UNITED STATES
POSTAL SERVICE™

Information Resource
Business Impact Assessment (BIA)

Version 5.10

July 27, 2011

Corporate Information Security Office
United States Postal Service
Raleigh, North Carolina

TABLE OF CONTENTS

1 INTRODUCTION

This document includes background information, roles and responsibilities, and instructions for completing the Information Resource Business Impact Assessment (BIA) Questionnaire.

Certification and Accreditation— Process that evaluates the security of information resources so that risks can be managed through their lifecycle.

The Questionnaire is attached as Appendix A. An information systems security officer (ISSO) will be assigned to provide guidance and consulting support.

1-1 WHAT THE INFORMATION RESOURCE BIA APPLIES TO

The BIA Questionnaire can encompass multiple business processes or focus on one particular aspect of the business.

1-2 WHAT INFORMATION RESOURCES ARE AFFECTED

A BIA must be completed for all information resources, regardless of whether they are developed in-house, out-sourced, or hosted in non-Postal Service facilities.

1-3 PURPOSE

The purpose of the BIA is to determine compliance with the privacy requirements, determine sensitivity and criticality, and determine the appropriate security requirements to protect the information resource.

1-4 DETERMINATION OF COMPLIANCE WITH PRIVACY REQUIREMENTS

The BIA ensures that programs involving customer or personnel information, or technologies that can be used for monitoring purposes adhere to Postal Service privacy requirements. Privacy requirements are based on applicable privacy laws, such as the Privacy Act, as well as privacy policies that the Postal Service has adopted. Compliance with privacy requirements is addressed in Section 2 of the BIA Questionnaire.

1-5 DETERMINATION OF SENSITIVITY

Sensitivity determines the level of security control requirements necessary to protect the confidentiality and integrity of the information. The levels of sensitivity are: non-sensitive, sensitive, sensitive-enhanced, and classified.

1-5.1 NON-SENSITIVE INFORMATION

Information that is not designated as classified, sensitive-enhanced, or sensitive is by default designated as non-sensitive information. An example is publicly available information. Even though information is designated as non-sensitive, it must still be protected (i.e., baseline requirements apply to all Postal Service information).

Privacy Requirements— Protection necessary to adequately meet applicable privacy laws and policies.

1-5.2 SENSITIVE INFORMATION

Sensitive information is hardcopy or electronic information or material that is not designated as classified or sensitive-enhanced, but that requires protection. Requirements to protect sensitive information are derived from law, regulation, the Privacy Act of 1974 as amended, business needs, and the contracting process. Types of sensitive information include:

a. Private information about individuals (e.g., employees, contractors, vendors, business partners, and customers) including race, marital status, age, birth date, and buying habits

b. Confidential business information that does not warrant enhanced protection including trade secrets, proprietary information, financial information, contractor bid or proposal information, and source selection information

c. Data susceptible to fraud, including accounts payable, accounts receivable, payroll, and travel reimbursement

d. Information illustrating or disclosing information resource protection vulnerabilities, or threats against persons, systems, operations, or facilities such as physical, technical or network/DMZ/enclave/mainframe/server/workstation specifics including security settings, passwords, audit logs

1-5.3 Sensitive-Enhanced Information

Sensitive-enhanced information is hardcopy or electronic information or material that is not designated as classified, but that warrants or requires enhanced protection. Types of sensitive-enhanced information include:

a. Personal identifiers (i.e., identify individuals in a recognizable form including social security numbers, driver license numbers, passport number, fingerprints, and other biometric information) and information about individuals (e.g., employees, contractors, vendors, business partners, and customers) protected by law including medical information and wire or money transfers

b. Information related to the protection of Postal Service restricted financial information, trade secrets, proprietary information, and emergency preparedness

c. PCI PAN (full credit card number) and sensitive authentication data

d. Law enforcement information and court restricted information, including grand jury material, arrest records, and information regarding ongoing investigations

e. Communications protected by legal privileges (e.g., attorney-client communications encompassing attorney opinions based on client-supplied information) and documents constituting attorney work products (created in reasonable anticipation of litigation)

1-5.4 Classified Information

Classified information is hardcopy or electronic information or material that has been designated as classified pursuant to Executive Order, statute, or regulation and requires protection against unauthorized disclosure for reasons of national security. Classified information must never be entered into any information resource that is (or may become) a part of or connected to the Postal Service information technology infrastructure.

1-6 Determination of Criticality

Criticality determines the need for continuous availability of the information. The levels of criticality are: non-critical (low) and critical (moderate and high).

1-6.1 Non-Critical Information Resource

Information that is not designated as critical-moderate or critical-high is by default designated as non-critical.

1-6.2 CRITICAL INFORMATION RESOURCE

Information is designated as critical if its unavailability would have a significant negative impact on a major business function including:

Security Requirements— Protection necessary to adequately secure the information resource.

a. Protecting customer or personnel life, safety, or health

b. Paying suppliers and employees

c. Collecting revenue (getting revenue, customer and business mailer services) or protecting revenue

d. Managing the movement of mail (transportation, logistics, delivery, and retail)

e. Communications (Postal alert and messaging systems)

f. Infrastructure services (data transfer, administrative services, and support systems)

An application may also be designated as critical if a critical application is dependent on this application for input.

1-7 DETERMINATION OF INFORMATION SECURITY REQUIREMENTS

The BIA determines the information security requirements for an information resource. The security requirements will vary with the applicability of federal legislation, regulations, and directives as well as industry requirements; the computing environment; the responses to the questions in the BIA Questionnaire; and the information resource's sensitivity and criticality designation. If any of the requirements are in conflict, the most restrictive requirement applies. The executive sponsor assumes the risks associated with not implementing the information security requirements, where permitted.

1-7.1 BASELINE INFORMATION SECURITY REQUIREMENTS

All information resources must implement controls sufficient to satisfy the baseline information security requirements. Baseline security requirements protect the postal computing environment and infrastructure from intentional or unintentional unauthorized use, modification, disclosure, or destruction.

1-7.2 SENSITIVE INFORMATION SECURITY REQUIREMENTS

Information resources processing sensitive information (e.g., private information about individuals, confidential business information, data susceptible to fraud, or information resource protection information) must implement baseline and sensitive information security requirements.

1-7.3 SENSITIVE-ENHANCED SECURITY REQUIREMENTS

Information resources processing sensitive-enhanced information (e.g., law enforcement information, court restricted information, or cardholder information) must implement baseline, sensitive, and sensitive-enhanced security requirements.

1-7.3.1 PCI Information Security Requirements

Information resources designated as PCI In-Scope must implement baseline, sensitive, sensitive-enhanced, and PCI information security requirements.

1-7.3.2 Law Enforcement Information Security Requirements

Information resources processing law enforcement information must implement baseline, sensitive, sensitive-enhanced, and law enforcement information security requirements.

1-7.4 Critical-Moderate Information Security Requirements

Information resources designated as critical-moderate must implement baseline and critical-moderate information security requirements.

1-7.5 Critical-High Information Security Requirements

Information resources designated as critical-high must implement baseline, critical-moderate, and critical-high information security requirements.

1-7.6 Conditional Information Security Requirements

If requested by the CIO, VP IT Operations, Manager CISO, or Functional VP, information resources must implement the indicated conditional information security requirements. Also, based on specific criteria the ISSO may recommend conditional information security requirements.

1-7.7 ISSO Recommended Information Security Requirements

ISSOs may recommend additional information security requirements during the BIA based on threats and vulnerabilities or generally accepted industry practices to better protect information resources. If any of these additional mandatory requirements conflict with the requirements included in Handbook AS–805, the most restrictive or protective requirement applies.

Information Security Requirements By Classification

	Information Security Requirements								
Classification Category	**Baseline**	**Sensitive**	**Sensitive-Enhanced**	**PCI**	**Law Enforcement**	**Critical-Moderate**	**Critical-High**	**Conditional**	**ISSO Recommended**
All Information Resources	X								
Non-Sensitive & Non-Critical	X							Con	Rec
Sensitive	X	X						Con	Rec
Sensitive-Enhanced	X	X	X					Con	Rec
PCI	X	X	X	X				Con	Rec
Law Enforcement	X	X	X		X			Con	Rec
PCI & Law Enforcement	X	X	X	X	X			Con	Rec
Critical-Moderate	X					X		Con	Rec
Critical-High	X					X	X	Con	Rec

X = Required

Con = If box is checked

Rec = If recommended by ISSO

1-8 When to Perform the BIA

The Information Resource BIA Questionnaire is completed in the Phase 2, Requirements, of the Technical Solution Life Cycle (TSLC). It must be updated periodically throughout the TSLC. (See Chapter 6, Re-Initiating the C&A in Handbook AS-805-A, Information Resource Certification and Accreditation (C&A) Process for the specific criteria.)

1-9 BIA Process Metrics

Following are the process metrics for official classification of information resources:

a. The ISSO completes the BIA process in the Requirements Phase with the Executive Sponsor and Portfolio Manager or their designees.

b. ISSO will include the Privacy Office who will provide guidance on the completion of the privacy compliance section and sensitivity determination section of the BIA process.

c. ISSO will include the Business Continuity Group who will particate in the completion of the criticality determination section of the BIA process.

d. The ISSO may also include the Treasury Department.

e. The Executive Sponsor, Portfolio Manager, Privacy Officer (or their designees) and ISSO all sign BIA within 10 days.

f. After the document is signed, the ISSO enters the information resource sensitivity designation in EIR within 48 business hours.

g. After the document is signed, the Business Continuity Representative enters the information resource criticality designations in EIR within 48 business hours.

h. The information resource is now classified officially and the sensitivity and criticality designations are the ONLY classification designations to be used in all subsequent discussions regarding funding, Disaster Recovery, Code Reviews, etc.

1-10 Benefits of the BIA Process

The benefits of the BIA process are as follows:

a. A structured and cost effective methodology that yields consistent and repeatable results.

b. Clear, succinct guidelines to ensure privacy compliance at an appropriate phase of the business planning process.

c. Determination of appropriate sensitivity and criticality designation.

d. Determination of information resource dependencies.

e. The focusing of security requirements on information resource sensitivity, criticality, function, and environment.

f. A risk-based approach that empowers business owners to select controls to satisfy the requirements based on the business risk.

g. Early determination of security requirements that can be integrated into plans, costs, design, development, and testing of information resources.

2 ROLES AND RESPONSIBILITIES

2-1 Executive Sponsors

Executive sponsors are the business managers with oversight (funding, development, production, and maintenance) of the information resources, and are responsible for the following:

a. Ensuring appropriate privacy and adequate security of their information resources.

b. Understanding potential threat events, risks, business impacts, and assets associated with their information resources.

c. Consulting with the chief privacy officer (CPO) on privacy requirements and the determination of information sensitivity.

d. Consulting with the manager of Business Continuance Management on business continuity requirements and the determination of criticality.

e. Providing financial and personnel resources to complete the BIA processes.

f. Engaging business partners as required.

Threat event— Something external to the information resource by which the confidentiality, integrity, and availability of information could be compromised.

Risk— The chance or possibility of harm being caused to the business as a result of a loss of the confidentiality, integrity, or availability of an information resource.

2-2 Portfolio Managers

Portfolio managers are responsible for the following:

a. Functioning as the liaison between executive sponsors and the information technology providers.

b. Supporting the executive sponsor in the completion of the BIA.

c. Ensuring appropriate privacy and adequate security is built into the information resources.

d. Understanding potential threat events, risks, business impacts, and assets associated with the information resources.

Business Impacts— Potential business consequences as a result of a loss of the confidentiality, integrity, or availability of an information resource.

Assets— Things of value that contribute to the capability of the information resource to achieve its business function.

Portfolio managers may designate other postal project managers to perform security-related activities in their behalf.

Designated engineering managers assume the role of portfolio manager for their own projects which are not done under direct IT management.

2-3 IBSSC Managers

IBSSC managers are responsible for the following:

a. Ensuring the technology solution meets the information security requirements defined by the BIA.

b. Ensuring the technology solution follows Postal Service development requirements defined in the TSLC process.

c. Managing the implementation and maintenance of the technology solution in their IBSSC.

2-4 Project Managers

Project managers are responsible for information resources development and implementation, and acquisition and integration. If an information systems security representative is not assigned, the project manager assumes those security responsibilities.

2-5 INFORMATION SYSTEMS SECURITY REPRESENTATIVES

An information systems security representative (ISSR) may be assigned by the executive sponsor or portfolio manager to perform security-related activities on their behalf. The role of the ISSR is an ad hoc responsibility performed in conjunction with assigned duties.

An ISSR provides support to the executive sponsor and portfolio manager during the completion of the BIA as required.

2-6 INFORMATION SYSTEMS SECURITY OFFICERS

Information systems security officers (ISSOs) are responsible for the following:

a. Coordinating the completion of a BIA for each information resource.

b. Providing advice and consulting support to executive sponsors and portfolio managers during the BIA process regarding the baseline security requirements that apply to all information resources and the security requirements required to protect an information resource based on the sensitivity and criticality designation.

c. Specifying additional security requirements based on risks determined during the risk assessment process, the discovery of vulnerabilities at any time during the information resource lifecycle, or on generally accepted industry practices.

2-7 EXECUTIVE SPONSOR DESIGNEES

Executive sponsors may designate in writing Postal Service employees to perform security-related activities on their behalf. However, ultimate accountability and responsibility reside with the executive sponsor.

2-8 CHIEF PRIVACY OFFICER

The CPO is responsible for the following:

a. Providing guidance on completing the privacy compliance section of the BIA Questionnaire.

b. Providing assistance to ensure compliance with privacy requirements.

c. Consulting on and reviewing the sensitivity determination section of the BIA and approving the determination of sensitivity.

2-9 BUSINESS CONTINUITY GROUP

The Business Continuity organization is responsible for consulting on business continuity requirements and participating in the completion of the criticality determination section of the BIA. Based on discussions with the project team, application owner, and Postal Service senior management, information resources will be designated as non-critical, critical-moderate, or critical-high.

3 INSTRUCTIONS FOR COMPLETING THE BIA QUESTIONNAIRE

Enter the information requested on the cover page of the BIA Questionnaire and in the header and footer. The Questionnaire is composed of the following sections:

1. *Project Identification* – identifies the contact information for the responsible parties and development/production information.
2. *Privacy Compliance* – documents compliance with privacy requirements, including laws and Postal Service policy.
3. *General Data Attributes* – documents data types, sources, access, sharing, and retention.
4. *Determination of Criticality* – establishes the criticality level associated with integrity (i.e., the correctness of information resource operation and the consistency and accuracy of information) and unavailability (i.e., the importance of each information resource relative to the overall mission of the Postal Service).
5. *Determination of Sensitivity* – establishes the sensitivity level associated with integrity and confidentiality (i.e., the sensitivity of the data collected and importance of each information resource relative to disclosure).
6. *Information Security Requirements To Be Implemented* – documents the baseline, sensitive, sensitive-enhanced, PCI, law enforcement, critical-moderate, critical-high, conditional, and ISSO recommended information security requirements for adequately securing the information resource.
7. *BIA Approvals*
    a. *Executive Sponsor Validation* – documents executive sponsor (or their designee) acknowledgement of the accuracy of the information collected in the BIA and the need to fund the development and maintenance of information security controls to satisfy the information security requirements for the information resource.

    b. *IT Acceptance of Responsibility* – documents portfolio and IBSSC manager or Engineering PCES manager acceptance of responsibility for implementing security controls which will satisfy the information security requirements for the information resource.

    c. *Privacy Office Verification* – documents the Privacy Official who reviewed the BIA for privacy compliance and sensitivity determination.

    d. *ISSO Certification* – documents the ISSO who coordinated the completion of the BIA and presented the information security requirements to the portfolio manager for inclusion in the TSLC requirements document for implementation during the development/integration process.

Instructions for completing each section of the BIA Questionnaire are detailed below.

SECTION 1 PROJECT IDENTIFICATION

In Section 1:

a. Enter *Contact Information* for responsible parties.

b. Enter *Development and Production Information*.

c. A major information system is defined as a system that requires special attention because of its importance to the Postal Service mission; its high development, operating, or maintenance costs; or its significant role in the administration of Postal Service programs, finances, property, or other resources.

SECTION 2 PRIVACY COMPLIANCE

In Section 2:

a. Answer questions by checking the appropriate boxes and providing the information requested.

b. Contact the CPO or designee if there are any questions regarding this section. The CPO is available to provide guidance via email or telephone.

c. If the CPO or designee was not represented during the completion of the BIA, the CPO will review the completed BIA Questionnaire, and if there are issues regarding privacy compliance or the information resource sensitivity designation, the CPO will contact the ISSO to get clarification or to arrange a teleconference with the executive sponsor.

SECTION 3 GENERAL DATA ATTRIBUTES

Complete Section 3-1, *Collected Data Types*, by checking the boxes that apply*.*

Complete Section 3-2, *Data Sources*, by checking the boxes that apply*.*

Complete Section 3-3, *Data Access*, by checking the boxes that apply*.*

Complete Section 3-4, *Data Sharing*, by checking the boxes that apply*.*

SECTION 4 DETERMINATION OF CRITICALITY

Complete Section 4-1, *Initial or Current Criticality Determination*, by checking any of the boxes that apply to the information resource.

Complete Section 4-2, *Identify Essential Business Functions*, by checking any of the boxes that apply to the information resource.

Complete Section 4-3, *Rationale for Criticality, by providing a brief resonse to each of the questions.*

Complete Section 4-4, *Business Continuity Criticality Determination*, by checking any of the boxes that apply to the information resource.

SECTION 5 DETERMINATION OF SENSITIVITY

Complete Section 5-1, *Data Element Sensitivity Designation*, by checking the elements in the following subsections:

- *Non-Sensitive*
- *Sensitive*
- *Sensitive-Enhanced*
  - *PCI*
  - *Law Enforcement*

Note: In the *Personal Information* subsection, the checked blocks with one asterisk will be considered sensitive only if they can be associated with name or other personal identifier (e.g., Social Security Number, Email address). For example, Birth Date/Age is considered sensitive if it can be associated with a name or other personal identifier.

Complete Section 5-2, *Impact of Unauthorized Use*, by checking the box that best reflects the impact to the Postal Service or the individual if the information is subject to unauthorized use. Note the impact should take into account the size of the Postal Service; i.e., a few thousand dollars fraud would have little impact unless the incident hits the newspaper. If an impact box is checked, the information resource is sensitive.

Complete Section 5-3.1, *PCI-Scope Determination*. The determination of whether an application is in-scope for PCI goes beyond the information being processed and includes shared resources and location on the network. To ensure the accuracy of the application determination, an assessment of the PCI information collected, stored, processed or transmitted by the application and the associated databases must be determined prior to the application BIA meeting. Discuss data elements stored, internal and external application dependencies, server(s) hosting the application, and network connectivity with Development Team. The PCI in-scope determination requires consideration of number of factors including data elements stored, processes, databases, hosting servers, and network connectivity.

Complete Section 5-3.2, *Justification for PCI-Scope Designation*. If either of the In-Scope boxes is checked, provide the reason for the designation and cite the documentation reviewed to arrive at this designation and the source of the documentation.

Complete Section 5-4, *Additional Sensitivity Impact Information*, by checking “Yes” or “No”. If checked “Yes”, please describe.

Complete Section 5-5, *Sensitivity Determination Summary*, as follows:

a. Section 5-1, *Data Element Sensitivity Designation*, Section 5-2, *Impact of Unauthorized Use*, Section 5-3, *PCI Scope Determination*, and Section 5-4, *Additional Sensitivity Impact Information*, should be considered together to determine information resource designation.

b. If there are questions, contact the CPO for privacy-related issues and the Treasury Department for PCI-related issues for assistance in making the determination.

SECTION 6 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED

Section 6-1, *Baseline Security Requirements*

All information resources must implement baseline security requirements to protect the Postal Service infrastructure.

Section 6-2, *Sensitive Information Security Requirements*

Information resources processing **sensitive information** must implement the following requirements:

1. Baseline security requirements
2. Sensitive information security requirements
3. Conditional information security requirements (if any)
4. ISSO-recommended security requirements (if any)

Section 6-3, *Sensitive-Enhanced Security Requirements*

Information resources processing **sensitive-enhanced information** must implement the following requirements:

1. Baseline security requirements
2. Sensitive information security requirements
3. Sensitive-enhanced security requirements
4. Conditional information security requirements (if any)
5. ISSO-recommended security requirements (if any)

Section 6-4, *PCI Information Security Requirements*

Information resources designated as **PCI In-Scope** must implement the following requirements:

1. Baseline security requirements
2. Sensitive information security requirements
3. Sensitive-enhanced security requirements
4. PCI security requirements
5. Conditional information security requirements (if any)
6. ISSO-recommended security requirements (if any)

Section 6-5, *Law Enforcement Information Security Requirements*

Information resources processing **law enforcement information** must implement the following requirements:

1. Baseline security requirements
2. Sensitive information security requirements
3. Sensitive-enhanced security requirements
4. Law enforcement information requirements
5. Conditional information security requirements (if any)
6. ISSO-recommended security requirements (if any)

Section 6-6, *Critical-Moderate Security Requirements*

Information resources processing **critical-moderate information** must implement the following requirements:

1. Baseline security requirements
2. Moderate critical information security requirements
3. Conditional information security requirements (if any)
4. ISSO-recommended discretionary security requirements (if any)

Section 6-7, *Critical-High Security Requirements*

Information resources processing **critical-high information** must implement the following requirements:

1. Baseline security requirements
2. Moderate critical information security requirements
3. High critical information security requirements
4. Conditional information security requirements (if any)
5. ISSO-recommended discretionary security requirements (if any)

Section 6-8, *Conditional Information Security Requirements*

Check the independent processes to be conducted based on specific information resource development and implementation criteria.

Note: Independent processes are evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to information resources. An independent process is conducted by an internal or external organization that is separate and distinct from those responsible for the development and operation of the information resource and strictly adheres to the separation of duties policy.

Section 6-9, *ISSO Recommended Information Security Requirements*

ISSOs may identify additional information security requirements during the BIA based on threats, vulnerabilities, and generally accepted industry practices to better protect information resources.

SECTION 7 BIA APPROVALS

There are two approval forms. One is for non Engineering information resources or technology solutions and the other is for Engineering information resources or technology solutions. The executive sponsor or designee signs and enters today's date. The portfolio manager and ISBBC manager (as applicable) sign and date the BIA accepting responsibility to implement the security requirements identified for non-Engineering information resources or technology solutions and the Engineering PCES manager signs and dates for Engineering information resources or technology solutions.

The Privacy Official signs and dates for privacy compliance and sensitivity determination.

The ISSO signs and dates certifying that BIA has been completed and the security requirements have been presented to the portfolio and IBSSC managers or the Engineering PCES manager for inclusion in the Technology Solution requirements.

BIA WRAP UP

File the Information Resource BIA Questionnaire with the C&A documentation package.

Forward a copy of the completed and signed BIA Questionnaire to the CPO and CISO at the following addresses:

Chief Privacy Officer
U.S. Postal Service
475 L'Enfant Plaza SW
Washington, DC 20260-4377

Corporate Information Security Office
ATTN: C&A Program Manager
475 L'Enfant Plaza SW, Room 2141
Washington, DC 20260-2141

This template is for instructional purposes only, use the eC&A application to create official C&A documentation.

UNITED STATES POSTAL SERVICE™

Business Impact Assessment (BIA) Questionnaire

INFORMATION RESOURCE NAME: ______________________________

EIR NUMBER: ______________________________

INFORMATION RESOURCE FINANCE NUMBER: ______________________________

LEVEL OF SENSITIVITY: ______________________________

LEVEL OF CRITICALITY: ______________________________

DATE: ______________________________

TABLE OF CONTENTS

Version 5.10

July 27, 2011

1 PROJECT IDENTIFICATION

CONTACT INFORMATION			
Functional Vice President:		**Other:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
Executive Sponsor:		**Executive Sponsor Designee:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
Portfolio Manager:		**Portfolio Manager Designee:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
IBSSC Manager:		**Project Manager:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
ISSO:		**ISSR:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
Privacy Office Designee:		**Business Continuity Management Designee:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
DEVELOPMENT AND PRODUCTION INFORMATION			
Development Organization:			
Development Site:			
Production Site(s):			
Major Information System:	□ Yes □ No		
Data Retention Period(s): (include if not noted in Section 2-1 question f.)			
Brief Description: (include purpose and key business functions)**:**			

2 PRIVACY COMPLIANCE

The purpose of this section is to ensure compliance with privacy requirements, including applicable laws and USPS policy. Questions or comments should be referred to the USPS Privacy Office. In general, privacy compliance covers two categories: 1) collection or maintenance of information relating to employees or customers, and 2) customer-facing websites. Customers covered by this section are external, non-supplier customers.

2-1 System of Records – Data Management

The Privacy Act of 1974 and USPS policy provide privacy protections for employee and customer information that the USPS or its supplier maintains in a 'system of records.' A system of records (SOR) is a file or technology solution from which employee or customer information is retrieved by an identifier. In those cases, data must be managed in accordance with comprehensive data practices that apply to that SOR. Each SOR has been published in the Federal Register, and is reprinted in USPS Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*. (See HBK AS-353, Appendix.)

a.	**Does the information resource or technology solution collect or store customer or employee information where data is retrieved by name, number, or other identifier assigned to the customer or employee?**	
	□ No (skip to 2-6.)	□ Yes (Privacy Act system of records (SOR) is required.)
b.	**Does an existing Privacy Act system of records (SOR) apply?**	
	□ No (skip to 'e' and contact Privacy Office to develop new SOR.)	
	□Yes (SOR name): ______________________________(For assistance, contact Privacy Office.)	
c.	**Does the existing SOR need to be modified?**	
	□ No	□ Yes (skip to 'e' and contact Privacy Office.)
d.	**Have you read, and will the information resource or technology solution comply with, all data mgmt practices in the SOR?**	
	□ No	□ Yes
e.	**When is the information resource or technology solution expected to be operational?**	
	(mm/dd/yyyy)	
f.	**What is the data retention period for records associated with this information resource or technology solution?**	
	(specify):	
	What is the process for purging records at the end of that period?	
	(specify):	
g.	**Will the information resource or technology solution meet all of the following? (Check all applicable boxes.)**	
	□ Information is reliable for its intended use.	□ Information is accurate.
	□ Information is complete.	□ Information is current.
h.	**Will the information resource or technology solution collect only the minimum information required for functional operation?**	
	□ Yes	□ No (explain):

2-2 Notice

The Privacy Act and USPS policy require that customers or employees receive a privacy notice when information is collected directly from them. A privacy notice describes why data is collected and what protections apply. The Privacy Office must review and approve all new forms (hard copy and electronic) that collect customer, employee, or other individuals' information. (See HBK AS-353, 3-2.2)

a.	**Is information collected directly from a customer or employee? (Check all applicable boxes.)**					
	□ No (skip to 2-3.)	□ individual customer	□ business customer	□ employee		
b.	**How is information collected? (Check all applicable boxes)**					
	□ in-person	□ hard-copy form	□ fax	□ online	□ phone	□ e-mail
c.	**Has a privacy notice been provided by the Privacy Office?**					
	□ No (skip to 2-3 and contact Privacy Office.)	□ Yes, PA Notice has been provided by the Privacy Office.				
d.	**How is a privacy notice provided?**					
□	**Individual customer**					
	□ online - link to notice	□ online - text is on screen	□ notice is on hard-copy form, fax, e-mail			
	□ via phone (specify):	□ other (specify):				
□	**Business customer**					
	□ online - link to notice	□ online - text is on screen	□ notice is on hard-copy form, fax, e-mail			
	□ via phone (specify):	□ other (specify):				
□	**All customers**					
	If online, is usps.com privacy policy link on each page of application?	□ Yes	□ No			
	If by other than usps.com: how is privacy notice provided?					
	□ Notice: "See usps.com privacy policy" or "For info regarding our privacy policies visit usps.com."					
	□ Other (specify):					
□	**Employee**					
	□ online - link to notice	□ online - text is on screen	□ notice is on hard-copy form, fax, e-mail			
	□ via phone (specify):	□ other (specify):				

2-3 Access

Under the Privacy Act and USPS policy, customers or employees may access (and request corrections to) information regarding themselves that the Postal Service maintains in an SOR. (See HBK AS-353, 3-4.)

a.	**How does the information resource or technology solution provide customers or employees with instructions for accessing or amending data related to them? (Check all applicable boxes.)**
□	Via link that leads to their information.
□	Via link or by text (near where data collected) that gives instructions on how to access/amend info.
□	Via a phone number of a USPS representative who will provide instructions.
□	Via other method (explain):

2-4 Choice

The Privacy Act and USPS policy require that information collected about customers and employees can only be used for the purpose(s) for which it was collected, unless consent is granted for a secondary use. For customers, this includes choice over secondary marketing uses, such as whether the USPS can up-sell or cross-sell, or share information with third parties. (See HBK AS-353, 3-2.3.)

a.	**Do you intend to use customer or employee information for a secondary use?**		
	□ No (skip to 2-5.)	□ Yes	
b.	**Whose information do you want to use for a secondary use?**		
□	**Individual customers**	*Information resource or technology solution must provide method for customer to express consent for secondary use (opt-in).*	
	How will information resource or technology solution provide a mechanism for opt-in?		□ usps.com registration
	□ Other (explain):		
□	**Business customers**	*Information resource or technology solution must provide method for customer to take affirmative step to prevent secondary use (opt-out).*	
	How will information resource or technology solution provide a mechanism for opt-out?		□ usps.com registration
	□ Other (explain):		
□	**Employees (and applicants)**		
	Will information resource or technology solution provide a mechanism for employees to consent to secondary use?		
	□ Yes (explain):		
	□ No (Contact Privacy Office to see if applicable SOR needs to be amended.)		

2-5 Redress – Customer Systems

Under USPS policy, customers may submit questions and inquiries regarding USPS privacy policies, and a process must be in place for responding in a timely manner. (See HBK AS-353, 3-4.3.)

a.	**How does the information resource or technology solution enable customers to submit questions or inquiries about USPS privacy policies or use of their data?**
□	Not applicable, as information will not be collected from customers (skip to 2-6.)
□	Via a link or reference to usps.com privacy policy.
□	Via other method (explain):

2-6 Suppliers/Contractors/Partners

Under the Privacy Act and USPS policy, suppliers, contractors, and business partners that 1) have access to customer or employee information; or 2) that help to build or operate a customer website, must adhere to USPS privacy policies. (See HBK AS-353, 3-6.)

a.	**Are suppliers/contractors/partners working on this information resource or technology solution?**		
	□ No (skip to 2-7.)	□ Yes	
b.	**Do suppliers/contractors/partners have access to customer or employee information?**		
	□ No	□ Yes	
c.	**Do suppliers/contractors/partners help design, build, or operate a customer-facing web site?**		
	□ No	□ Yes	
d.	**If yes checked for b. or c. above, list all suppliers/contractors /partners below.** **Check if contract includes privacy clause (1-1) or modified clause approved by law dept.**		
		□ Yes	□ No
		□ Yes	□ No
		□ Yes	□ No

2-7 Customer Activities – Measurement & Technologies

Under the E-Govt Act & USPS policy, the USPS has established policies for the use of technology, such as web analysis tools which can track customer behavior (e.g., cookies & web beacons). The policies limit types of permitted tools, types of data collected, and duration of tool activation. (See HBK AS-353, 3-6.)

a.	**Is technology used to collect information online relating to customer activity?** **(Check all applicable boxes)**			
	□ No (skip to d.)	□ blue.usps.gov	□ usps.com	□ Other (URL):
b.	**Check all tracking technologies used and check whether they comply with usps.com privacy policy.**			
	□ session cookie	□ Yes	□ No	
	□ persistent cookie	□ Yes	□ No	
	□ web beacon	□ Yes	□ No	
	□ other (specify):	□ Yes	□ No	
c.	**Check other technologies used, and whether they comply with usps.com privacy policy.**			
	□ Link to external site	□ Yes	□ No	
	□ ad banner	□ Yes	□ No	
	□ other (specify):	□ Yes	□ No	
d.	**Is technology used to collect information offline relating to customer behavior?**			
	□ No	□ Yes (explain):		

2-8 Gramm–Leach-Bliley Act – Financial Services

The USPS voluntarily complies with the Gramm-Leach-Bliley Act (GLB), Title V, which governs data management when certain financial services are provided. Examples of financial services include wire or monetary transfers; printing, selling, or cashing checks; or providing USPS credit services. It does not include payment by check or credit card issued by another entity. (See HBK AS-353, 2-3.5.)

a.	**Does the information resource or technology solution provide a financial service?**	
	□ No	□ Yes (contact Privacy Office)

2-9 Children's Online Privacy Protection Act

USPS voluntarily complies with the Children's Online Privacy Protection Act (COPPA). If a website collects information from children under the age of 13, COPPA requires notices and parental consent for certain activities. (See HBK AS-353, 2-3.6.)

a.	**Is it a customer information resource or technology solution that operates online?**	
	□ No (skip to 2-10.)	□ Yes
b.	**Is there reason to expect, that the information resource or technology solution will collect information from children under the age of 13?**	
	□ No	□ Yes (contact Privacy Office)

2-10 Privacy Risks

In accordance with the Privacy Act, E-Government Act, and USPS policy, the USPS identifies, analyzes, and mitigates privacy risks for systems that collect or maintain information related to customers or employees. (See HBK AS-353, 3-2.)

a.	**Does the information resource or technology solution collect or maintain information related to customers or employees, involve a customer web site, or use technology that can track customer behavior?**	
	□ No (skip to section 3.)	□ Yes
b.	**Has the information resource or technology solution been reviewed for any possible privacy risks or impacts?**	
	□ No (skip to section 3.)	□ Yes
c.	**Has the review identified any privacy risks and/or impacts related to the information resource or technology solution?**	
	□ No (skip to section 3.)	
	□ Yes (describe):	
d.	**Have efforts been made to mitigate privacy risks and/or impacts related to the information resource or technology solution?**	
	□ No	
	□ Yes (describe):	

3 GENERAL DATA ATTRIBUTES AND DEPENDENCIES **(Please check all that apply)**

3-1 Collected Data Types

□	Customer (external, non-vendor customer)
□	USPS Employee or Contractor
□	USPS Employment Applicant
□	Supplier or Business Partner
□	Mail Operations-related data
□	PCI (see Section 5-3, PCI-Scope Determination, below)
□	Other (specify):

3-2 Data from Other Sources

□	Customer (external, non-vendor customer)
□	USPS Employee or Contractor
□	USPS Employment Applicant
□	Supplier or Business Partner
□	Other USPS Data Source (specify):
□	Other Government Data Source
□	Consumer Reporting Agency
□	Law Enforcement Agency
□	Commercial Source or Database (specify):
□	Other (specify):

3-3 Data Access

Please check all the individuals and organizations that will have access.

□	Customer (external, non-vendor customer)
□	USPS Employees or Contractors
□	Supplier or Business Partners
□	Other (specify):

3-4 Voluntary Data Sharing

Please check all the individuals and organizations to which information will be shared on a voluntary basis (not legally required).

□	Customer (external, non-vendor customer)
□	Supplier, Business Partner, or other Business Entity
□	Other Government Agency(s) (federal, state, or local) (specify):
□	Law Enforcement Agency (specify):
□	Other (specify):
□	None

4 DETERMINATION OF CRITICALITY

4-1 Initial or Current Criticality Designation

□ None	**□ Noncritical (Low)**	**□ Critical-Moderate**	**□ Critical-High**

4-2 Identify Essential Business Functions

Checking one or more of the essential business functions below will determine, in conjunction with Business Continuity organization, the ISSO, and the application owner, if the technology solution is critical to the Postal Service essential business functions.

(Note: If any of the items below are checked, the information resource or technology solution may be designated as critical.)	
□	Protecting customer or personnel life, safety, or health
□	Paying suppliers and employees
□	Generating, collecting, or protecting revenue
□	Managing the movement of mail (transportation, logistics, delivery, and retail)
□	Communications (Postal alert and messaging systems)
□	Infrastructure services (data transfer, administrative services, and support systems)

4-3 Rationale for Criticality

1. Describe the business purpose of the application.

2. If one or more of the essential business functions in Section 4-2 above are checked, describe the significance of the impact.

3. What would happen if the application was not recovered in a timely manner? If possible provide both quantitative and qualitative data to support the criticality rationale.

4. Is there a manual workaround that could be used until the application is recovered? If so, please explain the workaround process, and describe the associated impact (e.g., more time, more personnel).

4-4 Business Continuity Criticality Determination

Based on an evaluation of the responses to the questions in 4-2, and the information provided in 4-3, this information resource is designated as (check one):

□ **Non-Critical (Low)**	□ **Critical-Moderate**	□ **Critical-High**
Business Continuity Criticality Rationale Narrative:		

5 DETERMINATION OF SENSITIVITY

5-1 Data Element Sensitivity Designation

For applications, check all the data elements that you are collecting, transmitting, using, retrieving, and/or storing. If you collect any data elements that are not listed below, contact the CPO for guidance on entering the data elements in the appropriate table below. The presence of these data elements determines the security designation.

NOTE: All information resources (technology solutions) must implement baseline requirements.

Non-Sensitive Information (Requires baseline requirements)			
□ Name	□ City, State, and ZIP (Home or Work)	□ Work Street Address	□ Work Phone Number
□ Work Fax Number	□ Work Cell Number	□ Work Pager Number	□ Work Email Address
□ Occupation	□ Job Description	□ USPS Salary	□ Professional Affiliations
□ ICQ/Chat Address	□ Gender	□ USPS Employee Title (position)	□ Other:
□	□	□	□
□	□	□	□

Sensitive Information (Requires baseline and sensitive requirements)			
Personal Information			
□ Photographs**	□ Income/Assets*	□ Personal Email Address**	□ Buying Habits*
□ Personal Cell Number*	□ Birth Date/Age*	□ Home Street Address*	□ Marital Status*
□ Race/National Origin*	□ Partial Social Security Number*	□ Change of Home Address*	□ Externally Obtained Demographic Info.*
□ Web Navigation Habits*	□ Customer Obtained Demographic Info.*	□ Personal Clubs and Affiliations*	□ Home Phone Number*
□ USPS Employee ID Number (EIN)*	□ Family Information	□ IP Address*	□ Truncated Credit Card Number* (first 6 and/or last 4 characters)
□ Cardholder Name, Expiration Date, and Service Code***	□ Other:	□	□
Business Information			
□ Bill Payee Name	□ Bill Payee Phone Number	□ Bill Payee Account Number	□ Bill Payee Address
□ Financial/Trade Secrets/Proprietary that does not warrant enhanced protection	□ Not Publicly Available USPS Documents (withholdable under FOIA)	□ Not Publicly Available Information from Business Partners	□ Bid and Proposal Information
□ Application Source Code	□ Building layouts	□ Other:	□
□	□	□	□
Information Resource Protection Information			
□ Platform Harden Standards	□ Security Settings	□ Architecture Diagrams	□ Authenticators (including Passwords, PINs, and related Identity Questions and Responses)**
□ Unpatched Vulnerabilities	□ Firewall Configurations and Rules	□ Other:	□
□	□	□	□

* *Data element with a name or personal identifier is Sensitive and must be encrypted in transit and at rest. Data element without a name or personal identifier is Non-Sensitive.*

** *Data element must be encrypted in transit and at rest.*

*** *Data element with a PAN must be encrypted in transit and at rest.*

Sensitive-Enhanced Information (Requires baseline, sensitive, and sensitive-enhanced requirements)			
Personal Information			
□ Full Social Security Number**	□ Driver's License Number**	□ Passport Number**	□ Bank Routing and Account Numbers**
□ Fingerprints**	□ Other Biometric Data**	□ USPS Applicant or Employee Medical Information**	□ Change of Address with court ordered non-disclosure**
□ USPS Personnel Records**	□ Other Account Number**	□ Other:	□
□	□	□	□
Business Information			
□ Financial/Trade Secrets/Proprietary Information that warrants enhanced protection	□ Emergency Preparedness	□ Other:	□
□	□	□	□
Information Resource Protection Information			
□ Encryption Keys**	□ Other:	□	□
Payment Card Industry Information			
□ Primary Account Number (PAN) or Full Credit Card Number** (16 characters)	□ Sensitive Cardholder Authentication Data Storage****	□ Other:	□
Law Enforcement Information			
□ Information compiled for law enforcement purposes	□ Communications Protected by Legal Privileges[1]	□ Other:	□
□	□	□	□

***** Data element must be encrypted in transit and at rest.*

*******Authentication data elements such as full magnetic strip or chip data and PIN/PIN Block must not be stored after authorization (even if encrypted).*

[1] Such as the deliberate process privilege, attorney-client privilege, and attorney work product doctrine.

5-2 Impact of Unauthorized Use

(Note: If any of the items below are checked, the information resource or technology solution will be designated as sensitive.)	
□	Information has moderate to significant potential to be used for financial gain through fraud or manipulation.
□	Unauthorized disclosure or misuse of the information would result in moderate to significant financial loss or negative impact to brand.
□	Unauthorized disclosure or misuse of the information would result in moderate to significant harm, embarrassment, inconvenience, or unfairness to the individual.

5-3 PCI-Scope Designation

5-3.1	**PCI Designation**	
□	In-Scope PCI Application *[If this box is checked, check PCI in Section 5-5.]*	
□	In-Scope Non-PCI Application *[If this box is checked, check PCI in Section 5-5.]*	
□	Out of Scope for PCI Application	
5-3.2	**Justification for PCI Scope Designation**	
Reason Provided for Application Designation		
Documentation Reviewed and the Source		

5-4 Additional Sensitivity Impact Information

Is there any other information that may impact the determination of the sensitivity level?	
□	No
□	Yes (describe):

5-5 Sensitivity Determination Summary

Based on the type of information being collected in 5-1, an evaluation of the responses in 5-2 to the impact of unauthorized use, the PCI-scope determination in 5-3, and any additional sensitive impact information in 5-4, check the Non-Sensitive, Sensitive, or Sensitive-Enhanced Information box. If the Sensitive-Enhanced Information box is checked, check the PCI, Law Enforcement, or both boxes if it applies. The level of sensitivity drives the security requirements outlined in section 6.

□ **Non-Sensitive**		
□ **Sensitive**		
□ **Sensitive-Enhanced**	□ **PCI In-Scope**	□ **Law Enforcement**

6 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED

The matrix below outlines which groups of security control requirements must be included in the technology solution requirements document based on the security classification. Once the design document for the technology solution has been developed, the security requirements must be revisited to determine whether the security control requirements are applicable. For example, if there is no wireless technology in the solution then the wireless security requirements would not apply. There could also be the need to add security requirements previously not addressed in the BIA because the technology solution design changed. The BIA security requirements incorporated into the final design will be input into the security test plan along with any additional security requirements recommended in the risk assessment process.

INFORMATION SECURITY REQUIREMENTS BY CLASSIFICATION

	Information Security Requirements								
Classification Category	**Baseline**	**Sensitive**	**Sensitive-Enhanced**	**PCI**	**Law Enforcement**	**Critical-Moderate**	**Critical-High**	**Conditional**	**ISSO Recommended**
All Information Resources	**X**								
Non-Sensitive & Non-Critical	**X**							**Con**	**Rec**
Sensitive	**X**	**X**						**Con**	**Rec**
Sensitive-Enhanced	**X**	**X**	**X**					**Con**	**Rec**
PCI	**X**	**X**	**X**	**X**				**Con**	**Rec**
Law Enforcement	**X**	**X**	**X**		**X**			**Con**	**Rec**
PCI & Law Enforcement	**X**	**X**	**X**	**X**	**X**			**Con**	**Rec**
Critical-Moderate	**X**					**X**		**Con**	**Rec**
Critical-High	**X**					**X**	**X**	**Con**	**Rec**

X = Required
Con = If box is checked
Rec = If recommended by ISSO

6-1 Baseline Information Security Requirements

Baseline information security requirements must be implemented by all information resources or technology solutions.

REQ. No.	**BASELINE INFORMATION SECURITY REQUIREMENT** (References are from Handbook AS-805 unless noted)
B-1	Implement applicable certification and accreditation (C&A) requirements and complete C&A deliverables (8-5)
B-2	Implement data retention in accordance with the legal retention requirements and applicable Records Retention Schedule (3-5.3)
B-3	Release information outside the Postal Service on clean, virus-free media (3-5.6.1)
B-4	Implement data disposal and destruction procedures; eradicate information on hardware and electronic media prior to re-use by another program or being released for maintenance (3-5.8)
B-5	Evaluate the use of cookies and other user tracking mechanisms (Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management*: 3-6)
B-6	Notify customers before transfer to an external site not under Postal Service control (MI AS-610-2007-4, *Web Site Affiliation Program*: Exit Pages)
B-7	Clearly define information security roles and responsibilities for all project personnel with appropriate separation of duties and responsibilities (6-2.2 and 6-2.1)
B-8	Request clearance or background screening for applicable personnel (outside the IBSSC) (6-4.1)
B-9	Require personnel attend awareness training initially and at least annually (6-5.3)
B-10	Train staff to handle security breaches and incidents (6-5.3)
B-11	Require personnel acknowledge in writing that they have read and understand Postal Service information security policies and procedures (6-5.2)
B-12	Implement surge protection for all information resources (7-4)
B-13	Use a formal system development methodology (e.g., TSLC) for information resource development projects (8-1)
B-14	Implement change/version control and configuration management (8-2.4)
B-15	Establish and maintain baseline information resource configurations and inventories (including hardware, software, firmware, and documentation) (8-2.4.1)
B-16	Harden information resources to Postal Service information security requirements (8-2.4.2 and 10-2.3.1)
B-17	Install security patches (8-2.4.4)
B-18	Test all software changes (including patches) before deploying to production (8-2.4.5)
B-19	Implement separate environments for development, system test, CAT, and production with separation of duties between personnel assigned to the development, system test, CAT, and production environments (8-3.1, 8-3.2, 8-2.5)
B-20	Restrict developer access to the production, CAT, and SIT environments (8-3.2)
B-21	Secure prior approval in writing from the executive sponsor and CIO or their designee, if non-sensitive production data is to be used in a development or test environment (8-3.3.3)

REQ. NO.	BASELINE INFORMATION SECURITY REQUIREMENT (References are from Handbook AS-805 unless noted)
B-22	Secure the additional prior approval in writing from the manager, CISO, if production data is to be used in a development or test environment outside of Postal Service facilities (8-3.3.4)
B-23	Label production files approved for use in a development, system test, or CAT environment as “copies” (8-3.3.4, 8-3.3.3, and 8-3.3.2)
B-24	Register information resource in eAccess (8-5.4.5)
B-25	Authorize access based on need-to-know and least privilege (9-3.1)
B-26	Restrict supervisory and administrative privileges (9-4.2.2)
B-27	Where accountability is required, prohibit shared accounts (9-4.2.4)
B-28	Limit training accounts to minimum functionality required to complete the training (9-4.2.1)
B-29	Implement controls to enable accounts used by vendors to support and maintain system components only when needed by the vendor and to monitor those accounts while being used (9-4.3.5)
B-30	Implement password controls to Postal Service information security requirements (9-6.1)
B-31	Implement session management controls to Postal Service information security requirements (9-6.10)
B-32	Implement controls to detect duplicate financial transactions (9-8.1)
B-33	Implement backup and recovery procedures (9-9.4.4)
B-34	Implement audit logging of security events (9-11)
B-35	Protect audit logs (9-11.4)
B-36	Review, maintain, and retain audit logs (9-11.5 and 9-11.6)
B-37	Implement full-disk encryption on all laptop computers (10-2.5)
B-38	Before an information resource goes in to production, activate all available safeguards; disable or remove extraneous features and files; document information resource security settings and maintain current; and remove testing artifacts including test data, default logon IDs, and passwords (10-3.1)
B-39	Configure DBMS software to Postal Service policies (10-3.7)
B-40	Evaluate and acquire COTS software from an approved source (10-3.8)
B-41	Perform timely information resource maintenance; and control tools, techniques, and mechanisms used to conduct information resource system maintenance (10-4.10 and 10-4.11)
B-42	Implement Postal Service network security controls (11-3)
B-43	Implement secure enclaves for externally facing information resources (11-3.8)
B-44	Isolate Postal Service networks from non–Postal Service networks (11-3.9)
B-45	Protect Internet–accessible information resources such as those residing on DMZs (11-5.1)
B-46	Secure approval from the Network Connectivity Review Board (NCRB) prior to establishing network connectivity (11-5.2)
B-47	Configure firewalls to Postal Service information security requirements (11-5.2.1)

REQ. NO.	**BASELINE INFORMATION SECURITY REQUIREMENT** (References are from Handbook AS-805 unless noted)
B-48	Protect firewalls to Postal Service information security requirements (11-5.2.3)
B-49	Locate Web servers and electronic commerce systems accessible to the public within a DMZ with NCRB approved access control (11.5.3)
B-50	Route all inbound traffic to the Intranet from the DMZ through a proxy–capable device (11-5.3)
B-51	Conduct vulnerability scan (14.2.2)
B-52	Implement authorized warning banner (14-3.3)
B-53	Only install approved software listed on the Infrastructure Tool Kit (ITK) 10-3.4.3
B-54	Implement "mutual" device and user authentication for wireless applications; i.e., the device, the user, and the network are able to recognize each to be who they say they are (11-11.1)
B-55	Implement a secure link between the device and the wireless access point (11-11.1)
B-56	Secure approval from the Director Information Technology Operations and the NCRB prior to the installation of access points, wireless cards, or any wireless technology (11-11.1)
B-57	Develop and maintain wireless and wired networks separately and distinctly (11-11.1)
B-58	Implement a firewall between the wired and wireless network segments if Postal Service certificates are not used to authenticate the devices to the network (11-11.1)
B-59	Register Postal Service–managed wireless devices as members of the USA domain (11-11.3.1)
B-60	Implement approved virus protection, security patches, and personal firewalls for Postal Service-managed wireless devices (11-11.3.1)
B-61	Authenticate wireless users through Active Directory (AD) credentials (11-11.3.1)
B-62	Identify internal and external dependencies using the table and instructions in the Information Security Requirements and Controls document of the C&A process (9-9.3.1)

6-2 Sensitive Information Security Requirements

Sensitive information security requirements must be implemented by all information resources or technology solutions designated as sensitive. These sensitive requirements must be included in the technical solution requirements **in addition to the baseline requirements**.

REQ. No.	**SENSITIVE INFORMATION SECURITY REQUIREMENT** (References are from Handbook AS-805 unless noted)
S-1	Complete all baseline requirements (3-4)
S-2	Label hardcopy and storage media containing sensitive information as “RESTRICTED INFORMATION” (3-5.1)
S-3	Store hardcopy and media containing sensitive information in a controlled area or a locked cabinet (3-5.2)
S-4	Store sensitive information on Postal Service-owned devices (3-5.3)
S-5	Segregate sensitive Postal Service information from non-Postal Service information (3-5.3)
S-6	Implement controls for (1) accessing or downloading sensitive electronic information off Postal Service premises or (2) taking sensitive electronic and non–electronic information off–site (i.e., non–Postal Service premises) including Postal Service data processed by business partners (3-5.5)
S-7	When sensitive information is no longer needed, ensure that hard copies are cross-cut shredded and electronic copies are eradicated using zero-bit formatting or another acceptable eradication procedure (3-5.8)
S-8	Implement information resource operational security training to address how to protect sensitive information throughout the lifecycle (6-5.3, 8-5.4.4, and 8-5.5.4)
S-9	Locate information resource containing sensitive information in a controlled area (7-2.3)
S-10	Secure prior approval in writing from the CPO, executive sponsor, and CIO or their designee(s) if sensitive information is to be used in development or test environment (8-3.3.3)
S-11	Encrypt sensitive information stored on removable devices or media based on Postal Service encryption and key recovery policies (9-7.1.2)
S-12	Encrypt sensitive information in transit based on Postal Service encryption and key recovery policies (9-7.1.2)
S-13	Install databases containing sensitive information on an internal network zone segregated from the DMZ (11-5.3)
S-14	Encrypt sensitive information at rest based on Postal Service encryption and key recovery policies (9-7.1.2)

6-3 Sensitive-Enhanced Security Requirements

Sensitive-enhanced information security requirements must be implemented by all information resources or technology solutions designated as sensitive-enhanced. These sensitive-enhanced requirements must be included in the technical solution requirements **in addition to the baseline requirements and the sensitive requirements**.

REQ. No.	SENSITIVE-ENHANCED INFORMATION SECURITY REQUIREMENT (References are from Handbook AS-805 unless noted)
SE-1	Complete all baseline and sensitive requirements (3-4)
SE-2	De-identify PII before using in system test or development environments (8-3.2.1 and 8-3.2.2)

6-4 PCI Information Security Requirements

Payment Card Industry (PCI) information security requirements must be implemented by all information resources or technology solutions processing PCI information. These PCI requirements must be included in the technical solution requirements **in addition to the baseline requirements, the sensitive requirements, and the sensitive-enhanced requirements**. PCI security requirements change over time. If new security requirements are identified, please inform the CISO Policy Program Manager.

REQ. No.	PCI INFORMATION SECURITY REQUIREMENT (References are from the Data Security Standard unless noted)
PCI-1	Complete all baseline, sensitive, and sensitive-enhanced requirements (AS-805 Sec. 3-4)
PCI-2	Implement a formal process for approving and testing all network connections and changes to firewall and router configurations (1.1.1)
PCI-3	Document cardholder data flows and all network connections including any wireless networks on the network diagram (1.1.2)
PCI-4	Implement a DMZ and configure firewall and router rule sets to limit inbound and outbound traffic (1.1.3)
PCI-5	Document roles and responsibilities for logical management of network components (1.1.4)
PCI-6	Document all services, protocols, and ports required for business (1.1.5.a)
PCI-7	Identify insecure services, protocols, and ports allowed, verify they are necessary for business and implement available security features (1.1.5.b)
PCI-8	Review firewall and router rule sets at least every 6 months (1.1.6)
PCI-9	Secure and synchronize router configuration files (1.2.2)
PCI-10	Install perimeter firewalls between any wireless networks and systems that store cardholder data (1.2.3)
PCI-11	Prohibit direct public access between the Internet and system components in the cardholder data environment (1.3)
PCI-12	Install database(s) in an internal enclave segregated from the DMZ (1.3.7)
PCI-13	Install a personal firewall on mobile Postal/employee/contractor-owned computers used to access the Postal Service Intranet from the Internet (1.4)

REQ. No.	**PCI INFORMATION SECURITY REQUIREMENT** (References are from the Data Security Standard unless noted)
PCI-14	Remove vendor-supplied default settings, accounts, and passwords before installing a system on the network (2.1)
PCI-15	Remove vendor defaults settings, passwords, and encryption keys for wireless environments and enable strong encryption for authentication and transmission (2.1.1)
PCI-16	Implement only one primary function per server (2.2.1)
PCI-17	Configure system security parameter settings to prevent misuse (2.2.3)
PCI-18	Remove unnecessary functionality and document enabled functions (2.2.4)
PCI-19	Encrypt non-console administrative access (2.3)
PCI-20	Ensure shared hosting providers protect the hosted Postal Service environment and cardholder data (2.4)
PCI-21	Keep cardholder data storage to a minimum and limit retention time (3.1)
PCI-22	Do not store the full contents of any track from the magnetic stripe on the back of the card or contained in a chip on the card under any circumstance (3.2.1)
PCI-23	Do not store the three-digit or four-digit card-validation code printed on the front of the card or the signature panel on the back of the card under any circumstance (3.2.2)
PCI-24	Do not store PINs or the encrypted PIN blocks under any circumstance (3.2.3)
PCI-25	Mask primary account number (PAN) when displayed (the first six or the last four digits are the maximum digits displayed) (3.3)
PCI-26	De-identify or remove PAN from tables, files, removable media, and audit logs (3.4)
PCI-27	Manage cryptographic keys separate from the native operating system mechanism, store cryptographic keys securely, and do not tie decryption keys to user accounts (3.4.1)
PCI-28	Encrypt cardholder data on removable media wherever stored (3.4.1)
PCI-29	Protect cryptographic keys against both disclosure and misuse (3.5)
PCI-30	Restrict cryptographic keys to the fewest number of custodians necessary (3.5.1)
PCI-31	Store cryptographic keys in the fewest possible locations and forms (3.5.2)
PCI-32	Fully document and implement key-management processes and procedures (3.6)
PCI-33	Generate strong cryptographic keys (3.6.1)
PCI-34	Implement secure cryptographic key distribution (3.6.2)
PCI-35	Implement secure cryptographic key storage (3.6.3)
PCI-36	Periodically (at least annually) change cryptographic keys (3.6.4)
PCI-37	Retire or replace old or suspected compromised cryptographic keys (3.6.5)
PCI-38	Implement split knowledge and dual control of cryptographic keys (3.6.6)
PCI-39	Prevent unauthorized substitution of cryptographic keys (3.6.7)
PCI-40	Require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities (3.6.8)
PCI-41	Use strong cryptography and security protocols to safeguard cardholder data during transmission over open, public networks (4.1)

REQ. NO.	**PCI INFORMATION SECURITY REQUIREMENT** (References are from the Data Security Standard unless noted)
PCI-42	For wireless networks transmitting cardholder data or connecting to the cardholder environment, use industry best practices to implement strong encryption for authentication and transmission (4.1.1)
PCI-43	Use strong cryptography to encrypt PANs and cardholder data sent via end-user messaging technologies (4.2.a)
PCI-44	Document policy stating that unencrypted PANs are not to be sent via end-user messaging technologies (4.2.b)
PCI-45	Deploy effective anti-virus software on all systems commonly affected by malicious software (5.1)
PCI-46	Maintain anti-virus software current, actively running, and generating audit logs (5.2)
PCI-47	Install critical vendor-supplied security patches within one month of release (6.1)
PCI-48	Identify newly discovered security vulnerabilities and update hardening standards (6.2)
PCI-49	Validate all input to prevent cross-site scripting, injection flaws, malicious code execution, etc. (6.5.1)
PCI-50	Implement effective error handling (6.5.5)
PCI-51	Develop software applications in accordance with an industry standard systems development methodology and the current PCI DSS (6.3)
PCI-52	Do not use production data (live PANs) for development or testing (6.4.3)
PCI-53	Remove test data and accounts before migrating systems to production (6.4.4)
PCI-54	Remove custom application accounts and developer and tester user IDs and passwords before migrating applications to production (6.3.1)
PCI-55	Review custom code to identify potential coding vulnerabilities (6.3.2)
PCI-56	Follow change control procedures for all changes to system components (6.4)
PCI-57	Document impact of all changes to system components (6.4.5.1)
PCI-58	Secure management sign-off for all changes to system components (6.4.5.2)
PCI-59	Test operational functionality of all changes to system components (6.4.5.3)
PCI-60	Prepare back-out procedures for all changes to system components (6.4.5.4)
PCI-61	Develop web applications based on secure coding guidelines that prevent common coding vulnerabilities in web software development (6.5)
PCI-62	For a public-facing web-based information resource, [1] engage an independent organization that specializes in application security to review custom application code at least annually and after any changes to address new threats and vulnerabilities or [2] install a web-application layer firewall in front of the public-facing web information resource (6.6)
PCI-63	Limit access to system components and cardholder information to only those individuals whose job requires access (7.1)
PCI-64	Restrict access rights to privileged user IDs to least privileges necessary to perform job responsibilities (7.1.1)
PCI-65	Assign privileges via eAccess based on an individual’s job classification and function (RBAC) (7.1.2 and 7.2.2)

REQ. NO.	**PCI INFORMATION SECURITY REQUIREMENT** (References are from the Data Security Standard unless noted)
PCI-66	Set access control systems for system components to default to the “deny-all” setting (7.2.3)
PCI-67	Assign all users a unique ID before allowing them to access system components or cardholder data (8.1)
PCI-68	Authenticate all users via password, passphrase, or two-factor authentication (8.2)
PCI-69	Implement two-factor authentication for all remote network access (8.3)
PCI-70	Render all passwords unreadable during transmission and storage on all system components using strong cryptography (8.4)
PCI-71	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects (8.5.1)
PCI-72	Implement controls to verify a user’s identity before his or her password is reset when the user requests a password reset by non-face-to-face method (8.5.2)
PCI-73	Set first-time passwords to a unique value for each user and force the user to change immediately at first use (8.5.3)
PCI-74	Immediately revoke access of terminated users (8.5.4)
PCI-75	Remove/disable inactive user accounts at least every 90 days (8.5.5)
PCI-76	Enable accounts used for remote maintenance only during the time period needed (8.5.6)
PCI-77	Communicate password procedures and policies to all users who have access to cardholder data (8.5.7)
PCI-78	Do not use group, shared, or generic accounts or passwords (8.5.8)
PCI-79	Change user passwords at least every 90 days (8.5.9)
PCI-80	Require a minimum password length of at least seven characters (8.5.10)
PCI-81	Require passwords contain numeric and alphabetic characters (8.5.11)
PCI-82	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she used (8.5.12)
PCI-83	Limit repeated access attempts by locking out the user ID after not more than six attempts (8.5.13)
PCI-84	Set the lockout duration to a minimum of thirty minutes or until a system administrator enables the user ID (8.5.14)
PCI-85	If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal (8.5.15)
PCI-86	Authenticate all access (including applications, system administrators, and users) to databases containing cardholder data (8.5.16)
PCI-87	Use facility entry controls to limit and monitor physical access to computer rooms, data centers and other physical areas with systems in the cardholder environment (9.1)
PCI-88	Use video cameras or other access controls mechanisms to monitor individual physical access to sensitive areas (excludes areas where only point-of-sale terminals are present) (9.1.1)
PCI-89	Restrict physical access to publicly accessible network jacks (9.1.2)

REQ. No.	**PCI INFORMATION SECURITY REQUIREMENT** (References are from the Data Security Standard unless noted)
PCI-90	Restrict physical access to wireless access points, gateways, and handheld devices (9.1.3)
PCI-91	Distinguish between Postal Service personnel and visitors in areas where cardholder data is accessible (9.2.a, 9.2.c, and 9.3.2.a)
PCI-92	Implement visitor controls (9.3.3)
PCI-93	Implement visitor logs to maintain a physical audit trail of visitor activity (9.4)
PCI-94	Store back-ups in a secure location, preferably an offsite facility and review the location's security at least annually (9.5)
PCI-95	Physically secure all hardcopy and electronic media containing cardholder data (9.6)
PCI-96	Maintain strict control over the internal and external distribution of media containing cardholder data (9.7)
PCI-97	Secure management approval for removal of media containing cardholder data from a secured area (9.8)
PCI-98	Maintain strict control over the storage and accessibility of media that contains cardholder data (9.9)
PCI-99	Cross-cut shred, incinerate, or pulp hardcopy media containing cardholder data when it is no longer needed for business or legal reasons (9.10.1)
PCI-100	Securely wipe or degauss electronic media when it is no longer needed for business or legal reasons (9.10.2)
PCI-101	Link all access to system components to individual users (10.1)
PCI-102	Implement automated audit trails for all system components to track all access to cardholder data (10.2.1)
PCI-103	Implement automated audit trails for all system components to track all actions taken by anyone with root or administrative privileges (10.2.2)
PCI-104	Implement automated audit trails for all system components to track all access to audit trails (10.2.3)
PCI-105	Implement automated audit trails for all system components to track invalid access attempts (10.2.4)
PCI-106	Implement automated audit trails for all system components to track the use of identification and authentication (10.2.5)
PCI-107	Implement automated audit trails for all system components to track the initiation of the audit logs (10.2.6)
PCI-108	Implement automated audit trails for all system components to track the creation and deletion of system-level objects (10.2.7)
PCI-109	Include user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component, or resource in the audit trail entries for all system components (10.3)
PCI-110	Implement Network Time Protocol (NTP) or similar technology for time synchronization (10.4.a)
PCI-111	Implement controls to prevent internal servers from receiving time signals from external sources (10.4.1.a)

REQ. No.	PCI INFORMATION SECURITY REQUIREMENT (References are from the Data Security Standard unless noted)
PCI-112	Designate specific external hosts from which the time servers will accept NTP time updates (10.4.1.b)
PCI-113	Limit viewing of audit trails to those with a job-related need (10.5.1)
PCI-114	Protect audit trails from unauthorized modifications (10.5.2)
PCI-115	Promptly back up audit trail files to a centralized log server or media that is difficult to alter (10.5.3)
PCI-116	Write logs for external-facing technologies onto a log server on the Intranet (10.5.4)
PCI-117	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (10.5.5)
PCI-118	Review logs for all system components at least daily. Include servers that perform security functions like intrusion-detection and authorization, authentication, and accounting (AAA) protocol servers such as RADIUS (10.6)
PCI-119	Retain audit history for at least one year with a minimum of three months immediately available for analysis (10.7)
PCI-120	Use a wireless analyzer at least quarterly or deploy a wireless IDS/IPS to identify all wireless devices in use (11.1)
PCI-121	Conduct internal and external network vulnerability scans by an approved scanning vendor at least quarterly, after any significant change in the network by Postal Service staff, and until passing results are obtained (11.2)
PCI-122	Conduct internal and external network-layer and application-layer penetration testing at least annually and after any significant changes to the infrastructure environment (11.3)
PCI-123	Implement intrusion detection and/or intrusion prevention systems to monitor all traffic in the cardholder environment and alert personnel to suspected compromises (11.4)
PCI-124	Implement file-integrity monitoring software to alert personnel of unauthorized modification of critical executables and files (11.5)
PCI-125	Update information security policy as required to address all PCI requirements (12.1)
PCI-126	Update the information resource risk assessment annually identifying new threats and vulnerabilities (12.1.2)
PCI-127	Review and update information security policy at least annually to reflect changes to business objectives or the risk environment (12.1.3)
PCI-128	Develop and implement daily operational security procedures that are consistent with PCI requirements (12.2)
PCI-129	Develop and implement usage policies and procedures for critical personnel-facing technologies such as remote-access, wireless, removable electronic media, laptops, PDAs, email, Internet (12.3)
PCI-130	Require explicit management approval to use critical personnel-facing technologies (12.3.1)
PCI-131	Require all use of critical personnel-facing technologies be authenticated (12.3.2)
PCI-132	Develop a list of all critical personnel-facing technology devices and the personnel authorized to use these devices (12.3.3)

REQ. No.	**PCI INFORMATION SECURITY REQUIREMENT** (References are from the Data Security Standard unless noted)
PCI-133	Label critical personnel-facing technology devices with owner, contact information, and purpose (12.3.4)
PCI-134	Develop a list of critical company-approved personnel-facing technology products (12.3.7)
PCI-135	Implement an automatic session disconnect for remote-access personnel-facing technologies after a specific period of inactivity (12.3.8)
PCI-136	Activate remote-access personnel-facing technologies for vendors only when needed and deactivate immediately after use (12.3.9)
PCI-137	Prohibit copy, move, and storage of cardholder data to local hard drives and removable electronic media when accessing cardholder data via remote-access personnel-facing technologies (12.3.10)
PCI-138	Define information security responsibilities for personnel supporting PCI (12.4)
PCI-139	Implement a formal security awareness program with multiple methods of communicating to all PCI personnel on the importance of cardholder data security (12.6)
PCI-140	Educate PCI personnel upon hire and at least annually (12.6.1)
PCI-141	Require PCI personnel to acknowledge at least annually that they have read and understand information security policies and procedures (12.6.2)
PCI-142	Screen PCI personnel prior to hire to minimize risk of attacks from internal sources (12.7)
PCI-143	Implement PCI policies and procedures to manage service providers (12.8)
PCI-144	Maintain a list of service providers (12.8.1)
PCI-145	Maintain a written agreement with each service provider that acknowledges the service provider is responsible for the security of the cardholder data the service provider processes (12.8.2)
PCI-146	Implement a process for ensuring due diligence from service providers prior to engagement (12.8.3)
PCI-147	Monitor service provider compliance with PCI DSS (12.8.4)
PCI-148	Implement an incident response plan to immediately respond to a system breach. The plan must address roles and responsibilities, specific incident procedures including communications and contact strategies, business continuity and recovery procedures, payment brand notification, customer notification, etc. (12.9 and 12.9.1)
PCI-149	Test the incident response plan at least annually (12.9.2)
PCI-150	Designate specific personnel to be available on a 24/7 basis to respond to alerts (12.9.3)
PCI-151	Provide appropriate training to staff with security breach response responsibilities (12.9.4)
PCI-152	Include alerts from security systems in the incident response plan (12.9.5)
PCI-153	Implement a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments (12.9.6)
PCI-154	Restrict inbound and outbound traffic to what is necessary and deny all other traffic (1.2.1)
PCI-155	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible service, protocols, and ports (1.3.1)
PCI-156	Limit inbound Internet traffic to IP addresses within the DMZ (1.3.2)

REQ. No.	PCI INFORMATION SECURITY REQUIREMENT (References are from the Data Security Standard unless noted)
PCI-157	Prohibit direct connections inbound and outbound for traffic between the Internet and the cardholder environment (1.3.3)
PCI-158	Prohibit the passing of internal addresses from the DMZ to the Internet (1.3.4)
PCI-159	Prohibit unauthorized outbound traffic from the cardholder data environment to the Internet (1.3.5)
PCI-160	Implement stateful inspection (i.e., dynamic packet filtering) (1.3.6)
PCI-161	Prohibit the disclosure of private IP addresses and routing information to unauthorized parties (1.3.8)
PCI-162	Develop hardening standards for all system components (2.2)
PCI-163	Enable only necessary and secure services, protocols, daemons, etc. (2.2.2)
PCI-164	Separate development/test and production environments (6.4.1)
PCI-165	Implement separation of duties between development/test and production environments (6.4.2)
PCI-166	Implement change control for patches and software modifications (6.4.5)
PCI-167	Validate buffer overflow boundaries and truncate input streams (6.5.2)
PCI-168	Prevent cryptographic flaws (6.5.3)
PCI-169	Properly encrypt all authenticated and sensitive communications (6.5.4)
PCI-170	Validate all parameters before inclusion (6.5.7)
PCI-171	Properly control access, sanitize input, and do not expose internal object references to users. (6.5.8)
PCI-172	Do not reply on authentication credentials and tokens automatically submitted by browsers to prevent cross-site request forgery (CSRF) (6.5.9)
PCI-173	Require management approve all access and specify required privileges (7.1.3)
PCI-174	Implement an automated access control system (7.1.4)
PCI-175	Establish an access control system for system components with multiple users that restricts access based on need-to-know (7.2.1)
PCI-176	Monitor vendor remote access accounts when in use (8.5.6.b)
PCI-177	Require all user access to, user queries of, and user actions on the database are through programmatic methods only (8.5.16.b)
PCI-178	Restrict direct access or queries to databases to database administrators (8.5.16.c)
PCI-179	Restrict application IDs use to applications and do not allow use of application IDs by individual users or other processes (8.5.16.d)
PCI-180	Protect video cameras and access control mechanisms from tampering or disabling (9.1.1.b)
PCI-181	Monitor video cameras and access control mechanisms and store the monitoring data for at least three months (9.1.1.c)
PCI-182	Implement procedure for granting badges, changing access requirements, and revoking badges (9.2.a)
PCI-183	Restrict access to the badge system to authorized personnel (9.2.b)

REQ. NO.	**PCI INFORMATION SECURITY REQUIREMENT** (References are from the Data Security Standard unless noted)
PCI-184	Implement visitor badges that indicate if a visitor must be escorted (9.3.1)
PCI-185	Implement visitor badges that expire (9.3.2.b)
PCI-186	Record visitor name, firm represented, and onsite individual authorizing access in a visitor log and retain the visitor log for 3 months (9.4.b)
PCI-187	Determine the sensitivity of all media (9.7.1)
PCI-188	Log and track all media removed from the facility (9.7.2)
PCI-189	Maintain inventory logs of all media and conduct media inventories at least annually (9.9.1)
PCI-190	Destroy media when it is no longer needed for business or legal reasons (9.10)
PCI-191	Lock containers containing media to be destroyed to prevent access to its contents (9.10.1.b)
PCI-192	Restrict access to time data to individuals with a need to access time data (10.4.2.a)
PCI-193	Log, monitor, and review all changes to time settings (10.4.2.b)
PCI-194	Accept time settings only from industry-accepted time sources (10.4.3)
PCI-195	Conduct quarterly external network vulnerability scans by an approved scanning vendor (ASV) (11.2.2)
PCI-196	Conduct internal and external vulnerability scans after any significant change to the system components by qualified internal Postal Service staff or qualified external third party (11.2.3)
PCI-197	Develop policies for acceptable use of critical technology (12.3.5)
PCI-198	Develop policies for acceptable network locations for critical technology (12.3.6)
PCI-199	Define information security responsibilities for the Manager, CISO (12.5)
PCI-200	Formally define responsibilities for creating and distributing security policies and procedures (12.5.1)
PCI-201	Formally define responsibilities for monitoring and analyzing security alerts and distributing information to appropriate security and business unit management personnel (12.5.2)
PCI-202	Formally define responsibilities for creating and distributing security incident response and escalation procedures (12.5.3)
PCI-203	Formally define responsibilities for administrating PCI-related user accounts and authentication management (12.5.4)
PCI-204	Formally define responsibilities for monitoring and controlling all access to PCI data (12.5.5)

6-5 Law Enforcement Information Security Requirements

Law enforcement information security requirements must be implemented by all information resources or technology solutions processing law enforcement information. These law enforcement requirements must be included in the technical solution requirements in addition **in addition to the baseline requirements, sensitive requirements, and the sensitive-enhanced requirements**.

REQ. No.	**LAW ENFORCEMENT INFORMATION SECURITY REQUIREMENT** (References are from Handbook AS-805 unless noted)
LE-1	Complete all baseline, sensitive, and sensitive-enhanced requirements (3-4)
LE-2	Implement physical and virtual (enclaves) isolation for law enforcement information (11-3)

6-6 Critical-Moderate Information Security Requirements

Critical-moderate information security requirements must be implemented by all information resources or technology solutions designated as critical-moderate. These critical-moderate requirements must be included in the technical solution requirements **in addition to the baseline requirements**.

REQ. No.	**CRITICAL-MODERATE INFORMATION SECURITY REQUIREMENT** (References are from Handbook AS-805 unless noted)
CM-1	Complete all baseline requirements (3-4)
CM-2	Store hardcopy and media containing critical Postal Service information in a controlled area or a locked cabinet (3-5.3)
CM-3	Implement information resource operational security training to address how to protect critical information resource information throughout the lifecycle (6-5.3)
CM-4	Locate information resource containing critical Postal Service information in a controlled area (7-2.3)
CM-5	Implement off-site storage of critical backup media (9-9.4.4.6)
CM-6	Locate off-site critical backup media storage in a location not subject to the same threats as the original media (9-9.4.4.6)
CM-7	Maintain an inventory of critical backup media offsite or in a fireproof container (9-9.4.4.4)
CM-8	Develop information resource business continuity plans (9-9.5)
CM-9	Complete a table top walkthrough or actual test of the information resource business continuity plans within 180 days of going into production (12-5)
CM-10	Complete a table top walkthrough or actual test of the information resource business continuity plans every 36 months (12-5)

6-7 Critical-High Information Security Requirements

Critical-high information security requirements must be implemented by all information resources or technology solutions designated as critical-high. These critical-high requirements must be included in the technical solution requirements **in addition to the baseline requirements and critical-moderate requirements CM-1 through CM-8**.

REQ. No.	**CRITICAL-HIGH INFORMATION SECURITY REQUIREMENT** (References are from Handbook AS-805 unless noted)
CH-1	Complete all baseline requirements and critical-moderate requirements (3-4)
CH-2	Complete an actual test of the information resource business continuity plans from an offsite location every 18 months using only software, data, and procedures from the offsite location (9-9.5 and 12-5)
CH-3	Based on information resource criticality, provide high availability; e.g., utilize secondary storage devices, implement redundancy, implement fault-tolerant systems, implement a mirrored site, etc. (9-9.6)

6-8 Conditional Information Security Requirements

The following four additional information security requirements can be required based on the situation. Review each security requirement below and determine if the requirement is necessary.

REQ. NO.	INFORMATION SECURITY REQUIREMENT
CR-1	□ Conduct an independent risk assessment if required by CIO, VP IT Operations, Manager CISO, or Function VP Conduct an independent risk assessment if recommended by ISSO because: □ Information resource will be publicly accessible □ Information resource will be developed offsite by non-Postal Service personnel □ Information resource will be hosted at a non-Postal Service site □ Information resource will be managed primarily by non-Postal Service personnel □ Information resource will have high visibility and impact will be high if something negative happens [Refer to AS-805-A, Section 5-2 for additional information on this security requirement.]
CR-2	□ Conduct an independent validation of security testing if required by CIO, VP IT Operations, Manager CISO, or Function VP Conduct an independent validation of security testing if recommended by ISSO because: □ Information resource will be publicly accessible □ Information resource transmits information between a Postal Service network and a public or other non-Postal Service network, or between a Postal Service demilitarized zone (DMZ) and a public network or non-Postal Service network □ Information resource will be developed offsite by non-Postal Service personnel □ Information resource will be hosted at a non-Postal Service site □ Information resource will be managed primarily by non-Postal Service personnel [Refer to AS-805-A, Section 5-4 for additional information on this security requirement.]
CR-3	□ Conduct an independent security code review if required by CIO, VP IT Operations, Manager CISO, or Function VP Conduct an independent security code review if recommended by ISSO because: □ Information resource will be publicly accessible □ Information resource transmits information between a Postal Service network and a public or other non-Postal Service network, or between a Postal Service demilitarized zone (DMZ) and a public network or non-Postal Service network □ Sensitive, sensitive-enhanced, or critical information resource will be developed offsite by non-Postal Service personnel □ Information resource contains COTS programs containing custom programming (HTML, XML, Java, JavaScript, CGI, ActiveX, etc.) or scripts [Refer to AS-805-A, Section 5-1 for additional information on this security requirement.]
CR-4	Conduct a security code review for the following situations (AS-805-A 4-5.4.3): □ Any externally facing or demilitarized zone (DMZ)-hosted information resource containing custom programming or scripting, regardless of the designation of sensitivity or criticality. □ Information resource designated as sensitive-enhanced, sensitive, and critical that contains active content code or CGI scripts. □ Conduct a security code review if recommended by ISSO.

6-9 ISSO Recommended Information Security Requirements

ISSOs may recommend additional information security requirements based on threats and vulnerabilities or generally accepted industry practices to better protect the information resource or technology solution.

REQ. NO.	INFORMATION SECURITY REQUIREMENT
ISSO-1	
ISSO-2	
ISSO-3	
ISSO-4	
ISSO-5	
ISSO-6	

7 BIA APPROVALS

7-1 Non Engineering BIA Approvals

The following BIA approvals are required for Non Engineering information resources or technology solutions:

7-1.1 Executive Sponsor Validation

I acknowledge that the information collected in the BIA is accurate and complete. I understand the need to allocate necessary funding to acquire and maintain information security controls to satisfy the information security requirements documented in this BIA process.

Executive Sponsor (or designee)	**Date (MM/DD/YYYY)**

7-1.2 IT Acceptance of Responsibility

I will ensure that Postal Service information security policies, guidelines, and procedures are followed in the development and integration of this information resource and that appropriate privacy and adequate information security controls are implemented to satisfy the information security requirements documented in this BIA process.

Portfolio Manager (or designee)	**Date (MM/DD/YYYY)**
IBSSC Manager (or designee)	**Date (MM/DD/YYYY)**

7-1.3 Privacy Office Verification

I reviewed this BIA for privacy compliance and sensitivity determination.

Privacy Official	**Date (MM/DD/YYYY)**

7-1.4 ISSO Certification

I certify that this BIA has been completed and that the resulting information security requirements have been transmitted to the Portfolio Manager for inclusion in the Technology Solution Life Cycle (TSLC) requirements and design documents and for implementation during the technology solution development and implementation.

ISSO	**Date (MM/DD/YYYY)**

7-2 Engineering BIA Approvals

The following BIA approvals are required for Engineering information resources or technology solutions:

7-2.1 Engineering Executive Sponsor Acceptance of Responsibility

I acknowledge that the information collected in the BIA is accurate and complete. I understand the need for and am responsible for requesting sufficient funding to acquire and maintain information security controls to satisfy the corporate information security requirements documented in this BIA process. Should sufficient funding not be available to satisfy the security requirements, this information resource will be restricted to the MPE/MHE address space.

Engineering Executive Sponsor (Developing Organization) **Title** **Date (MM/DD/YYYY)**

7-2.2 Engineering (PCES) Manager Acceptance of Responsibility

I acknowledge that the information collected in the BIA is accurate and complete. I understand the need for and am responsible for providing sufficient funding to acquire and maintain information security controls to satisfy the corporate information security requirements documented in this BIA process. Should sufficient funding not be available to satisfy the security requirements, this application will be restricted to the MPE/MHE address space.

Engineering (PCES) Manager (Receiving Organization) **Title** **Date (MM/DD/YYYY)**

7.2-3 Privacy Office Verification

I reviewed this BIA for privacy compliance and sensitivity determination.

Privacy Official **Date (MM/DD/YYYY)**

7.2-4 ISSO Certification

I certify that this BIA has been completed and that the resulting information security requirements have been transmitted to the Engineering Manager for inclusion in the Engineering development life cycle requirements and design documents and for implementation during the technology solution development and implementation.

ISSO **Date (MM/DD/YYYY)**