Executive Summary
Table of Contents
Observations
Appendix

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Developing a Successful Enterprise Information Security Policy

White Paper

Report Number
IT-WP-17-001

January 9, 2017

Print

OFFICE OF
INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Executive Summary

An information security policy is a baseline for how an organization plans to protect its information technology resources from threats caused by malicious internal and external attackers.[1] The policy must be flexible enough to change with emerging technologies, while also providing stability for the organization's existing technology resources and data. A successful information security policy safeguards the confidentiality, integrity, and availability of information and protects the organization's personnel, business partners, and the public. Organizations that do not have strong information security policies in place are more susceptible to data loss due to insider threats, corporate espionage, and cyber intrusions.

Developing a successful information security policy is a balancing act; too many security requirements can paralyze an organization, while not having enough can leave the organization vulnerable. Overly restrictive policies can cause business and system owners to develop work-arounds, impeding business activities and weakening security. Proper security measures need to be included in the policy to control and secure information and systems from unauthorized changes, deletions and disclosures, and unplanned outages.

In addition, best practices state that organizations should consider all types of threats when developing an information security policy.[2] While cyber threats caused by malicious attackers attract a lot of media attention, federal agencies and corporations must also protect themselves from other threats such as disgruntled employees, and unawareness or carelessness leading to accidental security exposures.[3] Furthermore, to show a return on investment, a federal agency or corporation should integrate an information security policy into its processes and procedures, and the policy must have the support of the stakeholders expected to follow it.[4]

The Corporate Information Security Office (CISO) is responsible for developing and communicating information security policies to the entire U.S. Postal Service. The CISO has a project underway to redesign its information security policies, procedures, and standards. As part of this effort, the CISO requested the U.S. Postal Service Office of Inspector General (OIG) to review Handbook AS-805, *Information Security*[5] and its supplementary handbooks,[6] which establish its information security policies.

[1] Tech Target, SearchSecurity.com, Definition, Security Policy, May 29, 2007.

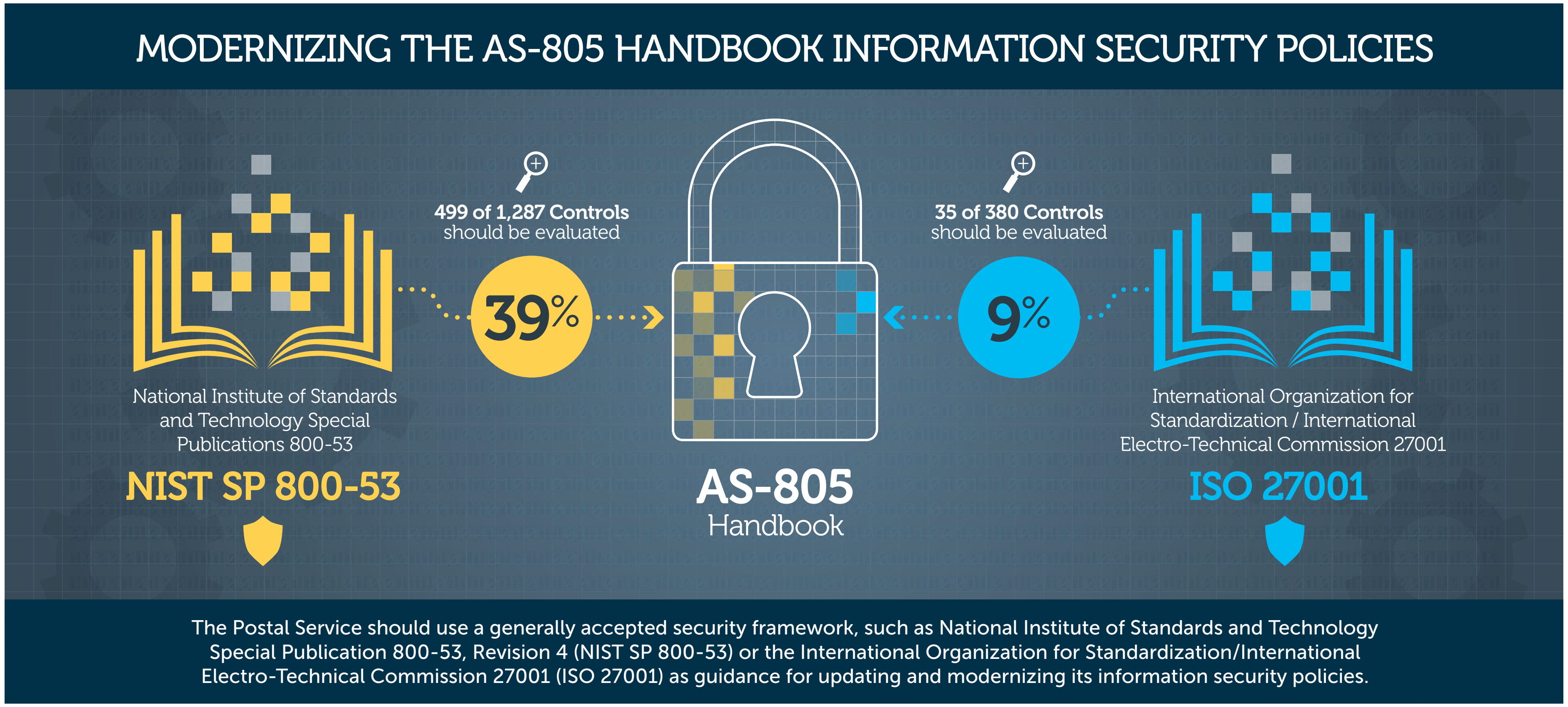
[2] SANS Institute InfoSec Reading Room, Information Security Policy - A Development Guide for Large and Small Companies, © SANS Institute 2007.

[3] SANS Institute InfoSec Reading Room, Information Security Policy - A Development Guide for Large and Small Companies, © SANS Institute 2007.

[4] Tech Target, SearchSecurity.com, Writing a Security Policy, July 21, 2003.

[5] Handbook AS-805, *Information Security*, dated May 2015.

[6] Handbooks AS-805 A, B, C, G, and H are supporting handbooks covering the following areas: Certification and Accreditation, Information Security Assurance, Personnel Security, Mail Processing/Mail Handling Equipment Security, and Cloud Security.



MODERNIZING THE AS-805 HANDBOOK INFORMATION SECURITY POLICIES

The Postal Service should use a generally accepted security framework, such as National Institute of Standards and Technology Special Publication 800-53, Revision 4 (NIST SP 800-53) or the International Organization for Standardization/International Electro-Technical Commission 27001 (ISO 27001) as guidance for updating and modernizing its information security policies.

The OIG has identified two opportunities for transforming the Postal Service's information security policy.

- The Postal Service should use a generally accepted security framework, such as National Institute of Standards and Technology Special Publication 800-53, Revision 4[7] (NIST SP 800-53), or the International Organization for Standardization/International Electro-Technical Commission 27001 (ISO 27001)[8] as guidance for updating and modernizing its information security policies. Following such a framework will ensure the Postal Service will have an effective information security policy that is easy to use and consistent for its users. Many federal agencies and corporations use these frameworks. For example, the Department of Homeland Security uses NIST SP 800-53 to provide a structured approach for managing information security. In addition, the FedEx Security Compliance policy requires its users to comply with ISO standards when processing FedEx Sensitive Data.[9]
- When redesigning the information security policy, an opportunity exists for the Postal Service to modernize its policy. The OIG's comparison of Handbook AS-805 to industry best practices showed that 499 of 1,287 (39 percent) NIST SP 800-53 controls and 35 of 380 (9 percent) ISO 27001 controls should be evaluated for addition to the Postal Service's information security policy.

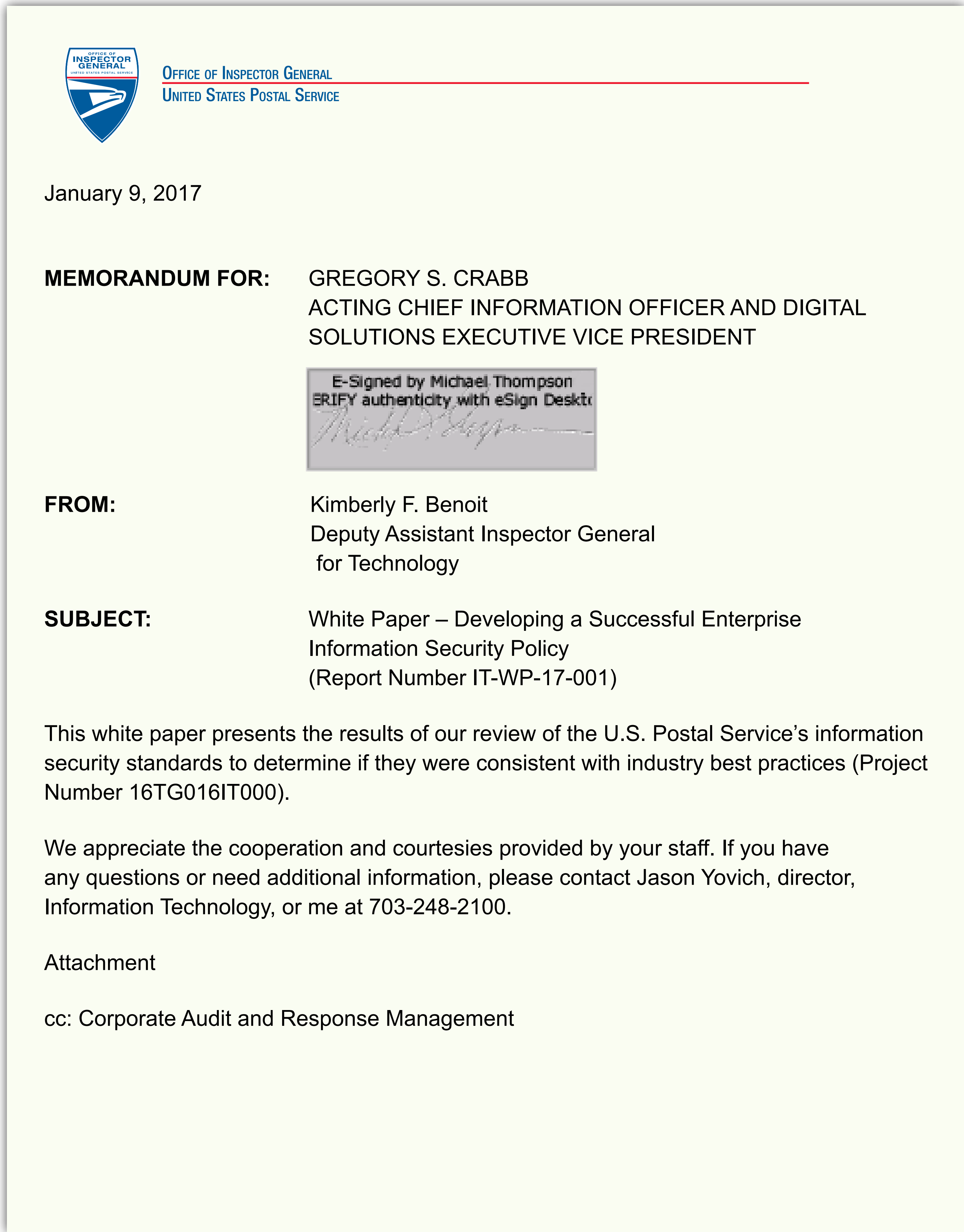
The information security landscape is constantly changing and, as such, it is critical that the Postal Service maintain information security policies that protect its critical applications and infrastructure. With an information security framework based on industry best practices in place, the Postal Service should maintain the confidentiality, integrity, and availability of its information technology.

[7] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013 (includes updates as of January 22, 2015).

[8] ISO/IEC *Information Technology, Security Techniques, Information Security Management Systems Requirements*, Second Edition, dated October 1, 2013.

[9] FedEx Sensitive Data includes personally identifiable information such as individual user passwords, personal identification numbers (PIN), and Social Security numbers.

Transmittal Letter



Office of Inspector General
United States Postal Service

January 9, 2017

MEMORANDUM FOR: GREGORY S. CRABB
ACTING CHIEF INFORMATION OFFICER AND DIGITAL
SOLUTIONS EXECUTIVE VICE PRESIDENT

E-Signed by Michael Thompson
ERIFY authenticity with eSign Deskt

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

SUBJECT: White Paper – Developing a Successful Enterprise
Information Security Policy
(Report Number IT-WP-17-001)

This white paper presents the results of our review of the U.S. Postal Service's information security standards to determine if they were consistent with industry best practices (Project Number 16TG016IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Observations

Introduction

The U.S. Postal Service's information security policies help safeguard the confidentiality, integrity, and availability of its information and protect the interest of its personnel, business partners, and the public. In order to be effective, it is critical that the Postal Service design its security policies in a way that supports effective and efficient operations and allows for ease of implementation. Postal Service Handbook AS-805, *Information Security*,[10] establishes information security policies that identify, classify, and protect the Postal Service's information resources. In addition to Handbook AS-805, there are supplemental handbooks[11] that contain additional requirements; however, Handbook AS-805 and its supplemental handbooks are not well-organized or user friendly to Postal Service business and system owners. By creating a more comprehensive set of policies, the Postal Service would be better able to protect its information systems.

The Corporate Information Security Office (CISO) is responsible for developing and communicating the Postal Service's information security policies. To improve cybersecurity, the CISO has initiated a series of initiatives, which include a redesign of its information security policies, which includes:

- Determining the current state of CISO security policies;
- Rewriting CISO security policies using industry best practices; and
- Establishing a process for creating future security policies.

Many federal agencies and corporations leverage a generally accepted information security framework, such as National Institute of Standards and Technology Special Publication 800-53, Revision 4[12] (NIST SP 800-53), or the International Organization for Standardization/International Electro-Technical Commission 27001[13] (ISO 27001), as guidance for updating and modernizing their information security policies. These are appropriate frameworks for the Postal Service since they are the leaders in providing information technology and security best practices to federal agencies and corporations to use when protecting their information resources. NIST SP 800-53 is organized into 18 control families, including access controls, incident response, system acquisitions, and configuration management. Each control family contains specific security controls related to the general security topic of the family. Similar to NIST SP 800-53, ISO 27001 contains 14 security control groups that, collectively, involve policy, oversight, supervision, manual processes, actions by individuals, and automated mechanisms implemented by information systems.

As part of the effort to redesign its information security policy, the CISO requested the U.S. Postal Service Office of Inspector General (OIG) review the existing Handbook AS-805 and its supplemental handbooks and determine if there were opportunities for improvement.

[10] Handbook AS-805, *Information Security*, dated May 2015.
[11] Handbooks AS-805 A, B, C, G, and H are supporting handbooks covering the following areas: Certification and Accreditation, Information Security Assurance, Personnel Security, Mail Processing/Mail Handling Equipment Security, and Cloud Security.
[12] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated April 2013 (includes updates as of January 22, 2015).
[13] ISO/IEC Information Technology, Security Techniques, Information Security Management Systems Requirements, Second Edition, dated October 1, 2013

Benefits of Using a Framework

As the CISO embarks on its information security policy redesign effort, it is facing a critical decision point for modernizing information security. The OIG believes the Postal Service would benefit from using a framework such as NIST SP 800-53 or ISO 27001 as guidance to update and modernize its information security policies. An industry best practice framework would provide a baseline for an effective information security policy that is easy to use and consistent.

Ease of Use

Handbook AS-805 is a single policy with many sections and sub-sections, which are not well organized, making it difficult for system and business owners to identify and comply with security requirements. The OIG's review found instances where individual controls were addressed in multiple sections of Handbooks AS-805. For example, access control policies are located in twelve different sections of Handbook AS-805, including the *Information Security Services, Account Management, and Controlling Access to Information* sections. In addition, change management control policies are located in ten different sections of Handbook AS-805, including the *Configuration Component Inventory, General Acquisition Policy, and Maintaining Network Asset Controls* sections.

NIST SP 800-53 and ISO 27001 are leaders in providing industry best practices to federal agencies and corporations. In contrast to Handbook AS-805, NIST SP 800-53 and ISO 27001 organize their information security controls by families or groups, which allows for easy navigation by both system and business users, as well as Postal Service suppliers. If the Postal Service organized its policies similarly to these standards, it would be easier to work with its external stakeholders, such as suppliers, who are more familiar with industry best practices rather than the unique Handbook AS-805 requirements. In addition, having a well-organized information security policy would make it easier for CISO to make updates based on need or emerging threats. By better organizing their policies, system and business owners would be able to strengthen their information systems and business functions, reducing the chance for data loss.

Consistency

Inconsistencies between Handbook AS-805 and its supplemental handbooks confuse business and system owners about which controls they should implement. Through the course of our audit work, the OIG has periodically identified these inconsistencies and recommended improvements. For example, the OIG reported[14] that its Engineering Systems used the policies in Handbook AS-805 G[15] instead of the stricter policies in Handbook AS-805, resulting in security deficiencies. The Postal Service should use a framework to establish a single authoritative source for information security requirements by eliminating the supplemental handbooks and centralizing all requirements into a consistent set of policies that align to industry standards. This would reduce the risk of business and system owners selectively implementing information security controls.

Modernizing Information Security Controls

Due to evolving internal and external threats, federal agencies and corporations responsible for critical infrastructure need to have a comprehensive approach for identifying and managing information security risks. Implementing a framework based on industry best practices will ensure the Postal Service establishes a consistent approach to information security that continually meets its business needs. This would also allow the Postal Service to design and implement a comprehensive suite of information security controls and other forms of risk management to address organizational and information technology infrastructure security risks.

[14] *Access Controls over Mail Imaging Systems* (Report Number IT-AR-16-004, dated January 14, 2016).

[15] Handbook AS-805 G, *Information Security for Mail Processing Equipment/Mail Handling Equipment* (MPE/MHE), October 2015.

The Postal Service has a tremendous task ahead in redesigning its information security policies to mirror established industry best practices. Currently, Handbook AS-805 is not well organized or user friendly. To enhance its security posture, the Postal Service should include additional controls in Handbook AS-805. The following section compares Handbook AS-805 to industry best practices; however, as management is embarking on the redesign effort, they must critically evaluate each control and determine its appropriateness to the Postal Service environment.

NIST SP 800-53

Our comparison of Handbook AS-805 to NIST SP 800-53 showed that the Postal Service should evaluate 499 of 1,287 (39 percent) controls for addition to its information security policies as part of its redesign efforts. Handbook AS-805 does not have the enhanced standards one would expect given the criticality of the the Postal Service's key systems. Below are three examples of enhancements Postal Service management should make to Handbook AS-805, based on our assessment of security controls in NIST SP 800-53:

- For Identification and Authentication, manage individual identifiers[16] by uniquely identifying each individual interacting with Postal Service systems. Categorizing the status of individuals by specific characteristics provides additional information about the people with whom Postal Service personnel are communicating.

- For Incident Response, perform testing to determine incident response effectiveness. The Postal Service should test its incident response capabilities to determine the overall effectiveness of its capabilities and to identify potential weaknesses or deficiencies.

- For System and Services Acquisition, establish policies and procedures for the effective implementation of security controls. Having security program policies and procedures at the organization level would allow the Postal Service to reduce or eliminate the need for system-specific policies and procedures.

Table 1 shows our comparison of NIST SP 800-53 controls to Handbook AS-805 and its supplemental handbooks.

[16] Characteristics identifying the status of individuals, such as contractors and foreign nationals.

Table 1: Comparison of NIST SP 800-53 Controls to Handbook AS-805

		Included[17] in	Not Included[18] in	Percentage
NIST SP 800-53 Control Families	Number of Controls	Handbook AS-805	Handbook AS-805	Not Included
Access Control (AC)	175	107	68	38.9%
Audit and Accountability (AU)	74	44	30	40.5%
Awareness and Training (AT)	18	16	2	11.1%
Configuration Management (CM)	90	60	30	33.3%
Contingency Planning (CP)	76	51	25	32.9%
Identification & Authentication Policy (IA)	81	42	39*	48.1%
Incident Response (IR)	60	14	46	76.7%
Maintenance (MA)	52	42	10	19.2%
Media Protection (MP)	34	30	4	11.8%
Personnel Security (PS)	42	32	10	23.8%
Physical & Environmental Protection (PE)	76	48	28	36.8%
Planning (PL)	34	28	6	17.6%
Risk Assessment Policy & Procedures (RA)	28	17	11	39.3%
Security Assessment & Authorization (CA)	42	30	12	28.6%
System & Communications Protection (SC)	137	85	52	38.0%
System and Information Integrity (SI)	118	65	53	44.9%
System and Services Acquisition (SA)	150	77	73	48.7%
Totals	**1,287**	**788**	**499**	
Percentage		**61%**	**39%**	

Source: OIG evaluation of Handbook AS-805 (including its supplemental handbooks) and NIST SP 800-53.

* The 'Not Included' figure contains seven controls related to Federal Identity, Credential, and Access Management (FICAM) and federal Personal Identity Verification (PIV), which do not apply to the Postal Service.

ISO 27001

Our comparison of Handbook AS-805 to ISO 27001 showed that the Postal Service should evaluate 35 of 380 (9 percent) controls for addition to its information security policies. Below are two examples of security controls the Postal Service could add based on our analysis of ISO 27001:

- Supplier Relationship, which mitigates risks associated with granting a supplier access to Postal Service information system resources. By having a supply chain process that limits information system access, the Postal Service would reduce the likelihood of unauthorized modifications at each stage in the supply chain.

- Compliance satisfies all legal, regulatory or contractual requirements related to information systems security. Postal Service policies and procedures should reflect all applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance regarding information systems security.

[17] "Included" indicates the OIG auditor determined that Handbook AS-805 nor its supplemental handbooks address the control.
[18] "Not Included" indicates the OIG auditor determined that neither Handbook AS-805 nor its supplemental handbooks address the control.

Table 2 shows our comparison of Handbook AS-805 to ISO 27001.

Table 2: Comparison of ISO 27001 Controls to Handbook AS-805

ISO 27001 Controls	Number of Controls	Included in Handbook AS-805	Not Included in Handbook AS-805	Percentage Not Included
A.5 Information Security Policies	34	34	0	0.0%
A.6 Organization of information security	34	34	0	0.0%
A.7 Human Resources Security	15	15	0	0.0%
A.8 Asset Management	24	22	2	8.3%
A.9 Access Control	29	28	1	3.4%
A.10 Cryptography	3	3	0	0.0%
A.11 Physical and environmental security	46	41	5	10.9%
A.12 Operations security	48	48	0	0.0%
A.13 Communications security	26	23	3	11.5%
A.14 System acquisition, development and maintenance	38	33	5	13.2%
A.15 Supplier Relationships	6	3	3	50.0%
A.16 Information security incident management	12	11	1	8.3%
A.17 Information security aspects of business continuity management	12	10	2	16.7%
A.18 Compliance	53	40	13	24.5%
Totals	**380**	**345**	**35**	
Percentage		**90.8%**	**9.2%**	

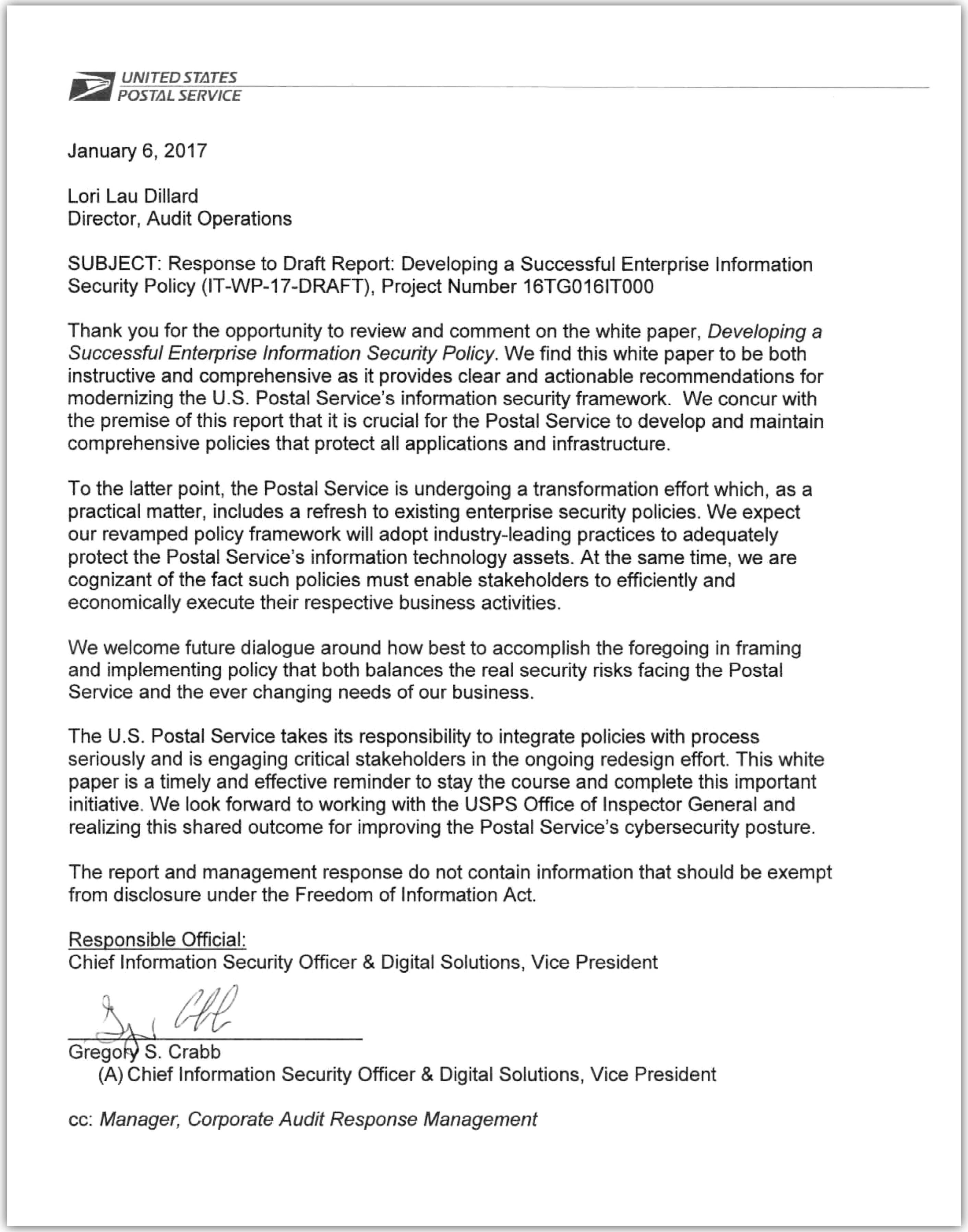
Source: OIG evaluation of Handbook AS-805 (including its supplemental handbooks) and ISO 27001.

The additional information security controls we identified would fundamentally strengthen the Postal Service's information systems and the environments in which those systems operate. If the Postal Service does not incorporate these controls into their security baseline, core business functions may be subject to a cyber intrusion resulting in data loss.

Conclusion – The Time to Modernize is Now

The information security landscape is constantly evolving and, as such, it is vital that the Postal Service maintain information security policies that protect its information systems. By updating its information security policies, the Postal Service will improve business and system owners' ease of use, provide consistent policy application, and modernize the overall security posture of the Postal Service. With an information security framework based on industry best practices in place, the Postal Service would ensure that it maintains confidentiality, integrity, and the availability of information technology.

Appendix A: Management's Comments



UNITED STATES
POSTAL SERVICE

January 6, 2017

Lori Lau Dillard
Director, Audit Operations

SUBJECT: Response to Draft Report: Developing a Successful Enterprise Information Security Policy (IT-WP-17-DRAFT), Project Number 16TG016IT000

Thank you for the opportunity to review and comment on the white paper, *Developing a Successful Enterprise Information Security Policy*. We find this white paper to be both instructive and comprehensive as it provides clear and actionable recommendations for modernizing the U.S. Postal Service's information security framework. We concur with the premise of this report that it is crucial for the Postal Service to develop and maintain comprehensive policies that protect all applications and infrastructure.

To the latter point, the Postal Service is undergoing a transformation effort which, as a practical matter, includes a refresh to existing enterprise security policies. We expect our revamped policy framework will adopt industry-leading practices to adequately protect the Postal Service's information technology assets. At the same time, we are cognizant of the fact such policies must enable stakeholders to efficiently and economically execute their respective business activities.

We welcome future dialogue around how best to accomplish the foregoing in framing and implementing policy that both balances the real security risks facing the Postal Service and the ever changing needs of our business.

The U.S. Postal Service takes its responsibility to integrate policies with process seriously and is engaging critical stakeholders in the ongoing redesign effort. This white paper is a timely and effective reminder to stay the course and complete this important initiative. We look forward to working with the USPS Office of Inspector General and realizing this shared outcome for improving the Postal Service's cybersecurity posture.

The report and management response do not contain information that should be exempt from disclosure under the Freedom of Information Act.

Responsible Official:
Chief Information Security Officer & Digital Solutions, Vice President

Gregory S. Crabb
(A) Chief Information Security Officer & Digital Solutions, Vice President

cc: *Manager, Corporate Audit Response Management*

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

U.S. Postal Service Office of Inspector General
1735 N. Lynn Street
Arlington, VA 22209

Telephone: 703-248-2100
www.uspsoig.gov

For media inquiries, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov