



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Highlights

Sufficient personnel resources were not devoted to cybersecurity functions.

Background

Cybersecurity is the body of processes, practices, and technology designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. In November 2014, the U.S. Postal Service announced a significant cyber intrusion had occurred that compromised large amounts of data. This report addresses cybersecurity functions of the Postal Service at the time the intrusion was identified. Our objective was to determine whether the Postal Service's structure, operations, and resourcing of cybersecurity functions aligned with industry best practices to support the enterprise. We examined Corporate Information Security Office processes and other Postal Service cybersecurity functions.

What The OIG Found

Management has taken significant positive action since the cyber intrusion based on input from business and industry experts. Enhancing the cybersecurity of the organization will be a long and challenging effort. Specifically, the Postal Service has additional work to do to align its structure, operations, and resourcing of cybersecurity functions with industry best practices.

At the time the intrusion was identified, Postal Service leadership had not emphasized cybersecurity, as evidenced by its undertrained employees, lack of accountability for risk acceptance decisions, ineffective collaboration among cybersecurity teams, and continued operation of unsupported systems. Because leadership had not established an effective cybersecurity culture to support business operations and drive employee behaviors, employees were not prepared to recognize and appropriately respond to cybersecurity risks.

Additionally, staffing and support for cybersecurity functions provided for basic operations and compliance with legal and industry requirements. However, it did not provide for effective operations, including skilled, 24-hour-a-day incident response and analysis, effective vulnerability management, or role-based training. This is because sufficient personnel resources were not devoted to cybersecurity functions. Without adequate resources, the Postal Service did not have the cybersecurity capabilities to prevent, detect, or respond to advanced threats.

Finally, the Postal Service lacked a comprehensive risk-based cybersecurity strategy. Consequently, it was not prepared for the rapidly changing threat landscape nor could it effectively manage the corresponding risks.

The Postal Service has already begun taking action to address the strengthening of cybersecurity functions. These include an extensive joint forensic investigation with subject matter experts and initiated implementation of enhanced monitoring capabilities and procurement of 24-hour security operations center services. Existing plans for improvements in access management, intrusion detection, and authentication processes have been accelerated. In addition, the postmaster general appointed a vice president-level chief information security officer.

What The OIG Recommended

We recommended management develop, execute, and communicate a strategy to embed a strong cybersecurity culture into daily operations and adequately staff and resource cybersecurity operations. We also recommended management implement a plan for the organization to exercise the appropriate governance and incident response.

Transmittal Letter

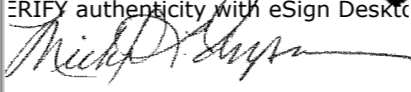


OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 17, 2015

MEMORANDUM FOR: RANDY S. MISKANIC
ACTING CHIEF INFORMATION OFFICER
AND EXECUTIVE VICE PRESIDENT

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

E-Signed by Michael Thompson
VERIFY authenticity with eSign Desktop


FROM: Michael L. Thompson
Acting Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – U.S. Postal Service Cybersecurity Functions
(Report Number IT-AR-15-008)

This report presents the results of our audit of U.S. Postal Service Cybersecurity Functions (Project Number 15TG008IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Cover	
Highlights.....	1
Background.....	1
What The OIG Found.....	1
What The OIG Recommended	1
Transmittal Letter.....	2
Findings.....	4
Introduction	4
Conclusion	4
Cybersecurity Culture	4
Cybersecurity Staffing and Resourcing.....	8
Cybersecurity Strategy.....	11
Recommendations.....	14
Management’s Comments	15
Evaluation of Management’s Comments.....	15
Appendices.....	17
Appendix A: Additional Information	18
Background	18
Objective, Scope, and Methodology.....	18
Prior Audit Coverage	19
Appendix B: Cybersecurity Best Practices for Security Operations Centers.....	20
Appendix C: Cybersecurity Best Practices for Computer Incident Response Teams.....	21
Appendix D: Cybersecurity Best Practices for Vulnerability Management	22
Appendix E: Cybersecurity Best Practices for Telecommunication Network Operations Centers.....	23
Appendix F: Key Questions to Ask.....	24
Appendix G: References.....	25
Appendix H: Management’s Comments	27
Contact Information	40

Findings

Cybersecurity is the body of processes, practices, and technology designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

At the time the intrusion was identified, Postal Service leadership had not fostered a culture of effective cybersecurity across the enterprise.

Introduction

This report presents the results of our audit of U.S. Postal Service Cybersecurity Functions (Project Number 15TG008IT000). This was a self-initiated audit to determine whether the structure, operations, and resourcing of the Postal Service's cybersecurity functions align with best practices to support the enterprise. See [Appendix A](#) for additional information about this audit.

Cybersecurity is the body of processes, practices, and technology designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access. Within the Postal Service Chief Information Office (CIO), the Corporate Information Security Office (CISO) leads the defense and protection of the cybersecurity environment. At the time of our review, a manager of Corporate Information Security directed multiple teams, including the Computer Incident Response Team (CIRT). Within Information Technology (IT) Telecommunication Services, the Perimeter Security team provides support by managing several external vendors that provide primary Internet connectivity and monitor the Postal Service infrastructure's external cyber entry points.

In November 2014, the Postal Service disclosed a cyber intrusion had occurred. The Postal Service notified personnel that the personally identifiable information of over 800,000 current and former employees, 485,000 workers' compensation records, and the customer inquiry records of about 2.9 million customers had been compromised. The Postal Service worked closely with federal agencies, as well as private sector specialists, to investigate and remediate the cyber intrusion.

The Postal Service's infrastructure prior to the intrusion was designed to respond to cybersecurity threats with a defense concentrated on keeping individuals out of the network. This type of defense was commonly used before advanced persistent threats¹ were widely recognized and is currently considered ineffective when used on its own. Instead, to have effective cybersecurity, organizations need to incorporate multiple layers of prevention, detection, and response while maintaining resilient systems that enable the organization to operate while under attack and rapidly recover essential functions.²

Conclusion

Postal Service leadership had not fostered a culture³ of effective cybersecurity across the enterprise. Staffing and resources for cybersecurity functions focused heavily on complying with specific legal and industry requirements, leaving limited resources for systems that are not subject to these requirements. In addition, management had not integrated cybersecurity risks into a comprehensive cybersecurity strategy. While it has worked with business and industry experts to initiate significant positive action since the cyber intrusion of November 2014, the Postal Service could attain more effective cybersecurity operations by continuing efforts to re-align its structure, operations, and resources to better address operational risks and protect business operations.

Cybersecurity Culture

The Postal Service had not adequately emphasized cybersecurity responsibilities as an integral part of its business operations because it had not established a cybersecurity culture to support business operations and drive behavior. Cybersecurity culture is demonstrated when staff members consider the security of information while using it, the IT group anticipates the need for security in its systems, program managers embrace security measures, and senior managers engage in cybersecurity-related decision making.⁴

¹ A network attack in which an adversary gains access to a network and remains undetected for a long period of time.

² National Institute of Standards and Technology (NIST), Special Publication (SP) 800-39, *Managing Information Security Risk – Organization, Mission, and Information System View*, March 2011.

³ A pattern of behaviors, beliefs, assumptions, attitudes, or ways of doing things that promotes security.

⁴ ISACA®, *Creating a Culture of Security*, Steven Ross, 2011.

The Postal Service has not established a cybersecurity culture to support business operations and drive behavior.

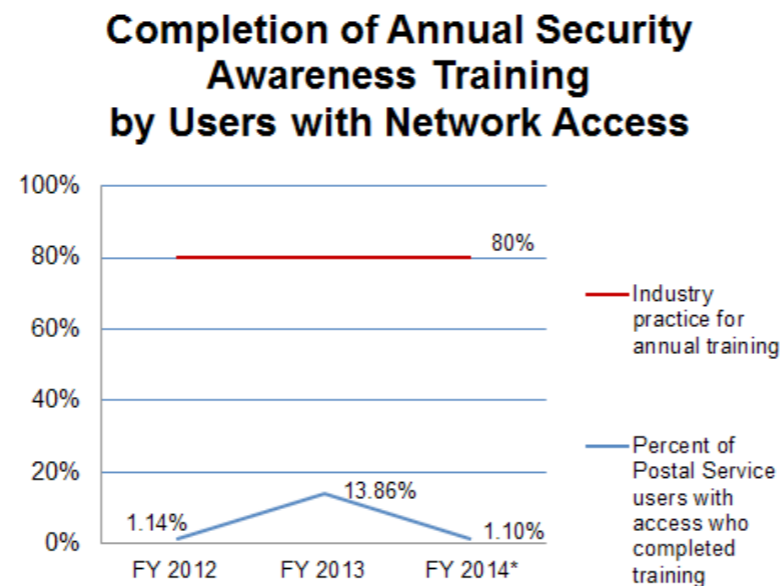


The U.S. Postal Service Office of Inspector General (OIG) found multiple indications of a weak cybersecurity culture. These include inadequate security awareness training, inadequate risk acceptance and accountability, operating systems and software the vendor no longer supports,⁵ and a lack of collaboration on cybersecurity functions within the organization. As a result, employees were unprepared to recognize and respond to advanced cybersecurity risks.

Low Completion Rates and Weak Policies for Annual Security Awareness Training

- In recent years, the percentage of Postal Service network users who completed annual security awareness training was substantially below common industry practice.⁶ Figure 1 provides the completion rates for each fiscal year.

Figure 1. Annual Security Awareness Training by Users with Network Access



* Contractors with access to the Postal Service network were granted access to the Learning Management System beginning late in FY 2014.

Source: OIG prior audit report,⁷ Postal Service Learning Management System, and Gartner.

- Postal Service policy did not require annual security awareness training for every individual granted access to the Postal Service network, but only for users in the CIO area and new hires in their first year of employment with network access. Although the 2015 *Strategic Training Initiative* document identifies groups that should take annual security awareness training, it does not require participation for all network users.

⁵ Operating systems and software that are no longer supported by the vendor are also referred to as "end-of-life."

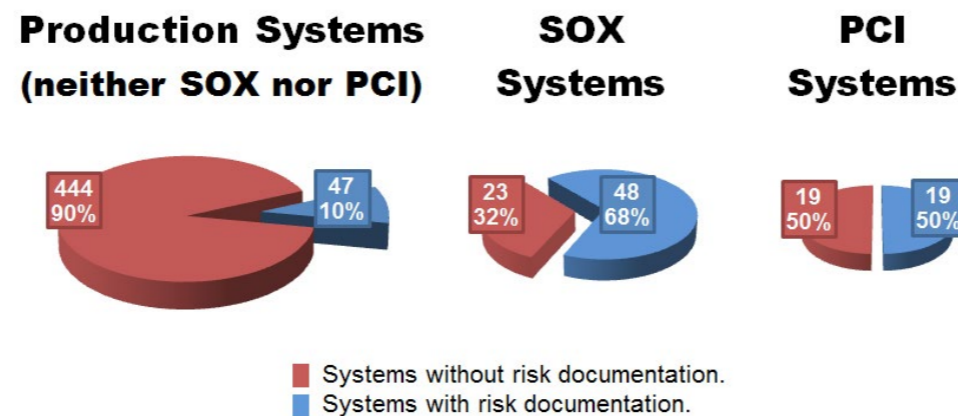
⁶ According to an analyst at Gartner, Inc.® (Gartner), a leading IT research and advisory company.

⁷ *Security Awareness Training Program* (Report Number IT-AR-12-008, dated June 25, 2012). The Postal Service identified corrective action in 2013 for recommendations in the report. However in the subsequent years, Postal Service policy regarding annual security awareness training has changed and completion rates for FYs 2013 and 2014 have remained below industry practice.

Risk Acceptance and Accountability Policies are not Enforced

- The CISO is responsible for assessing risks⁸ associated with system deployment through the certification and accreditation (C&A) process.⁹ The functional business owners of a system and the vice president (VP) for IT have the authority to accept risks. Senior managers indicated the decision to move a system to production was often made before the C&A is completed and all risks are identified. In 2014, 43 systems went into production before the C&A process was finished. In addition, there were two instances where management decided to accept risk in lieu of implementing OIG recommendations.¹⁰ For example, the business owners accepted the risk of storing unencrypted personnel data even though the compensating controls identified did not resolve the residual risk.¹¹
- Despite current policy indicating that managers are personally accountable for the adverse outcomes of risk-acceptance decisions,¹² some senior managers we interviewed indicated that there are no repercussions for their decisions.
- Management has incomplete or inadequate risk information on a substantial majority of the systems in production. Risk analyses are more likely to be documented (risk reduction memos, risk mitigation plans, risk acceptance letters, and security exception letters) for the systems that are subject to legal or industry compliance.¹³ In contrast, only 10 percent of the systems not subject to compliance requirements have risk documentation. Many of these systems contain sensitive information or are critical to Postal Service operations. While it is possible that a system presents no risk in the Postal Service environment, it is unlikely that 90 percent of the production systems not subject to compliance are risk-free and warrant no documentation. Figure 2 provides a visual representation of the systems with and without risk documentation in each of these areas.

Figure 2. Concentrations of Risk Documentation in Production and Compliance Areas



Source: OIG analyses.

⁸ Handbook AS-805, *Information Security*, Section 8-5.6.5, Accreditor Escalates Security Concerns or Accredits Information Resource.

⁹ The C&A process is a formal security analysis and management approval process to assess residual risk before a system is put into production. One of the objectives of the process is to evaluate the security controls and processes chosen to protect a system.

¹⁰ *SAP Human Capital Management System Security Assessment* (Report Number IT-AR-12-005, dated March 19, 2012) and *South Florida District Vulnerability Assessment* (Report Number IT-AR-14-001, dated October 22, 2013).

¹¹ While the data in the cyber intrusion was not extracted directly from the system identified in the risk acceptance letter, sensitive data should be encrypted at rest and in transit in the Postal Service network.

¹² Handbook AS-805, Section 2, Security Roles and Responsibilities, para 2.13; and Section 4-6, Risk-Based Information Security Framework.

¹³ Postal Service must comply with Sarbanes-Oxley Section 404 requirements including an annual assertion on the effectiveness of the internal control structure over financial reporting. In addition, as a merchant accepting debit and credit card payments, they must comply with the Payment Card Industry Data Security Standards which include an annual on-site security audit and quarterly network scans.

Postal Service cybersecurity staffing is significantly below industry levels with one position for every 7,038 users. The most common industry ratio is one position for every 500 to 999 users.

Maintaining Outdated Operating Systems and Software

In a limited review of the Postal Service network, we identified systems and software that are unsupported by the vendor and pose a significant security risk because patches to correct security vulnerabilities are no longer available. They include:

- Sixteen of 31 sampled software versions.
- Nine operating systems across 39 servers, including one operating system that supports five servers for the Postal Service's debit and credit card payment processing system.

History of Poor Collaboration

There have been instances where the various groups responsible for cybersecurity services or functions have not effectively collaborated on cybersecurity issues identified within OIG reports:

- Engineering Systems has not coordinated effectively with the CISO to complete impact assessments and document information security requirements for its systems.¹⁴
- An internal web server was inadvertently available to the public through the Internet because engineers and system administrators had insufficient information about the network, application, and server configurations.¹⁵
- Managers delayed notifying the CIRT for 12 days following a breach of USPS.com data in 2011.¹⁶

By establishing and promoting an effective cybersecurity culture throughout the organization, the Postal Service has an opportunity to prevent cybersecurity weaknesses from occurring in the future and better prepare its employees to identify and address cybersecurity risks. Management has taken actions in response to the specific recommendations within the reports, which did not specifically identify a lack of collaboration.

Cybersecurity Staffing and Resourcing

Staffing and resources have not been sufficient to support tasks beyond basic operations and comply with legal and industry requirements. This lack of support exists because funding for cybersecurity functions at the Postal Service was below industry practices and also fragmented across multiple areas and funding codes. As a result, management has been unable to take proactive measures to prevent or remediate threats to the network.

Limited Cybersecurity Staffing

- Postal Service cybersecurity staffing is significantly below industry levels. There are 53 full-time equivalent (FTE) security positions¹⁷ for 373,000 network users – or one FTE for every 7,038 users – compared to the most common industry ratio of one FTE position for every 500 to 999 users. Figure 3 compares Postal Service FTEs to the estimated number of FTEs for the same number of end users in each comparable industry.

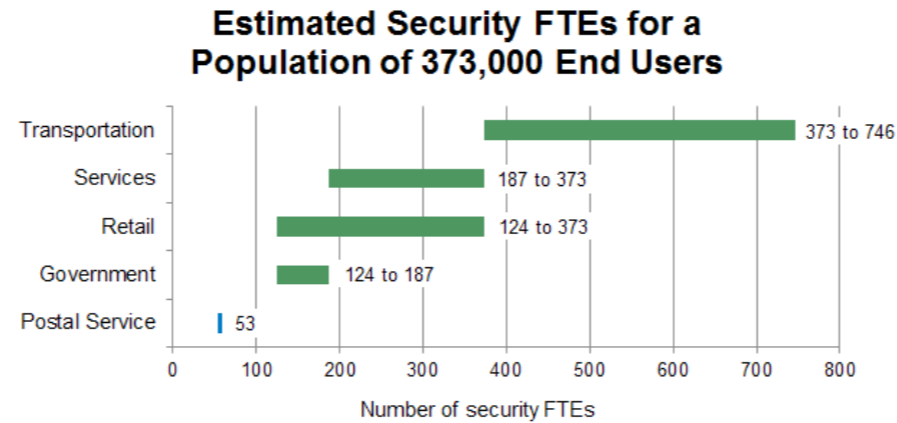
¹⁴ *South Florida District Vulnerability Assessment* (Report Number IT-AR-14-001, dated October 22, 2013) and *Engineering Systems and Network Operations Disaster Recovery Plan, Merrifield, VA Campus* (Report Number IT-AR-13-007, dated September 24, 2013).

¹⁵ *Web Server Security Assessment* (Report Number IT-AR-13-004, dated March 4, 2013).

¹⁶ *USPS.com Data Breach* (Report Number IT-AR-12-004, dated March 15, 2012).

¹⁷ The staffing numbers include the CISO and Perimeter Security team members and team leads providing core cybersecurity services. They do not include completely outsourced functions such as contracted telecommunications network operations centers.

Figure 3. Comparison of Postal Service FTEs to Industry Practices



Source: OIG analysis and Gartner (April 2014).

- The Postal Service did not have a Security Operations Center (SOC) that supports round-the-clock, detailed analysis, trending, and threat assessments of cybersecurity issues. See [Appendix B](#) for SOC best practices.
- The CIRT, which serves as the initial alert, monitoring, and categorization function for all incidents, has been staffed with four employees who support the automated and manual efforts used in analysis, triage, and response to the roughly 14 billion events recorded in a single month. See [Appendix C](#) for CIRT best practices.
- The vulnerability management program, executed by the Security Vulnerability Assessment (SVA) team, has not had sufficient resources to provide a comprehensive vulnerability management program, including penetration testing. See [Appendix D](#) for vulnerability management best practices.
- The CISO had insufficient resources to conduct thorough risk assessments. Each member assigned to the C&A process is currently responsible for an average of 46 production systems plus numerous additional systems that are under development.
- The Postal Service’s agreement with the U.S. Department of Homeland Security (DHS) to participate in the Continuous Diagnostics and Mitigation program includes the capability for external scans; however, the Postal Service is one of only three (of 155) agencies that do not use the scanning service.¹⁸
- There is no record of role-based training resources for Postal Service cybersecurity staff in either the current training course records¹⁹ or the *Strategic Training Initiative*. Role-based training, required by internal policy²⁰ and recommended by best practices,²¹ provides management and staff members with key information about their duties relating to cybersecurity and operational processes.

¹⁸ The former Postal Service CISO manager reportedly advised DHS that it could not scan Postal Service systems without a schedule and prior coordination because of outages attributed to a previous DHS scan.

¹⁹ As exhibited in the Learning Management System.

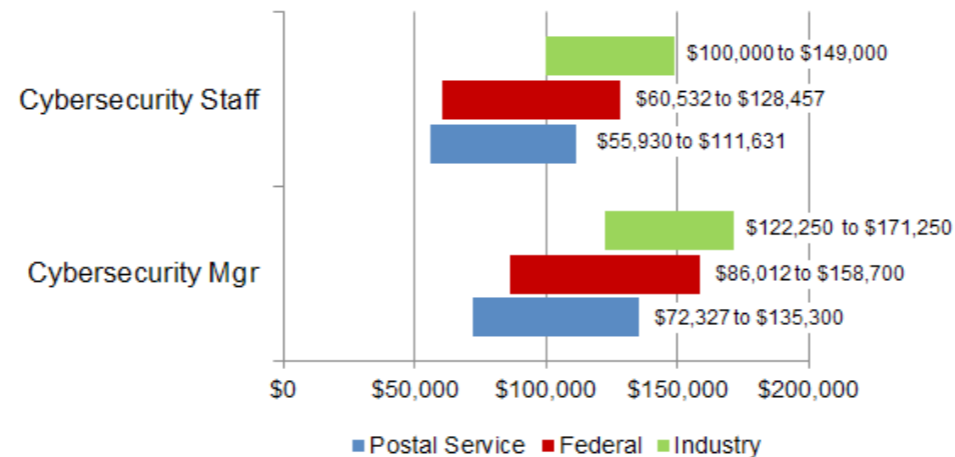
²⁰ Handbook AS-805, Section 6-5.3, Training Requirements, Exhibit 6-5.3 states that all C&A stakeholders must complete annual training on the C&A process and all personnel with computer operations responsibilities must be trained in handling security breaches and incidents.

²¹ NIST, SP 800-16, rev. 1, *A Role-Based Model for Federal Information Technology/Cyber Security Training*, Toth and Klein, October 2013, states that role-based training supports competency development, helps personnel understand and learn how to better perform their specific security roles, and ultimately better secures the organization’s mission. It is required for any individual who has influence over an information system, application or network, data, and/or the organization’s mission.

Challenges in Hiring and Maintaining Skilled Staff

- Postal Service pay bands for skilled cybersecurity staff positions²² are not competitive compared to industry salary ranges. [Figure 4](#) provides charts depicting the salary ranges used to attract new cybersecurity talent for key positions. In January 2015, three of 44 cybersecurity employee positions (7 percent) were vacant.

Figure 4. Cybersecurity Salary Range Comparisons



Source: OIG analyses and OPM.

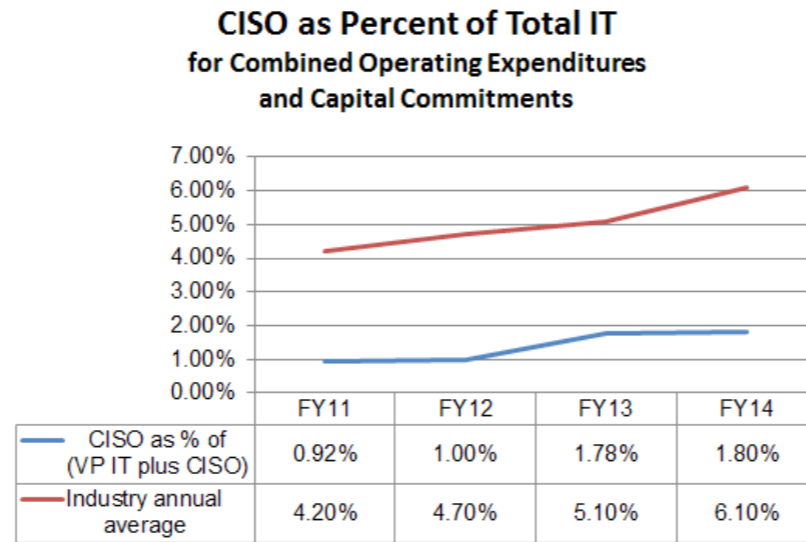
- Management has not created plans to develop team members' technical cybersecurity skills. Thirteen of 41 (32 percent) employees in our review completed at least one technical training course in fiscal year (FY) 2014; however, the courses were not aligned to advance Postal Service cybersecurity or enhance specific skills for individuals. By developing staff into highly skilled security practitioners, management will improve the effectiveness of the cybersecurity tools used, enhance the staff's ability to develop effective response plans, and demonstrate commitment to career development, which promotes retention.

Funding for cybersecurity staff and support at the Postal Service has been below industry averages. The Postal Service spent an average of 1.4 percent of its IT budget on cybersecurity from FYs 2011 through 2014, while industry averages for this period are about 5 percent. In addition, costs are fragmented across multiple areas and funding codes, making it difficult to isolate cybersecurity efforts throughout the organization, which limits visibility into overall spending. While fragmentation is common in cybersecurity funding because it involves multiple organization functions, best practices recommend that leadership has visibility into and understanding of cybersecurity spending to ensure that risk is appropriately managed. Further, the CISO should have influence over cybersecurity-related spending across the enterprise.²³ [Figure 5](#) shows the gap between the Postal Service and industry in recent years.

²² For federal salaries, we incorporated the special incentive pay for IT series positions available through the Office of Personnel Management's (OPM) special rate schedules and locality pay for Postal Service IT centers in California, the District of Columbia, Minnesota, and North Carolina. For the Postal Service, we used the variable pay bands available to technical and management employees in cybersecurity functions.

²³ Gartner, *Identifying the Real Information Security Budget*, October 20, 2011.

Figure 5. Cybersecurity Funding in Proportion to IT



Source: OIG analysis of Postal Service accounting records²⁴ and Gartner (2014).

The Postal Service would be better prepared for a rapidly changing threat landscape and effectively managing risks by integrating cybersecurity risk considerations into the organization’s overall cybersecurity strategy.

As a result of the limited staffing and support caused by funding issues, the Postal Service has been unable to develop proactive cybersecurity capabilities to prevent or remediate advanced threats.

Cybersecurity Strategy

The Postal Service has not integrated cybersecurity risk considerations, such as governance and incident response guidance, into an overall cybersecurity strategy. It lacks a comprehensive strategy because management has not determined the organization’s risk tolerance,²⁵ which would guide strategic direction. As a result, the Postal Service has been unable to prepare for the rapidly changing threat landscape and effectively manage risks.

Incomplete Integration for Governance and Strategy

- In February 2015, the Postal Service announced a restructuring that changed the position of manager, CISO to chief information security officer and VP of Digital Solutions. This change combined the duties of two full-time positions into a single VP for CISO and Digital Solutions rather than having a VP solely dedicated to CISO responsibilities. The Federal Information Security Management Act of 2002 (FISMA) requires that information security be the primary duty of the information security officer. While the Postal Service is not required to comply, FISMA reflects common industry practice.
- Postal Service Handbook AS-805, which sets information security policy for the organization, lacks a framework for risk management that includes framing, assessing, responding to, or monitoring risk.
- The Postal Service’s overarching emergency management planning processes and Integrated Emergency Management Plan²⁶ (IEMP) address threats from severe weather, fire, and biohazards. They do not address cybersecurity threats.

²⁴ Funding reflected in Figure 5 for the CISO includes non-traditional cyber functions such as the eAccess and eDiscovery teams – which could not be isolated from the finance accounts for the CISO. We excluded funding for the telecommunications network operations center-related services of the Perimeter Security team, as we were unable to reliably isolate these costs from other expenditures included in the accounts.

²⁵ The level of risk or degree of uncertainty that is acceptable to an organization.

²⁶ The current IEMP is under revision. While management stated there are plans to incorporate checklists related to location-based cybersecurity or IT issues, a revised IEMP was not available for review during the audit.

Inadequate Incident Response Guidance and Clearances

- The incident response guidance available to the Postal Service staff in the fall of 2014 was not clear regarding when to invoke the Mass Data Compromise Review Plan (MDCRP).²⁷ In addition, contradictions²⁸ between the MDCRP and other incident-related guidance in the *CIRT Operations Manual* may delay involvement of non-CIRT staff in response and mitigation.
- Management had not prepared for a cybersecurity incident by ensuring appropriate security clearance levels were in place for individuals responsible for incident response activities. Several points of contact identified in the MDCRP did not have sufficient clearance to receive national security information regarding a cyber intrusion. In addition, when key members of the cybersecurity teams do not have appropriate security clearances, they are not able to access data from external responders and the broader intelligence community, such as National Cybersecurity Protection System (NCPS) data,²⁹ which requires a top secret clearance.
- Neither the MDCRP nor the *CIRT Operations Manual* contained guidance or instructions for coordinating with the telecommunication network operations centers (T-NOC)³⁰ when responding to a cybersecurity incident. See [Appendix E](#) for T-NOC best practices.
- Neither the MDCRP nor the *CIRT Operations Manual* included response procedures for incidents identified by organizations outside of the Postal Service. These documents only addressed incidents detected internally and by automated alerting systems.

Actions Taken to Improve Cybersecurity

The Postal Service has taken actions to improve some of the cybersecurity concerns noted in this report. The manager, Corporate Information Security position was changed to a chief information security officer and VP of Digital Solutions, a shared VP function within CIO organization in February 2015, to provide greater oversight of cybersecurity functions. As noted previously, best practice is for the CISO function to be assigned the primary responsibility for a role, rather than a shared duty. Additionally, the Postal Service engaged in a joint forensic investigation with subject matter experts following the cyber incident. They have initiated enhanced monitoring capabilities and plans are underway to procure SOC services to monitor enterprise security in real-time from a centralized location; and to discover, prioritize, remediate, and report on events in the Postal Service IT environment. Finally, management has accelerated existing plans to strengthen access management, intrusion detection, and authentication processes.

In addition, the Postal Service has two strategic initiatives³¹ related to the topics discussed in this report. One objective of DRIVE initiative 51, Leverage Technology and Data to Drive Business Value, is to use the latest technology and risk management tools to increase cybersecurity capability. This effort includes an external cybersecurity risk assessment targeted for completion in May 2015, and creation of a cybersecurity risk management dashboard scheduled for production in August 2015.

The Postal Service developed DRIVE initiative 44, Enterprise Risk Management, to provide reasonable assurance that significant risks to and opportunity losses for the Postal Service are systematically and effectively identified, evaluated, and mitigated where appropriate. We have not evaluated either DRIVE initiative as part of this audit.

²⁷ The MDCRP defines the roles and responsibilities of the critical incident response team members, identifies the primary and alternate points of contact, and provides methodologies for conducting response activities.

²⁸ For example, both the MDCRP and *CIRT Operations Manual* contain different guidance on incident response and notification procedures. Although the MDCRP is incorporated into the manual as Chapter 5, the manual has no other reference to the MDCRP and does not describe when the MDCRP should be invoked.

²⁹ NCPS is designed to detect advanced persistent threats against government networks. Consumers of NCPS data (also known as EINSTEIN) receive alerts when malicious or potentially malicious activity is detected.

³⁰ Telecommunications Services has contracted for T-NOC services from several providers. For this audit, we focused on the primary Internet connectivity providers (AT&T™, Verizon™, and XO Communication) and the T-NOC support they provide to the Postal Service.

³¹ The Postal Service's portfolio of strategic initiatives is known as Delivering Results, Innovation, Value, and Efficiency, or DRIVE.

The cyber intrusion has put the Postal Service in a period of awareness that it should leverage to enhance the cybersecurity culture, appropriately resource functions, and establish a strategic direction. Despite the initiatives described above, the Postal Service may be subject to escalating damage from intrusions with increasing frequency and severity and remain susceptible to less sophisticated threats. To be better prepared, management must continue to address cybersecurity deficiencies. [Appendix F](#) contains questions to guide executive leaders toward attaining more effective cybersecurity operations by implementing the necessary corrective actions.

Recommendations

We recommend the acting chief information officer and executive vice president coordinate with the executive leadership team to:

1. Develop and execute a strategy based on an organizational risk assessment and determination of the risk tolerance to embed a strong cybersecurity culture into daily operations.
2. Communicate the cybersecurity strategy and initiate cultural changes through initiatives focused on security education, training, and awareness activities to all U.S. Postal Service employees, contractors, and senior leadership.
3. Separate the joint duties of the chief information security officer and vice president of Digital Solutions and designate a senior-level chief information security officer with information security as the primary duty.

We recommend the acting chief information officer and executive vice president:

4. Provide adequate resources for cybersecurity operations, including:
 - Funding commitments to enable proactive prevention, detection, response, and mitigation of sophisticated cyber threats.
 - Providing visibility into fragmented cybersecurity funding to facilitate a coordinated approach to reducing business risk.
5. Adequately staff cybersecurity operations functions based on the organization's risk tolerance. Specifically, staffing levels should support business requirements to:
 - Ensure the security operations center provides skilled cyber threat and intrusion analysis and experienced threat remediation and response management staff.
 - Expand Computer Incident Response Team functions to include comprehensive incident management and response, including anomalous activity detection.
 - Create centralized network operations center capabilities and require participation as part of a cybersecurity incident response with the security operations center and Computer Incident Response Team.
 - Expand the existing vulnerability management program to encompass the federal objectives for continuous monitoring, including penetration testing.

We recommend the acting chief information security officer and Digital Solutions vice president:

6. Develop and implement a plan for the organization to exercise the appropriate governance and incident response.

Management's Comments

Management agreed with all the findings and with recommendations 1, 2, 4, 5, and 6. Management neither agreed nor disagreed with recommendation 3 and will conduct a study to evaluate the recommended action.

Regarding recommendation 1, management stated they have devised a strategic security roadmap to develop and revise the enterprise-wide cybersecurity strategy using risk assessments performed by business and industry subject matter experts. Management requested that recommendation 1 be closed upon issuance of the report.

Regarding recommendation 2, management stated they intend to execute significant portions of the CyberSafe component of an organizational training and awareness strategy in FY 2016.

Regarding recommendation 3, management intends to evaluate the separation of the chief information security officer and VP of Digital Solutions positions by the end of FY 2015.

Regarding recommendation 4, management stated they are executing a multi-phase improvement plan that includes investments for cybersecurity operations to be funded by September 30, 2015.

Regarding recommendation 5, management stated they have initiated a significant reorganization of the CISO capabilities including appropriate staffing level increases and contracting augmentation to be fully implemented by September 2017.

Regarding recommendation 6, management stated they will complete a comprehensive review and update to the enterprise-wide incident management, control, and response process prior to December 31, 2016.

See [Appendix H](#) for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report.

Regarding recommendation 1, management's comments address the development of a strategy; we agree they have developed and begun implementing the strategy. The OIG will close recommendation 1 and continue to do work in this area.

Regarding recommendation 2, the OIG will monitor the USPS Cybersecurity Organizational Training and Awareness Improvement Strategy.

Regarding recommendation 3, the OIG encourages the Postal Service to include best practices for separation of duties in the study of information security leadership.

Regarding recommendations 4 and 5, the OIG will monitor improvements in cybersecurity funding visibility and centralized network operations center capabilities as part of Cybersecurity Phase II implementation.

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.

Appendices

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

Appendix A: Additional Information	18
Background	18
Objective, Scope, and Methodology.....	18
Prior Audit Coverage	19
Appendix B: Cybersecurity Best Practices for Security Operations Centers.....	20
Appendix C: Cybersecurity Best Practices for Computer Incident Response Teams.....	21
Appendix D: Cybersecurity Best Practices for Vulnerability Management	22
Appendix E: Cybersecurity Best Practices for T elecommunication Network Operations Centers.....	23
Appendix F: Key Questions to Ask.....	24
Appendix G: References	25
Appendix H: Management’s Comments	27

Appendix A: Additional Information

Background

At the time of the audit, the Postal Service's CISO was composed of two primary operational groups in Raleigh, NC, and Washington, DC. The manager, Corporate Information Security, acted as the CIO's primary liaison regarding the organization's information security functions and was charged with addressing threats and risks to the organization's information security. The Raleigh Operations teams included the CIRT, security operations, the Network Connectivity Review Board, and SVA. The Headquarters Operations teams managed the C&A process, oversaw security clearance processing, managed the security awareness program and annual training requirements, and served as business owner for the eAccess system.³² Cybersecurity functions are also supported throughout the organization by system administrators, database administrators, inspectors, and others who are individually responsible for configuring, maintaining, and protecting Postal Service resources.

Under the VP for IT, the Telecommunication Services Perimeter Security team provides coverage for certain cybersecurity responsibilities related to T-NOCs. They include monitoring network traffic on over 30,000 endpoints for anomalies, monitoring network security alerts and logs, supporting security incident detection and prevention technologies, and reporting suspected incidents to the CIRT. Telecommunication Services also manages several external vendors who operate their own T-NOCs 24 hours a day, 7 days a week, and report incidents to CIRT through Telecommunications Services.

Objective, Scope, and Methodology

Our objective was to determine whether at the time the cyber intrusion was identified, the Postal Service's cybersecurity functions aligned with industry best practices for determining whether the structure, operations, and resourcing effectively support the enterprise. We did not evaluate the Postal Service's response or corrective actions following the cyber intrusion of 2014, as we will evaluate that incident in a separate audit. To accomplish our objective we:

- Reviewed cybersecurity operations for the period September through October 2014. When data was not available for the September-October timeframe, we relied on comparable data from November 2014 through March 2015.
- Conducted interviews with onsite personnel, gathered data from Postal Service systems, and reviewed documentation related to policies and procedures, structure, and operations of the CISO organization and the scope and operations of the T-NOC, SOC, and CIRT.
- Reviewed training completion rates for users and individuals with cybersecurity responsibilities to determine whether adequate security awareness training existed from FYs 2012 through 2014.
- Evaluated the background investigation and clearance levels for individuals with cybersecurity and incident management responsibilities.
- Reviewed cybersecurity-related operating expenditures and capital commitments and planned expenditures for FYs 2011 through 2014.
- Reviewed best practices for cybersecurity operations from sources such as NIST, the MITRE Corporation (MITRE®), and Carnegie Mellon University Software Engineering Institute; as well as recent studies and academic analyses from ISACA, Ernst & Young®, and Gartner (see [Appendix G](#) for a list of the references used).

³² eAccess is the system used for managing requests, approvals, and reviews of access to Postal Service systems and infrastructure components.

We conducted our work from December 2014 through July 2015, 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 June 12, 2015, and included their comments where appropriate.

We assessed the reliability of data extracted from Postal Service computer systems by interviewing managers knowledgeable about the data and relying on tests of the data conducted during prior OIG audits. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG previously issued eight reports on the activities or responsibilities of the CISO organization and the Perimeter Security team. In these reports, we provided relevant information on concerns with CIRT operations, vulnerability scanning, security operations, and security training. The report titles and dates are provided in the table below.

Report Title	Report Number	Final Report Date	Monetary Impact
Backup and Recovery of Essential Data	IT-MA-14-001	8/20/2014	None
Topeka, KS, Material Distribution Center - Information Technology General Controls	IT-AR-14-006	6/11/2014	None
South Florida District Vulnerability Assessment	IT-AR-14-001	10/22/2013	None
Management and Utilization of Software Licenses	IT-AR-13-006	7/31/2013	None
Data and Voice Communications	IT-AR-13-005	6/14/2013	None
Web Server Security Assessment	IT-AR-13-004	3/4/2013	None
Fiscal Year 2012 Information Technology Internal Controls	IT-AR-13-003	1/28/2013	None
Security Awareness Training Program	IT-AR-12-008	6/25/2012	None

Appendix B: Cybersecurity Best Practices for Security Operations Centers

Real-Time Analysis	
• Call Center	• Real-Time Monitor/Triage
Intel and Trending	
• Cyber Intel Collection and Analysis	• Cyber Intel Fusion
• Cyber Intel Distribution	• Trending
• Cyber Intel Creation	• Threat Assessment
Incident Analysis and Response	
• Incident Analysis	• Countermeasures
• Tradecraft Analysis ³³	• Remote/On-Site Incident Response
• Coordinate/Respond	
Artifact Analysis	
• Forensic Artifact Handling	• Forensic Artifact Analysis
• Malware Analysis	
Tool Life-Cycle Support	
• Perimeter Device Operation & Maintenance	• Custom Signatures
• SOC Infrastructure Operation & Maintenance	• Tool Engineering & Deployment
• Sensor Tuning & Maintenance ³⁴	• Tool Research & Development
Audit and Insider Threat	
• Audit Data Collection & Distribution	• Insider Threat Case Support & Investigation
• Audit Content & Creation	
Outreach	
• Product Assessment	• Situational Awareness
• Security Consulting	• Redistribution of Tactics, Techniques, & Procedures
• Training & Awareness Building	• Media Relations

Source: MITRE (2014).

³³ Carefully coordinated engagements with an adversary where the SOC performs a sustained study and analysis of the adversary's techniques (as the adversary is allowed to continue activity) in order to inform ongoing monitoring.

³⁴ Care and maintenance of the sensor platform owned and operated by the SOC that includes integrating tools, updating systems, and minimizing unreliable output.

Appendix C: Cybersecurity Best Practices for Computer Incident Response Teams

- Create an incident response policy and test regularly.
- Develop incident response and reporting procedures.
- Establish guidelines for coordinating and communicating with external parties.
- Staff and train Incident Response Team members to include general, role-based, and technical training.
- Help an organization detect incidents and rapidly respond to minimize losses and destruction, identify weaknesses, and restore IT operations without delay.
- Maintain records about the status of incidents, along with other pertinent information.
- Safeguard data related to incidents containing sensitive information on recent security breaches, exploited vulnerabilities, and users who may have performed inappropriate actions.
- Prioritize subsequent activities that encompass the containment, eradication, and recovery of an incident.
- Hold a “lessons learned” meeting to review the effectiveness of the incident handling process and identify necessary improvements to existing security controls and practices.
- Provide help to users when security incidents occur in their systems and share information concerning common vulnerabilities and threats.
- Perform an initial analysis to determine the incident’s scope, attack methods, and targeted vulnerabilities.
- Incident response team should work quickly to analyze and validate an incident, documenting each step taken.
- Develop written guidelines for prioritizing incidents.
- Establish and maintain accurate notification mechanisms.

Source: OIG analyses of NIST and Carnegie Mellon University data.

Appendix D: Cybersecurity Best Practices for Vulnerability Management

Network Mapping:

Sustained, regular mapping of the organization's networks to understand the size, shape, makeup, and perimeter interfaces through automated or manual techniques.

Vulnerability Scanning:

Interrogation of the organization's hosts for vulnerability status, usually focusing on each system's patch level and security compliance, typically through automated, distributed tools.

Vulnerability Assessment:

Full knowledge, open-security assessment of an organization site, enclave, or system.

Penetration Testing:

No knowledge or limited-knowledge assessment of a specific area of the organization.

Source: MITRE (2014).

Appendix E: Cybersecurity Best Practices for Telecommunication Network Operations Centers

- Maintain near 100 percent availability of networks and services.
- Intrusion detection system/intrusion prevention system monitoring.
- Escalate possible incidents to the CIRT and help deploy countermeasures.
- Work as a peer of SOC to coordinate new technologies, hardware, or software placed on the network.
- Provide monitoring data to security program managers.
- Control access to network resources.
- Monitor users of network resources.
- Create a platform-specific minimum configuration standard for all routers, switches, and perimeter devices that follow industry best practices for security and performance.
- Tighten network perimeter security and ensure proper configuration management of network devices (such as firewall rules sets).
- Ensure timely patching of systems or devices to decrease vulnerabilities.
- Ensure adequate hardware and software resources are available and used to safeguard networks.
- Ensure access control by means of authentication of network users by process of identifying users, including login and password dialog, challenge and response, and messaging support and authorization access controls requested by the user are in place.
- Provide training to individuals based on their particular job functions.

Source: OIG analyses of MITRE, NIST, and other sources.

Appendix F: Key Questions to Ask



Is the Postal Service Focused on the Right Things?

When it comes to cybersecurity, resources need to be distributed to address risk. Often when resources are insufficient to cover the spectrum of risk, organizations focus on compliance, leaving many risks unaddressed.



Is Current Cybersecurity Reactive or Proactive?

Ensuring an organization's cybersecurity force has the support and resources it needs to carry out its mission is critical. Without them, the organization cannot operate proactively to address cybersecurity risks before they become a problem. An organization must ensure it is ready for tomorrow's threats and risks.



Where Do We Need to Adapt Our Culture?

An organization's culture is self-perpetuating. What has always been done will continue to be done. Decision makers are able to identify weakness caused by culture and affect change to address these shortcomings.



Do We Collaborate Effectively to Respond to Threats?

Collaboration among different levels of management, functions, and groups helps decision makers see where resources are needed and can have the most impact.



Do We Have the Right Balance of Talent?

Obtaining the right talent can be a tough task. A strategic approach must be used when determining what level of talent will be out-sourced and what will be kept in-house. Whatever an organization decides, the focus should be on quality over quantity.



Can Executive Management Articulate Cyber Risks and Explain Their Approach and Response to Such Risks?

Having a well-defined process to identify and respond to risk makes it easier for executives to understand the organization's cybersecurity when having to explain the approach internally and to outside entities.

Appendix G: References

Based on the review of best practices, we identified guidance on selected aspects of cybersecurity operations, with particular attention to T-NOC, SOC, CIRT, and SVA functions. For each of these areas, we reviewed information on the placement of each function, roles and responsibilities, skill sets, operational structure (such as 24-hour coverage), tools, and resources necessary to combat threats to an organization's cybersecurity. This is a list of the materials we used to perform this audit. It may help management as they plan enhancements to cybersecurity.

- Billington CyberSecurity, *Achieving Cyber Resiliency: What Steps Can We Take to Achieve Enhanced Cyber Resiliency in One Year's Time?*, 5th Annual Billington Cybersecurity Summit, 2014.
- Carnegie Mellon Software Engineering Institute, *Handbook for Computer Security Incident Response Teams (CSIRT)*, 2nd ed., West-Brown, Stikvoort, Kossakowski, Killcrece, Ruefle, and Zajicek, April 2003.
- Cisco Systems, Inc., *Network Management System: Best Practices White Paper*, July 11, 2007.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO), *COSO in the Cyber Age*, Mary Galligan and Kelly Raum, January 2015.
- Ernst & Young, *Cyber Program Management, Identifying ways to get ahead of cybercrime*, October 2014.
- Gartner, *Determining Whether the CISO Should Report Outside of IT*, Scholtz, June 17, 2014.
- Gartner, *Identifying the Real Information Security Budget*, Wheatman, October 20, 2011.
- Gartner, *Information Security Organization Dynamics*, Scholtz, August 4, 2014.
- Gartner, *IT Key Metrics Data 2015: Key IT Security Measures: by Industry*, Hall, Futela, and Gupta, December 15, 2014.
- Gartner, *IT Key Metrics Data 2015: Key IT Security Measures: Current Year*, Hall, Futela, and Gupta, December 15, 2014.
- Gartner, *IT Key Metrics Data 2015: Key IT Security Measures: Multiyear*, Hall, Futela, and Gupta, December 15, 2014.
- Gartner, *IT Key Metrics Data 2015: Key IT Security Measures: Security Priorities and Processes*, Hall, Futela, and Gupta, December 15, 2014.
- Gartner, *Security Governance, Management and Operations Are Not the Same*, McMillan and Scholtz, January 23, 2013.
- Gartner, *Survey Analysis: Information Security Governance, 2014-15*, Scholtz, September 30, 2014.
- Gartner, *Tips and Guidelines for Sizing Your Information Security Organization*, Scholtz and McMillan, April 24, 2014.
- ISACA, *Creating a Culture of Security*, Ross, 2011.
- ISACA, *Defining Information Security Management Position Requirements, Guidance for Executives and Managers*, 2008.

- ISACA, *Key Elements of a Threat and Vulnerability Management Program*, Pironti, 2006.
- MITRE, *Ten Strategies of a World-Class Cybersecurity Operations Center*, Carson Zimmerman, 2014.
- NIST SP 800-16, *Information Technology Security Training Requirements: A Role - and Performance-Based Model*, Wilson, de Zafra, Pitcher, Tressler, and Ippolito, April 1998.
- NIST SP 800-16 rev. 1, 3rd draft, *A Role-Based Model for Federal Information Technology/Cybersecurity Training*, Toth and Klein, March 2014.
- NIST SP 800-35, *Guide to Information Technology Security Services*, Grance, Hash, Stevens, O'Neal, and Bartol, October 2003.
- NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, Grance, Stevens, and Myers, October 2003.
- NIST SP 800-37, rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach*, Joint Task Force Transformation Initiative, February 2010.
- NIST SP 800-39, *Managing Information Security Risk - Organization, Mission, and Information System View*, Joint Task Force Transformation Initiative, March 2011.
- NIST SP 800-40, rev 3, *Guide to Enterprise Patch Management Technologies*, Souppaya and Scarfone, July 2013.
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, Wilson and Hash, October 2003.
- NIST SP 800-61, rev. 2, *Computer Security Incident Handling Guide*, Cichonski, Millar, Grance, and Scarfone, August 2012.
- NIST SP 800-65 rev. 1, *Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (draft)*, Bowen, Kissel, Scholl, Robinson, Stansfield, and Voldish, July 2009.
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, Bowen, Hash, and Wilson, October 2006.
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, Scarfone, Souppaya, Cody, and Orebaugh, September 2008.

Appendix H: Management's Comments

RANDY S. MISKANIC
ACTING CHIEF INFORMATION OFFICER
AND EXECUTIVE VICE PRESIDENT



July 17, 2015

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Report – U.S. Postal Service Cybersecurity Functions
(Report Number IT-AR-15-DRAFT, project number 15TG008IT000)

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

Since the scope of this audit was based solely on the state of cybersecurity when the intrusion was discovered in 2014, the findings do not reflect the current state of the organization's capabilities. The management processes, staffing, computing environment protections, training and awareness and other controls have been substantially upgraded based upon the learnings from the 2014 cyber intrusion. As such, while we generally agree with the intent of the findings as accurate for the period prior to the intrusion, we would encourage the USPS OIG to incorporate the substantial changes in processes and the significant number of activities undertaken in response to the 2014 cyber intrusion.

In this regard, while we find that we can agree with the broad intent of most of the recommendations in the report, we believe that nature of the threats we face requires more flexible and active management processes and modes of response than those identified by the OIG.

The U.S. Postal Service has made significant improvements since the 2014 cyber intrusion incident and will continue to make significant investments over the next few years to improve our ability to defend against aggressive advanced persistent threats like the one that resulted in the cyber incident announced November 2014. Protecting the privacy of customer, employee, supplier and the Postal Service information has been and always will be a priority for the Postal Service. This incident along with many others that have occurred in federal government and commercial entities over the past year have demonstrated the need for ever greater comprehensive cybersecurity capabilities involving technology, people and processes to defend against threats, monitor systems for possible unauthorized access and eradicate intruders.

The U. S. Postal Service has since developed and is executing a multiple phase cybersecurity improvement strategy to meet its security objectives and address security needs across the enterprise. In Phase 1, the investment focused on the pressing need for remediation of the infrastructure and developing technical capabilities for identifying and protecting against the most immediate threats.

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-1500
WWW.USPS.COM

Phase 1 Cyber Security Improvements (Remediation and US-CERT Recommendations)

Phase 1 tactical improvement efforts commenced on November 8, 2014 and consisted of detailed remediation activities that focused on rebuilding the impacted infrastructure and the implementation of technical capabilities for identifying and protecting against the most immediate threats. These activities were defined in close cooperation with US-CERT, CMU-SEI, Microsoft, and other subject matter experts with the common objective of eradicating the actor from the network, restricting privileged accounts, implementation of improved authentication, monitoring, and domain management. The remediation project scope included approximately 1,000 technical activities that were necessary to fulfill the objectives detailed above.

Below is a detailed listing of some of the corrective actions taken immediately starting the weekend of November 8, 2014 and continued through February 2015.

- ❖ The U.S. Postal Inspection Service (USPIS), USPS Corporate Information Security Office (CISO), the Department of Defense Computer Forensics Laboratory (DC3), Microsoft, Verizon, and Lockheed Martin conducted forensic investigations as a result of the breach. These investigations revealed the attackers' signature techniques and helped to identify the extent and limits of the breach.
- ❖ CISO followed the remediation plan recommended by US-CERT, initiating a "Brownout" network and system outage November 8-9 to eradicate the actor from the network and to begin remediation of security vulnerabilities:
 - Removed compromised systems;
 - Disabled compromised accounts;
 - Forced users to change passwords and increase password complexity;
 - Disabled remote access for administrators;
 - Disabled web email.
- ❖ Conducted a review of privileged access.
 - Removed local administrative rights for many users. Users requiring local rights are not allowed to operate on the main user domain.
 - Reduced the number of users with high-level access. (Since the breach, the number of privileged system administrators has decreased from ~1500 down to ~50.).
 - Removed ~20,000 inactive devices.
- ❖ The organization implemented two-factor authentication to provide for better protection against unauthorized use of USPS IT resources.
 - Two factor authorization is now required for administrative functions and select sensitive applications.
 - A more widespread deployment of two factor authentication is in the planning stage.
- ❖ CISO has improved monitoring capabilities by increasing and centralizing the collection and analysis of network events and user actions. These events are being collected and analyzed in a Security Information and Event Management system (SIEM). The centralization of data will make it easier for CISO and an externally sourced SOC to correlate events and detect threats across the enterprise.

Phase 2 Cybersecurity Improvements (Capability Assessments and Implementation)

For Phase 2, the organization has committed to an investment for staff augmentation and funding to implement the critical security enhancements recommended by agencies and industry partners. Additionally, the Postal Service procured assistance from external subject matter experts representing government, academia and the defense industry to perform security assessments to help the Postal Service understand and prioritize risks associated with cyber threats and identify future security enhancements to be executed in future phases.

- ❖ Security professionals from Microsoft, General Dynamics, Raytheon/Blackbird Technologies, Deloitte, Symantec and Hewlett-Packard have been engaged to augment the USPS personnel focused on improving information security.
- ❖ In February 2015 significant architectural changes were made to our computing environment based on recommendations from leading security experts. This architecture offers better assurance that privileged accounts are used only by authorized staff.
- ❖ CISO commenced a procurement process for the services of an outsourced Security Operations Center (SOC) to provide 24/7/365 cyber security monitoring and investigation into suspicious behavior – several bids have been received, CISO is in final selection phase.
- ❖ A variety of efforts are underway to implement intrusion detection and intrusion prevention throughout the organization.

Several external organizations specializing in security analysis and threat avoidance services conducted top-down security assessments of the environment. These business partners working with the Postal Service have completed information security assessments and after action analysis of varying types and scopes. The business partners contributing were Raytheon/Blackbird Technologies, CMU-SEI-CERT, Deloitte, ICS-CERT, Microsoft, and US-CERT.

Phase 3 Cybersecurity Improvements (Reference Security Architecture)

In preparation for Phase 3, a careful and extensive process (depicted in Figure 1) was conducted in which a wide range of recommendations from the business partner assessments and from other internal and external entities were analyzed. These were combined with recommendations from pertinent OIG audits, PCI compliance requirements, and access control updates related to the FY2014 SOX significant deficiency, resulting in over 600 individual recommendations. Following a careful deduplication and consolidation activity, 178 unique recommendations were identified that must be addressed in order for the U.S. Postal Service to protect the enterprise against advanced cyber threats and ensure continuity of operations.

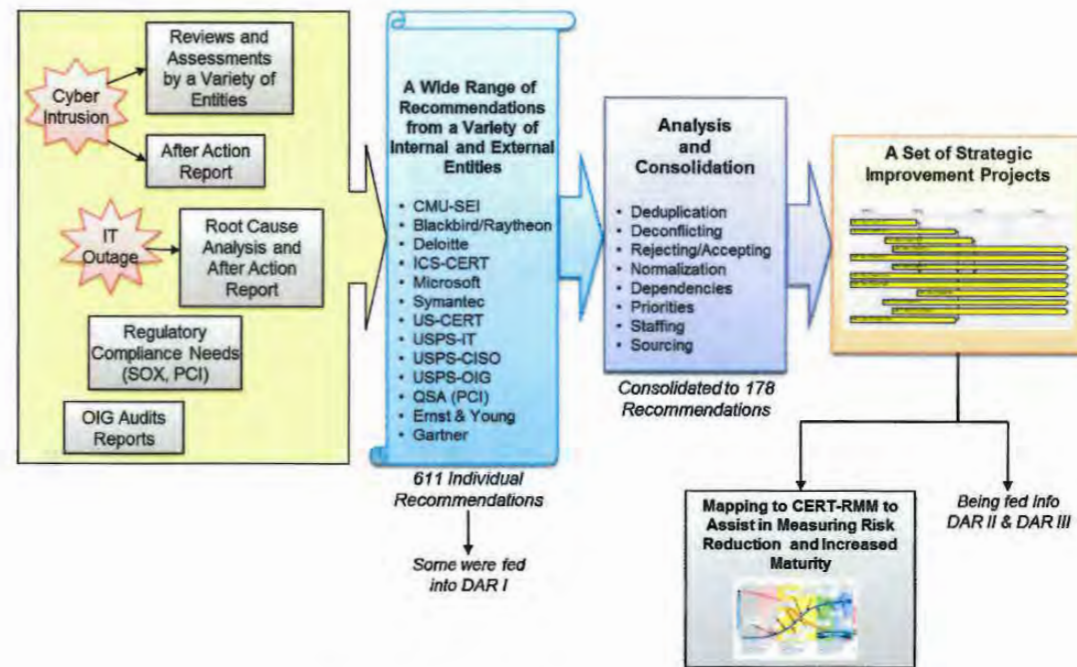


Figure 1 - Analysis of Recommendations

The recommendations were reviewed by multiple industry experts and grouped into 15 projects that provide a strategic security roadmap (see Table 1). This grouping into projects also allowed USPS to:

- Identify lines of responsibility
- Strategically identify risks and dependencies between the various teams (IT, CISO, Engineering, and USPIS)
- Develop appropriate timeframes to track and complete these projects

Table 1 - List of 15 Overarching Improvement Projects

	Project Title	High-Level Description of the Project
1	Cybersecurity Program Development	Develop and revise the USPS enterprise-wide cybersecurity strategy, policies, governance structure, compliance program, and risk management framework.
2	CISO Organizational Structure	Planning, design, and implementation of an expanded CISO organization that can prevent, respond to, and recover from cybersecurity events.
3	Supplier Management	Establish, revise, and manage controls used to ensure the resilience of services and assets provided by external organizations.
4	Current State Assessments	Conduct assessments of the USPS cybersecurity program and related functions to identify gaps, track improvements, and inform risk-based decisions.
5	Cybersecurity Awareness and Training	Promote cybersecurity awareness and develop the skills of personnel responsible for protecting USPS information, systems, and interests.
6	Application, Host, and Network Security	Develop and improve capabilities to provide network visibility, better performance, and efficient management of information systems across USPS.
7	Data Security	Establish and manage controls in support of the confidentiality, integrity, and availability of USPS information.
8	Incident Management, Control, and Response	Develop the capability to identify and analyze events, detect incidents, and determine appropriate organizational responses.
9	Preparedness Planning, Business Continuity, IT Disaster Recovery	Plan for and implement process improvements to ensure continuity of essential operations of services and related assets.
10	Monitoring	Develop capabilities to collect, record, and distribute information about USPS networks, information systems, and critical infrastructure.
11	Threat and Vulnerability Management	Advance the ability to identify, analyze, and manage cybersecurity vulnerabilities and threats in a timely manner.

	Project Title	High-Level Description of the Project
12	Design and Creation of Security Operations Center	Recruit, outsource, and on-board qualified cybersecurity personnel in support of the establishment of a 24/7/365 Security Operations Center.
13	Identity and Access Management	Revise and develop policies and processes related to the creation, maintenance, and deactivation of identities with access to USPS information assets.
14	Asset, Change, and Configuration Management	Improve the ability to identify, document, configure, and manage assets throughout their lifecycle.
15	Physical Security	Develop and manage appropriate physical, environmental, and geographical controls to support USPS operations. Improve the ability to access, store, and protect sensitive information.

Phase 3 activities will improve the security posture of USPS not only through technological enhancements but also in changes to security policy and procedures to ensure a top-down approach for improving the confidentiality, integrity, and availability of USPS data and assets. The projects encompassed will address major gaps across the enterprise, enabling U.S. Postal Service to:

- Improve Management, Governance, Compliance, Education, and Risk Management
- Protect, Shield, and Defend the enterprise from threats and Prevent threats to the enterprise
- Monitor, Detect, and Hunt adversaries on the network
- Respond to and Recover from incidents, and Sustain operations when incidents occur

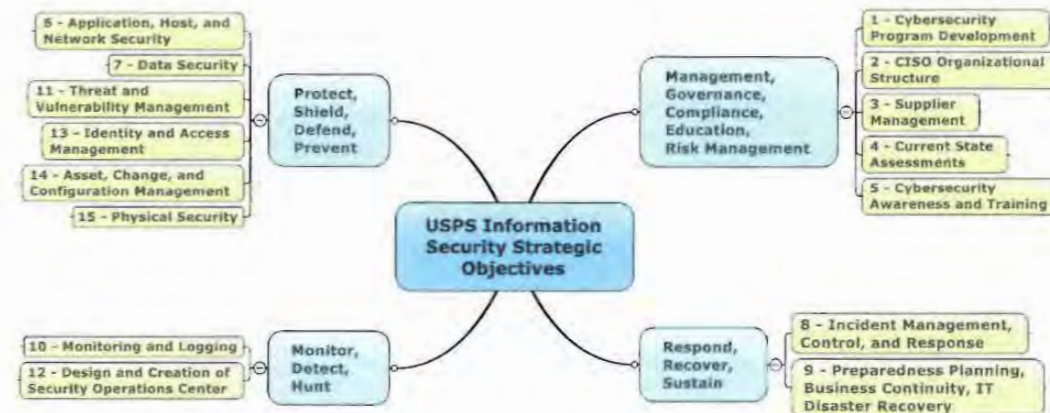


Figure 2 - Grouping of the 15 Projects by USPS Information Security Strategic Objectives

In order to address gaps, and recognizing that many of the projects require significant resources, a redesign of the CISO organizational structure was necessary to align appropriate roles and responsibilities and augment resources to prevent, detect, and respond to threats and ensure operational resilience. The Chief Information Security Officer has obtained approval to significantly expand and improve the organizational structure. Below is the current notional structure.



Figure 3 - Proposed CISO Organizational Structure

In summary, some of the key expected benefits from Phase 3 activities are as follows:

- Remediates the FY2014 SOX significant deficiencies.
- Significantly improves USPS defenses against advanced persistent threats, including the kind behind the 2014 cyber intrusion.
- Improves the manner by which critical employee, customer, and operational data is secured within the enterprise.
- Equips USPS to better analyze, investigate, and respond to incidents that do occur and reduce their impact.
- Initiates training and awareness activities that will create a culture of security throughout USPS and help defeat the kind of attack that caused the 2014 cyber intrusion.
- Strengthens enforcement of USPS cybersecurity policies internally and among suppliers and business partners.
- Addresses a prioritized subset of the 600+ cybersecurity improvement recommendations provided by internal (e.g., USPS-OIG), federal (e.g., DHS's US-CERT), and industry subject matter experts.
- Performs in-depth assessments and architectural studies on both the administrative and the mail processing environments to enable sound decisions about the next set of technology investments that will better support USPS's information security strategic objectives.

Phase 4 Cybersecurity Improvements

Planning for Phase 4 investment will begin in Quarter II of FY2016. Several aspects of Phase 4 will be based on the results of the additional assessments to be conducted in Phase 3, such as a network segmentation redesign that will ensure that enclaves are properly built, flow of traffic is restricted at multiple layers, and auditing is performed to limit the ability for a cyberattack to move laterally through the network. Phase 4 will cover other security enhancements involving people, processes, and technology, including implementation of any of the recommendations not implemented through Phase 3, and will provide for further third-party assessments to validate that security processes and procedures are being followed to thwart advanced attacks.

Recommendation 1:

We recommend the Acting Chief information Officer and Executive Vice President coordinate with the executive leadership team to:

- Develop and execute a strategy based on an organizational risk assessment and determination of the risk tolerance to embed a strong cybersecurity culture into daily operations.

Management Response:

Management agrees with the intent of this recommendation and has already performed detailed risk assessments and developed a cybersecurity strategy. During the intrusion the Postal Service engaged multiple external entities to perform risk assessments and provide subject matter expertise. These included US-CERT, Microsoft, Carnegie Mellon, and USPS OIG to help identify improvements that will enhance USPS cybersecurity capabilities. Following remediation, the Postal Service engaged Ernst and Young, Deloitte, Raytheon and ICS-CERT to conduct assessments focusing on improving cybersecurity within USPS. Some recommendations were addressed as part of the cyber incident remediation plan and others are being addressed as part of the USPS Cybersecurity Strategic Plan.

The Postal Service Cybersecurity Strategic Plan is based on the methodical approach described above to define the 15 areas of cybersecurity improvement for the Postal Service. Information security experts consolidated a wide range of recommendations from the business partner assessments and from other internal and external entities. These were combined with recommendations from pertinent OIG audits, PCI compliance requirements, and access control updates related to the FY2014 SOX significant deficiency, resulting in over 600 individual recommendations. Following a careful deduplication and consolidation activity, 178 unique recommendations were identified that must be addressed in order for USPS to protect the enterprise against advanced cyber threats and ensure continuity of operations. These recommendations have been grouped into 15 projects that provide a strategic security roadmap.

The strategic security roadmap is based on a variety of organizational risk assessments is intended to embed a strong cybersecurity culture into daily operations.

Responsible Management Officials: Acting Chief Information Officer and Executive Vice President and Acting Chief Information Security Officer and Digital Solutions Vice President.

Management requests recommendation number one be reported in the final report as closed.

Recommendation 2:

We recommend the acting chief information officer and executive vice president coordinate with the executive leadership team to:

- Security education, training, and awareness activities to all U.S. Postal Service employees, contractors, and senior leadership.

Management Response:

Management agrees with the intent of this recommendation and has already launched the CyberSafe at USPS security awareness campaign in June 2015. The CyberSafe at USPS campaign focus is to educate the Postal community of employees, suppliers and customers with tips and resources to enhance their understanding of cybersecurity threats and how they can help protect the postal network and information. The Postal Service is leveraging industry experts in the development of content and it is also partnering with the DHS Stop, Think, Connect Campaign and promoting the content that is already available.

CyberSafe at USPS started internally with employees and includes a centralized website with tips and videos, launch of a new web based training focused on password security, how to identify and report phishing attacks and an easy to remember email address to report incidents: cybersafe@usps.gov. This program will expand to include role-based training for those who have access to USPS network and specific awareness messaging and training for suppliers and customers.

The CyberSafe at USPS is one component of a comprehensive cybersecurity organizational training and awareness (OTA) strategy that has been defined and is in the process of being executed. This strategy supports USPS strategic goals by helping to reduce USPS cybersecurity risk through awareness, training and communications activities for USPS employees (and suppliers and customers). Implementing this strategy also supports related cybersecurity goals such as:

- Enable USPS staff to better defend the USPS information networks, secure USPS data, and mitigate mission risks
- Develop and maintain staff and capabilities to manage cyber operations
- Demonstrate USPS's commitment to protection and sustainment of critical enterprise, employee, customer, and supplier information assets
- Contribute to the development of security culture at USPS
- Demonstrate effectiveness through monitoring and measurement of user community network behaviors and activities.

On June 29, 2015, Carnegie Mellon's Software Engineering Institute delivered the "USPS Cybersecurity Organizational Training and Awareness Improvement Strategy".

Target Implementation Date: CyberSafe at USPS awareness and training plan was launched in June 2015. The "USPS Cybersecurity Organizational Training and Awareness Improvement Strategy" will be funded and executed to meet the security education, training, and awareness activities to all U.S. Postal Service employees, contractors, and senior leadership.

Management will implement significant portions of the CyberSafe campaign in FY2016.

Responsible Management Officials: Acting Chief Information Security Officer and Digital Solutions Vice President.

Recommendation 3:

We recommend the Acting Chief Information Officer and Executive Vice President coordinate with the executive leadership team to:

- Separate the joint duties of the chief information security officer and vice president of Digital Solutions and designate a senior-level chief information security officer with information security as the primary duty.

Management Response:

Management will conduct a study to evaluate this recommendation. Information security is the primary responsibility of the Chief Information Security Officer and Digital Solutions Vice President. The study will evaluate best practices made in government and industry for the proper leadership of an information security program.

Management will complete the study by the end of FY2015.

Recommendation 4:

We recommend the acting chief information officer and executive vice president:

- Provide adequate resources for cybersecurity operations, including:
 - Funding commitments to enable proactive prevention, detection, response, and mitigation of sophisticated cyber threats.
 - Provide visibility into fragmented cybersecurity funding to facilitate a coordinated approach to reducing business risk.

Management Response:

Management agrees with the intent of this recommendation. As detailed above, USPS is executing a multi-phase strategic cybersecurity improvement plan that included the investment approval in March 2015 to address immediate remediation. The plan also includes a funding request scheduled for presentation to the USPS Investment Review Committee in August 2015. The cybersecurity improvement plan also includes the coordination with USPS HR to restructure and increase the size of the CISO team through a combination of USPS and contractor resources. In order to address gaps, and recognizing that many of the projects require significant resources, a redesign of the CISO organizational structure is necessary to align appropriate roles and responsibilities and augment resources to prevent, detect, and respond to threats and ensure operational resilience. Cybersecurity Phase II funding will be presented for approval on August 18, 2015.

Target Implementation Date: Cybersecurity Phase II will be funded by September 30, 2015.

Responsible Management Officials: Acting Chief Information Security Officer and Digital Solutions Vice President.

Recommendation 5:

We recommend the Acting Chief Information Officer and Executive Vice President:

- Adequately staff cybersecurity operations functions based on the organization's risk tolerance. Specifically, staffing levels should support business requirements to:
 - Ensure the Security Operations Center provides skilled cyber threat and intrusion analysis and experienced threat remediation and response management staff.
 - Expand Computer Incident Response Team functions to include comprehensive incident management and response, including anomalous activity detection.
 - Create centralized network operations center capabilities and require participation as part of a cybersecurity incident response with the security operations center and Computer Incident Response Team.
 - Expand the existing vulnerability management program to encompass the federal objectives for continuous monitoring, including penetration testing.

Management Response:

Management agrees with the intent of this recommendation. Security professionals from Microsoft, General Dynamics, Raytheon/Blackbird Technologies, Deloitte, Symantec and Hewlett-Packard have been engaged to augment the USPS personnel focused on improving information security. U.S. Postal Service is implementing a significant reorganization of its CISO capabilities to include appropriate staffing level increases and the establishment of a 24/7/365 security operations center (SOC). The SOC contract award will occur in July 2015 and will provide continuous monitoring of internal security events and logs; including real-time monitoring of events, alarms, fault isolation, malicious activity, customer notification, and escalation and service restoration, along with analysis and trending of successful and unsuccessful attacks. The SOC will also expand the CIRT functions to identify, recognize, respond and troubleshoot security issues timely as well as identify current and potential security risks along with recommending mitigation strategies.

The enhanced CISO function will also include expanded:

- Process, procedure and policy writing and compliance testing capabilities
- Security architecture design capabilities
- Threat intelligence capabilities
- Threat detection and response capabilities
- Penetration testing resources and capabilities
- Information security review and accreditation capabilities
- Risk identification, tracking and management capabilities
- Security awareness and training delivery and effectiveness measurement capabilities

Target Implementation Date: The Cybersecurity Phase 3 investments including organizational changes, process enhancements and technology enhancements will be fully implemented by September 2017.

Responsible Management Officials: Acting Chief Information Security Officer and Digital Solutions Vice President.

Recommendation 6:

We recommend the Acting Chief Information Security Officer and Digital Solutions Vice President:

- Develop and implement a plan for the organization to exercise the appropriate governance and incident response.

Management Response:

Management agrees with the intent of this recommendation. As outlined in the previous responses, USPS is implementing significant updates to its cybersecurity capabilities and included are updates to policy, governance and security clearance requirements. Policy documents such as AS-805, the Integrated Emergency Management Plan, the Mass Data Compromise Plan and the Computer Incident Response Team Operations Manual are all included in a governance review and policy update that is planned as a part of Phase 3.

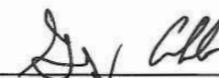
In particular, the Postal Service is planning to strengthen existing governance and compliance practices to ensure that policies and associated standard operating procedures are followed by all business and operational functions at all times. Any business or operational unit seeking a policy exception will be required to request an evaluation and provide justification to the governance structure. Risks associated with any such exception will be assessed and managed as part of the governance process.

The Postal Service is planning to develop and put into practice a comprehensive, enterprise-wide incident management, control, and response process, in which the response activities of USPS-IT, information security, emergency management, and National Preparedness are integrated and coordinated. Such an enterprise-wide incident response process must take into consideration existing independently developed response plans, such as the Mass Data Compromise Response Plan (developed by the USPS information security team), the Response Plan for Breaches involving PII (developed by the USPS Chief Privacy Office), and the USPS Crisis Communications Plan (developed by Corporate Communications). This activity will require significant coordination among internal stakeholders and policy updates.

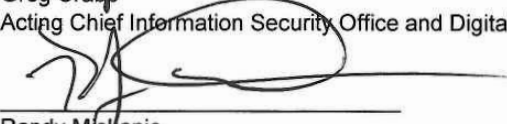
Target Implementation Date: The comprehensive policy review and updates will be completed with many updates being implemented prior to December 31, 2016.

Responsible Management Officials: Acting Chief Information Security Officer and Digital Solutions Vice President.

Responsible Management Officials:



Greg Crabo
Acting Chief Information Security Office and Digital Solutions Vice President



Randy Miskanic
Acting Chief Information Officer and Executive Vice President

- 13 -

cc: Manager, Corporate Audit Response Management



Contact us via our [Hotline](#) and [FOIA](#) forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100