16 applications at the [redacted] and for six of the 55 Engineering-supported applications at other locations. Appendix C, Table 1 identifies the 16 resident applications; Appendix E, Table 3 identifies the status of the 10 resident applications for which an assessment has not been prepared; and Appendix E, Table 4 identifies the status of the six non-resident applications for which an assessment has not been prepared. In addition, management did not timely update 17 applications at [redacted] and other locations as shown in Appendix F, Table 5. See Appendix D, Table 2 for a listing of 38 completed BIAs.

Postal Service policy requires management to prepare a BIA or IIA for all applications to determine the level of sensitivity and criticality and the information security requirements to assist management in prioritizing the recovery of IT services. Management, however, did not set the proper priority to complete the required BIAs or IIAs and did not stress

[16] The Postal Service's database of record that maintains information about existing Postal Service applications, toolsets, and data.
[17] eMARS provides inventory management for parts and labor for all plants, as well as reporting and alert capabilities related to inventory management.
[18] For the eMARS system.
[19] Business managers with oversight (funding, development, production, and maintenance) of the applications.

their importance. Without initial or updated BIAs or IIAs for applications, management would be significantly hampered in developing an effective DRP for continuing operations of critical applications at an alternative recovery site.

Corrective Actions Taken

Since December 4, 2012, which was during our audit, management initiated corrective actions to create or update 24 BIAs. Thirty-eight BIAs (53.5 percent) are considered complete and current for the 71 supported applications.[20] The BIAs or IIAs for the remaining 33 applications are in various stages of completion. See Appendix E, Tables 3 and 4 and Appendix F, Table 5 for a listing of these applications.

Recommendations

We recommend the vice president, Engineering Systems, in coordination with the vice president, Network Operations:

1. Establish, implement, and test a disaster recovery plan for Engineering Systems and Network Operations in [redacted] that is commensurate with the sensitivity of data, available resources, and level of risk for the applications and incorporates an appropriate alternative site located far enough away from the [redacted] that it will not be affected by the same disaster.

2. Timely complete or update, as appropriate, business impact or infrastructure impact assessments for all applications supported by Engineering Systems.

Management's Comments

Management agreed with our findings and recommendation 2 and partially agreed with recommendation 1.

Addressing recommendation 1, management stated that the recommendation does not take into consideration that the identified systems are off-line and have no impact on day-to-day processing of mail. However, management intends to create and conduct limited testing of the DRP based on updated BIAs for each of the applications. Furthermore Network Operations will use the [redacted] as their disaster recovery site for the majority of the application and systems due to the high cost of implementation at alternative testing locations. The target implementation date is May 23, 2014.

Regarding recommendation 2, management will complete or update, as appropriate, BIAs and IIAs for applications designated as critical or business-controlled. The target implementation date is December 20, 2013.

Management also disagreed with the $102.4 million of other impact because they believe the OIG's analysis and underlying methodology to calculate financial impacts

[20] We did not assess the accuracy or completeness of the BIAs. We may do this in a future review.

was flawed and based on one individual's opinion. Further, management claimed the OIG never requested a team assessment of the projected recovery time.

See Appendix G for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report.

Regarding recommendation 1, management asserted that the recommendation did not take into consideration that the identified systems had no impact on mail processing. However, this assertion is premature until a DRP based on completed BIAs and IIAs is developed.

To address management's disagreement regarding calculation of the other impact and the recovery period, the OIG worked with management's designated subject matter expert to calculate other impact and management had ample opportunity during the review to complete additional risk assessments that could further refine residual risk and the time needed to recover operations from a catastrophic event. Management did not provide any support that they could recover the critical applications hosted or supported at the [redacted] within 1 day.

The OIG considers both 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.

Appendix A: Additional Information

Background

Postal Service policy[21] and generally accepted industry standards[22] require all major IT sites to develop a DRP. A DRP is an information system-focused plan designed to restore the operability of the target system, applications, or computer facility infrastructure at an alternative site after an emergency. The DRP identifies key personnel and priority procedures for relocating information systems operations to an alternative location and is activated after major system disruptions with long-term effects.

Postal Service policy tasks the installation head to develop, maintain, and test the DRP. The CISO Business Continuance Management group, the Information System Security officer, and the application owner jointly determine the criticality designation by considering the impact of the information resource on numerous effects. Finally, each application must have DRP documentation stored in the IT Artifact Library.

Objective, Scope, and Methodology

Our objective was to determine whether Engineering Systems and Network Operations management at the [redacted] has a DRP and whether the plan complies with Postal Service policies, industry standards, and best practices. We limited our audit to the applications maintained and supported by Engineering Systems and Network Operations at the [redacted].

To accomplish this objective, we interviewed on-site [redacted] program managers and administrators to determine who was responsible for network configurations, application data, and building services restoration and priorities for disaster recovery. We corroborated DRP and BIA and IIA responsibilities for the [redacted] with the Postal Service's CISO and Business Continuity Planning and Infrastructure Relationship management. We determined the status of BIA and IIA based on documentation in the IT Artifacts Library and EIR and from management's assertions for all 71 Engineering Systems-supported applications. Finally, we reviewed the 2011 VRAT[23] responses completed by the former Engineering Systems Installation head and the 2010 COOP.

We conducted this performance audit from October 2012 through September 2013 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

[21] Handbook AS-805, Section 12.
[22] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*.
[23] A questionnaire used by the Inspection Service to assess facility security.

our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on August 19, 2013 and included their comments where appropriate.

We assessed the reliability of the transactions data from the eMARS system by interviewing the Solutions Center Business Project leader. Specifically, we discussed with an eMARS expert the transaction types, which transactions would require manual reentry, and how much time would be needed to enter the transactions manually if eMars was not functional for determining other impact. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

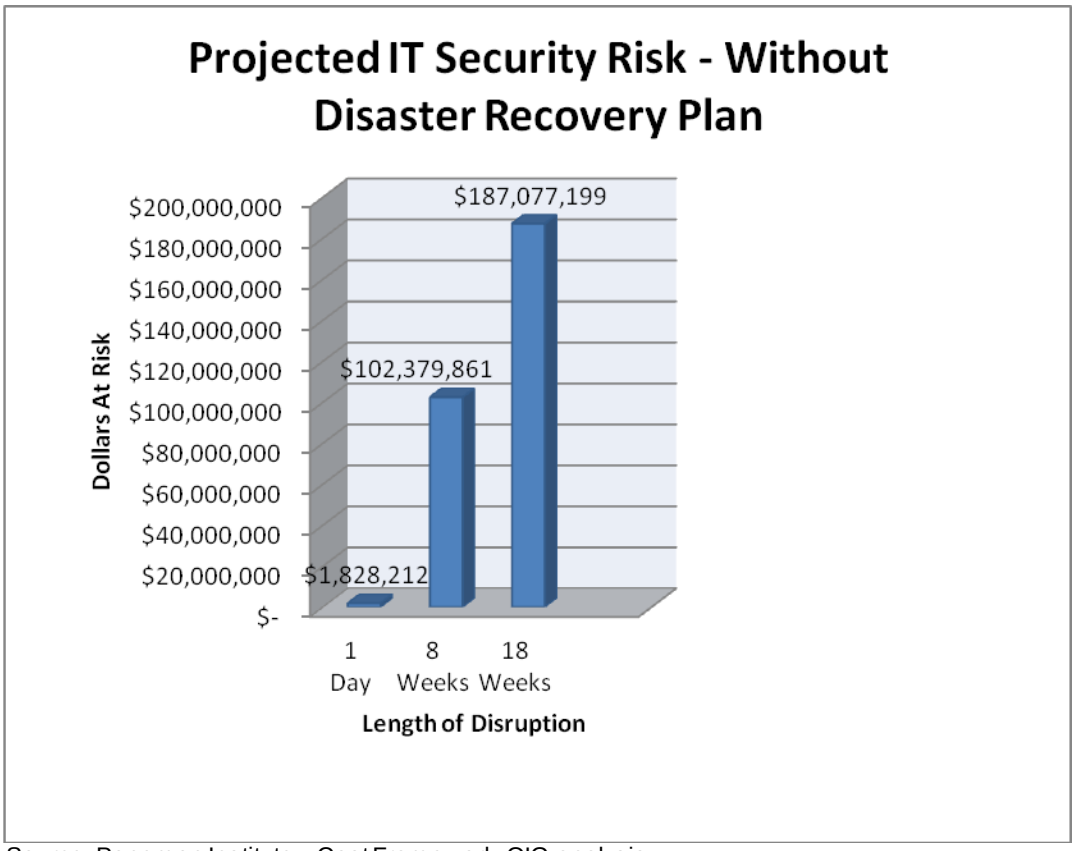
The OIG did not identify any prior audits or reviews related to the objective of this audit.

Appendix B: Other Impact

Recommendation	Impact Category	Amount
1	IT Security[24]	$102,379,861

Computer software, networks, and data are vulnerable or at risk of loss due to disruption of critical Postal Service operations and services longer than necessary because a DRP was not available and tested. Figure 1 shows the risk associated with three recovery periods.

Figure 1. Projected IT Security Risk – Without Disaster Recovery Plan



Source: Ponemon Institute – Cost Framework, OIG analysis.

We calculated the other impact of $102,379,861 because a DRP (and supporting BIAs and IIAs) was not available and tested for the 16 applications at the [redacted]. In determining the risk associated with the loss of operations at the [redacted], we selected the eMARS application as a representative system because its production servers are at the [redacted] and it is used throughout the Postal Service.

[24] Computer software, networks, and data that are vulnerable or at risk of loss because of fraud, inappropriate or unauthorized disclosure of sensitive data, or disruption of critical Postal Service operations and services.

Through interviews with the eMARS Solutions Center Business project leader and manager — designated by management as the point of contact and subject matter expert for eMARS — we determined that a full functional recovery of the system at an alternative location outside the [redacted] without a DRP may take 8 to 18 weeks. However, the 18 weeks represents the eMARS manager's worst case scenario, while 8 weeks would be a more reasonable recovery period.

The vice president, Network Operations, stated that, in his opinion, the best case scenario should be less than 1 day because he could quickly provide the funding and resources needed to restore this application. No information was provided to discount the 18-week recovery period nor was any support provided for the less than 1-day recovery period. We were unable to find any comparable authoritative sources for a system that provided an 'average' recovery period, so we used the 8-week recovery period, as it represents a reasonable recovery period (in an environment without an established or tested DRP and all associated BIAs and IIAs completed) and the eMARS manager considers it to be the most likely outcome. As a result of this audit, management asserted that they have taken steps to mitigate the potential loss of functionality caused by a disaster by pursuing logistical support and equipment so the Postal Service can use a [redacted] as an alternative to the facility at [redacted]

We worked with the eMARS manager to obtain eMARS transactional and labor cost data to calculate the cost of not having the eMARS system available. Using the cost framework published in a white paper[25] by the Ponemon Institute, we conservatively calculated the risk associated with the loss of functionality of the [redacted] for one of the 71 supported applications as follows:

- To determine direct costs[26] related to the loss of eMARS system functionality, we worked closely with management to develop the factors for this calculation. The weekly manual labor cost to process maintenance and order parts is about $12.8 million, or $102,379,861 for the 8-week period. We based the calculation on average required weekly labor hours (252,466[27]) and the average hourly rate for a maintenance worker ($50.69).[28]

- We did not include a probability factor in our calculations because, according to best practices, "when the consequences of a risk are severe, probability is misleading in assessing the risk's importance. A risk with catastrophic consequences is important, even if it is considered unlikely."[29]

[25] Ponemon Institute, *Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact on Infrastructure Vulnerability,* March 2011.
[26] An expense that can be assigned to or identified with a specific activity (Business Dictionary.com).
[27] A rounded number of hours that is the average required weekly labor for processing transactions manually (1,770,538 transactions at 8.55556 minutes per transaction divided into 60 minutes per hour).
[28] Hourly wages rate given by management.
[29] Gartner: *Use the Risk Pyramid to Assess Risk in Five Minutes,* G00210317, May 2, 2011. Gartner, Inc. is the world's leading IT research and advisory company that delivers technology-related insight to their clients.

We did not include the loss of [redacted] support for the other engineering applications in the event of a disaster in the other impact calculation, although this would put additional data at risk of loss. Our other impact calculation represents one measure of potential exposure to the Postal Service in the event of a disaster at the [redacted] however, this should not be considered the maximum exposure or risk to the Postal Service.

Appendix C: Applications Hosted at the [redacted]

Sixteen business and infrastructure applications are hosted at the [redacted], as shown in Table 1.

Table 1. Applications Hosted at the [redacted]

	Application Name
1	Automated Parcel Bundle Sorter Image Controller
2	eMARS
3	Engineering Intranet
4	Flat Identification Code Sort
5	Forwarding Control System
6	Integrated Data System
7	Intelligent Mail Enterprise[30]
8	KONFIG® Configuration Management II Enterprise Configuration Management System
9	Mail Processing Infrastructure Workstation
10	Next Generation Transaction Concentrator
11	Powered Industrial Vehicle Management System
12	Remote Computer Reader
13	Remote Directory File Monitor
14	TeamTrack
15	Technology Management Office System (TMOS)[31]
16	Web Enabled Automated Package Processing System (APPS) Processing Results Log Message (PRLM) Analysis Tool

Sources: Applications program managers and system administrator interviews and the EIR.

[redacted]

Appendix D: Impact Assessments Completed for Engineering-Supported Applications

Management has completed BIAs for 38 of 71 supported applications (Table 2). The remaining 33 applications include 16 applications that require an initial assessment (Appendix E, Table 3 and Table 4) and 17 applications that need updated assessments (Appendix E, Table 5). The CISO included some applications in this list that are in the development stage since policy[32] requires a completed and approved BIA as part of the C&A package[33] before that development application moves into production. We will update the category in any subsequent reviews or audits.

Completion of the BIAs or IIAs assists management in restoring the most essential applications in the proper order. Many of these applications are essential for mail processing plant operations and moving the mail.

Table 2. Completed Impact Assessments

Index Number	Application Name	Abbreviation or Acronym	Completion Date[34]
1342	Transportation Optimization Plan and Scheduler	TOPS	2/11/2013
1351	Logistics Contract Management System	LCMS	2/1/2013
1360	Yard Management System	YMS	4/11/2013
2693	E-Maintenance Activity reporting and Scheduling	eMARS	4/22/2013
2398	Concentration and Convoy Tracking	CONCON	2/1/2013
3062	Rail Management Information System	RMIS	7/19/2013
3075	Transportation Routing Information Panel System	TRIPS	7/19/2013
3108	Surface Air Management System	S-AMS	5/15/2012
3137	Postal Automated Redirection System	PARS	2/20/2013
3238	Intelligent Mail Data Acquisition	IMDAS	4/24/2013
3267	National Traffic Management System	NTMS	4/29/2013
3466	E-Facilities Management System	EFMS	4/27/2012
3520	Biohazard Detection System Detection System National Controller	BDSNAT	4/27/2012
3683	Surface Air Support System Mobile	SASS Mobile	3/10/2013
3740	International Document Portal	IDP	2/20/2013
3797	External Label List System	ELLS	8/13/2012
3849	Network Operations - Help	NOMSHELP	7/18/2013
3940	Mail and Image Reporting System	MIRS	4/14/2011
3941	National Air and Space System Web	NASSWEB	3/14/2013
3943	Mobile Repossession and Reassignment	MRR	6/28/2013
4003	Directory Services	DIRSERV	2/26/2012

[32] Handbook AS-805.
[33] A formal security analysis and management approval process that assesses residual risk before the resource is put into production.
[34] Management initiated corrective actions to create or update 24 BIAs subsequent to the initiation of our audit on December 4, 2012.

Table 2. Completed Impact Assessments (Continued)

Index Number	Application Name	Abbreviation or Acronym	Completion Date
4102	Enterprise Energy Management System	EEMS	10/10/2012
4130	Global Business System	GBS	4/27/2012
4192	Lean Six Sigma Continuous Improvement Project Tracker	INSTANTIS	5/3/2013
4206	Intelligent Mail Enterprise	IME	12/20/2011
4212	Quick Test Professional	QTP	2/10/2012
4268	Technology Management Office System	TMOS	2/13/2013
4293	Electronic Parcel Locker Central Management System	ePLCMS	10/20/2011
4303	Plant Scanning System	PSS	3/7/2012
4308	Move To Competitive Registration System	MTCRS	1/31/2013
4317	Automated Parcel Bundle Sorter Image Controller	APBS-IC	4/9/2013
4327	Variance Modules	VM	1/24/2013
4336	Outbound Data Concentrator	ODC	8/23/2013
4350	Singulation Scan Induction Unit	SSIU	12/4/2012
4353	Inbound Custom Data Concentrator	IDC	5/3/2013
5029	ID Code Sorting Server	ICS-SERVER	1/3/2012
6186	Networks Intranet	NI	3/15/2013
None	Team Track	TEAM TRACK	6/13/2013

Source: CISO and Engineering Systems status as of July 19, 2013.

Appendix E: Impact Assessments Not Completed

As a result of our audit, Engineering Systems and Network Operations management are completing the initial assessment by following the BIA or IIA process for 10 business and infrastructure applications that were not completed and reside at the [redacted] KONFIG is a commercial off-the-shelf application and, along with the Engineering intranet, is waiting for Engineering Systems and CISO to determine the appropriate assessment needed. Also noted in management's comments are those applications slated for retirement or consolidation with another application.

Table 3. Impact Assessments Not Completed – [redacted]

Index Number	Application Name	Abbreviation or Acronym	Management Comment
3208	Flat ID Code Sort	FICS	In process
4168	Web Enabled APPS PRLM Analysis Tool	WEBAPAT	In signature process
4309	Mail Processing Infrastructure Workstation	MPIW	In process
4337	Next Generation Transaction Concentrator	NGTC	In process
6116	Remote Computer Reader	RCR	In process
None	KONFIG	KONFIG	In process
None	Remote Directory File Monitor	RDFM	To be consolidated with PARS
None	Forwarding Control System	FCS	To be consolidated with PARS
None	Engineering Intranet	ENGINEERING INTRANET	Awaiting determination
None	Integrated Data System	IDS	In process

Source: CISO and Engineering Systems status as of July 19, 2013.

Engineering Systems and Network Operations management are completing the initial assessment by either following the BIAs or IIA process for six business and infrastructure applications that were not completed and reside at sites other than the [redacted] (see Table 4).

Table 4. Impact Assessments Not Completed

[redacted]

Index Number	Application Name	Abbreviation or Acronym	Management Comment
2718	National Directory Support System	NDSS	In process
3074	Vehicle Tracking Analysis and Performance System	VTAPS	In retirement process
3837	Change of Address Reporting System	None	In signature process
4213	Service Test	SERVICE TEST	In retirement process
4241	Equipment Inventory Management System	EIMS	Consolidating with Remedy 7
4271	Inspection Service Toolkit	IS TOOLKIT	Pending scheduling, no current funding

Source: CISO and Engineering Systems status as of July 19, 2013.

Appendix F: Impact Assessments Requiring Update

BIAs and IIAs for 17 business and infrastructure applications supported by Engineering need to be updated.

Table 5. Impact Assessments Requiring Update

Index Number	Application Name	Abbreviation or Acronym	Completion Date	Management Comment
1339	Web Mail Condition Reporting System	WEB MCRS	3/17/2009	In process
1343	Distribution Table Maintenance System	DTMS	4/7/2009	In signature process
1344	Web Load Restraint Reporting System	WEBLRRS	6/9/2010	In retirement
1362	Web End-of-Run	WEBEOR	3/31/2009	In process
1373	Mail Processing Equipment (MPE) Watch	MPEWATCH	2/7/2006	In process
1395	Web Management Operating Data System	WEBMODS	2/4/2008	In process
2716	Web Enabled Service Standard Directory	WEB SSD	5/20/2009	In process
3221	Web Remote Encoding Center Operations Analysis Database System	WEBROADS	8/4/2009	In process
3236	Business Reply Mail Accounting System	BRMAS	4/6/2006	In process
3263	Deployment Scheduler	EDEPLOY	7/14/2009	In process
3311	Mail Processing Operating Plan System	MPOPS	10/15/2009	In process
3327	Statis Table Support System	STSS	3/4/2008	In process
3630	Powered Industrial Vehicle Management System	PIVMS	6/22/2006	In process
3636	Vehicle Information Transportation Analysis and Logistics Web	VITAL WEB	6/1/2008	In process
3696	Postal Automated Redirection System Database System	PADS	3/28/2006	To be consolidated with PARS
3730	Envelope Reflectance Meter III	ERM-III	3/16/2007	In process
3942	Surface Air Management System - Alaska	SAMS-ALASKA	5/19/2011	In process

Source: CISO and Engineering Systems status as of July 19, 2013.

Appendix G: Management's Comments

UNITED STATES POSTAL SERVICE

September 13, 2013

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Audit Report – Engineering Systems and Network Operations Disaster Recovery Plan – [redacted]
(Report Number IT-AR-13-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. The Postal Service considers disaster recovery plans a serious matter. This level of importance is evident by our ability to restore mail processing and delivery services after disaster events such as Super Storm Sandy. Since many of the applications, reviewed as part of this audit, are not considered mission critical to postal operations, the cost to replicate the servers in alternate locations are not justified.

We plan to continue to use the [redacted] as the primary disaster recovery site. We acknowledge the risks as outlined in the OIG report regarding the relative proximity of the buildings. However, both the [redacted] and the [redacted] have sufficient capabilities to handle most local disasters/events.

We disagree with the $102.4 million other impact risk. As discussed during prior meetings with the OIG, analysis and underlying methodology used as the basis to calculate financial impacts associated with this audit are flawed. Both the time to recover and the assumption that all data missed due to an outage would be manually input is not reasonable and is based on one individual's opinion. In addition, at no time during the 10-month long investigation, we were asked to provide a team assessment of projected recovery time.

The following is our response to the recommendations contained in the report:

Recommendation 1:
Establish, implement, and test a disaster recovery plan for Engineering Systems and Network Operations in [redacted] that is commensurate with the sensitivity of data, available resources, and level of risk for the applications and incorporates an appropriate alternative site located far enough away from the [redacted] that it will not be affected by the same disaster.

Management Response/Action Plan:
The management partially agrees with this recommendation. The recommendation does not take into consideration that the identified systems are off-line and have no impact on day-to-day processing of mail. Therefore, we will create and conduct limited testing of the Disaster Recovery Plan's based on updated Business Impact Assessments (BIA) for each of the applications. (Sensitivity, criticality, and recovery time objectives.) Network Operations will use the [redacted] as their disaster recovery site for the majority of the applications and systems due to the high cost of implementing at alternate testing locations.

Target Implementation Date:
May 23, 2014

Responsible Engineering Systems Official:
Manager, Engineering Software Management

Responsible Network Operations Official:
Manager, Maintenance Planning and Support

Recommendation 2:
Timely complete or update, as appropriate, business impact or Infrastructure Impact Assessments (IIA) for all applications supported by Engineering Systems.

Management Response/Action Plan:
The management agrees with this recommendation and will complete and/or update, as appropriate, BIAs and IIAs for all applications designated as critical or business-controlled.

Target Implementation Date:
December 20, 2013

Responsible Engineering Systems Official:
Manager, Engineering Software Management

Responsible Network Operations Official:
Manager, Maintenance Planning and Support

FOIA Statement:
The subject report and this response contain information related to disaster recovery, if released, could be exploited and cause substantial harm to the U.S. Postal Service. The Manager, Corporate Information Security will determine what portions of the report should be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act.

If you have any questions or comments regarding this response, please contact Bruce D. Dickinson at (703) 280-7649, John F. Keegan at (703) 280-7230, or Thomas D. Duchesne at (703) 280-7501.

Michael J. Amato
Vice President, Engineering Systems

David E. Williams
Vice President, Network Operations

cc: Megan J. Brennan
Ellis a. Burgoyne
John T. Edgar
Charles L. McGann
Corporate Audit and Response Management