# Application

# Business Impact Assessment

Version 3.83

September 1, 2006

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

# TABLE OF CONTENTS

1 INTRODUCTION ........ 1

1-1 WHAT THE APPLICATION BIA APPLIES TO ........ 1
1-2 WHAT APPLICATIONS ARE AFFECTED ........ 1
1-3 PURPOSE ........ 1
1-4 WHEN TO PERFORM THE BIA ........ 3
1-5 BIA PROCESS METRICS ........ 3
1-6 BENEFITS OF THE BIA PROCESS ........ 3

2 ROLES AND RESPONSIBILITIES ........ 4

2-1 EXECUTIVE SPONSORS ........ 4
2-2 PORTFOLIO MANAGERS ........ 4
2-3 INFORMATION SYSTEMS SECURITY REPRESENTATIVES ........ 4
2-4 INFORMATION SYSTEMS SECURITY OFFICERS ........ 4
2-5 EXECUTIVE SPONSOR DESIGNEES ........ 5
2-6 PORTFOLIO MANAGER DESIGNEES ........ 5
2-7 PROGRAM MANAGERS ........ 5
2-8 PROJECT MANAGERS ........ 5
2-9 CHIEF PRIVACY OFFICER ........ 5

3 INSTRUCTIONS FOR COMPLETING THE BIA QUESTIONNAIRE ........ 6

SECTION 1 PROJECT IDENTIFICATION ........ 6
SECTION 2 PRIVACY COMPLIANCE ........ 6
SECTION 3 GENERAL DATA ATTRIBUTES ........ 7
SECTION 4 DETERMINATION OF SENSITIVITY ........ 7
SECTION 5 DETERMINATION OF CRITICALITY ........ 7
SECTION 6 GENERAL APPLICATION DATA ........ 8
SECTION 7 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED ........ 8
APPLICATION MODULE REQUIREMENTS GENERATOR ........ 10
SECTION 8 ACCEPTANCE OF RESPONSIBILITY ........ 10
SECTION 9 VERIFICATION ........ 10
BIA WRAP UP ........ 10

APPENDIX A - APPLICATION BIA QUESTIONNAIRE ........ A-1

APPENDIX B - APPLICATION MODULE REQUIREMENTS GENERATOR ........ B-1

APPENDIX C - GOOD BUSINESS PRACTICES ........ C-1

# 1 INTRODUCTION

This document includes an introduction concerning what you need to know, responsibilities, and instructions for completing the Application Business Impact Assessment (BIA) Questionnaire.

**Information Security Assurance—** Process that evaluates the security of applications so that risks can be managed through the lifecycle.

The Questionnaire is attached as Appendix A. In most cases, you will complete an automated version with the information systems security officer (ISSO) who will be assigned to provide guidance and consulting support.

## 1-1 WHAT THE APPLICATION BIA APPLIES TO

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

## 1-2 WHAT APPLICATIONS ARE AFFECTED

A BIA must be completed for all applications, 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 application based on its sensitivity and criticality.

### 1-3.1 DETERMINATION OF COMPLIANCE WITH PRIVACY REQUIREMENTS

The BIA ensures that programs involving customer or employee 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 Application BIA Questionnaire.

### 1-3.2 DETERMINATION OF SENSITIVITY AND CRITICALITY

The Postal Service uses two information designation categories: sensitivity and criticality. All applications are evaluated for both categories:

- Sensitivity

  Sensitivity determines the need to protect the confidentiality and integrity of the information. The levels of sensitivity are: sensitive, business-controlled sensitive, and nonsensitive.

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

- Criticality

  Criticality determines the need for continuous availability of the information. The levels of criticality are: critical, business-controlled critical, and noncritical.

### 1-3.3 Determination of Security Requirements

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

The BIA determines the information security requirements for an application. The security requirements associated with the protection of an application are categorized as baseline, mandatory, discretionary, and discretionary treated as mandatory. The security requirements will vary with the application's sensitivity and criticality designation and the responses to the questions in the BIA Questionnaire.

**Note:** Although not part of the BIA, satisfactory implementation of good business practices by other Postal Service organizations is required for a secure computing environment. See Appendix C, *Good Business Practices*, for a list of these requirements.

- Baseline Requirements

  Baseline security requirements are requirements that must be implemented by all Postal Service applications to protect the Postal Service infrastructure. These requirements are noted with an X in a box in the baseline (BAS) column in Section 7, *Information Security Requirements To Be Implemented*, in the Application BIA Questionnaire.

- Mandatory Requirements

  Mandatory security requirements are requirements that must be implemented based on the sensitivity and criticality designation of the Postal Service applications and the responses to several questions in Section 6, *General Application Data*. In the automated BIA, the software will automatically put an X in a box in the mandatory (MAN) column in Section 7, *Information Security Requirements To Be Implemented*, in the Application BIA Questionnaire. When completing the hardcopy version, the ISSO will indicate the mandatory requirements for the application with an X in a box in the mandatory (MAN) column in Section 7, *Information Security Requirements To Be Implemented*, in the Application BIA Questionnaire.

- Requirements treated as Mandatory

  In some instances, there are security requirements that based on responses to selected questions in Section 6, *General Application Data*, of the BIA Questionnaire must be treated as mandatory. When any of these questions are answered "Yes", the requirement will be noted with an X (automatically by the system or manually by the ISSO) in the MAN column in Section 7, *Information Security Requirements To Be Implemented*, in the Application BIA Questionnaire.

  The four security requirements affected are requirement numbers 4-2, 8-9, 8-10, and 8-15.

- Additional Security Requirements

  Additional security requirements not listed here may be required due to changes in technology, changes in the Postal Service mission, and the discovery of new vulnerabilities in applications and infrastructure during the risk assessment process.

For **nonsensitive** and **noncritical** applications, appropriate controls must be implemented to satisfy the baseline security requirements.

For **sensitive**, **business-controlled sensitive**, **critical**, and **business-controlled critical** applications, the appropriate controls must be implemented to satisfy the baseline security requirements and the mandatory security requirements.

## 1-4 When to Perform the BIA

The Application BIA Questionnaire is completed in the first phase of the application information security assurance (ISA) process and must be updated every five years or whenever a significant change is made to the application.

## 1-5 BIA Process Metrics

Following are the criteria for official classification of applications:

a. The ISSO starts the BIA process and enters the start date in EIR within 10 days after the start of the Definition Phase.

b. The ISSO completes the BIA with the Portfolio Manager and Executive Sponsor together.

c. The Portfolio Manager, Privacy Officer and ISSO all sign BIA within 10 days.

d. After the document is signed by the Portfolio Manager, Privacy Officer and ISSO, the ISSO enters the application sensitivity and criticality designations in EIR within 48 business hours.

e. The application 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.

## 1-6 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 application dependencies.

e. The focusing of security requirements on application 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 applications.

# 2 ROLES AND RESPONSIBILITIES

## 2-1 Executive Sponsors

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

a. Ensuring appropriate privacy and adequate security of their applications.

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

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

d. Determining the sensitivity designation level.

e. Determining the criticality designation level.

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

g. Engaging business partners as required.

**Threat event—** Something external to the application 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 application.

## 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 applications.

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

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

**Assets—** Things of value that contribute to the capability of the application to achieve its business function.

## 2-3 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.

## 2-4 Information Systems Security Officers

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

a. Providing advice and consulting support to executive sponsors and portfolio managers regarding the BIA processes.

b. Facilitating the completion of the BIA.

## 2-5 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.

## 2-6 PORTFOLIO MANAGER DESIGNEES

Portfolio managers may designate in writing Postal Service employees to perform security-related activities on their behalf. However, ultimate accountability and responsibility reside with the portfolio manager.

## 2-7 PROGRAM MANAGERS

Portfolio managers may designate in writing program managers to perform security-related activities on their behalf in support of the executive sponsor.

## 2-8 PROJECT MANAGERS

Project managers are responsible for application development, acquisition, or integration.

## 2-9 CHIEF PRIVACY OFFICER

The chief privacy officer (CPO) is responsible for the following:

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

b. Providing assistance to ensure compliance with privacy requirements.

c. Providing guidance on the sensitivity level determination.

# 3 INSTRUCTIONS FOR COMPLETING THE BIA QUESTIONNAIRE

The format of the automated version generally follows the hardcopy version. The hardcopy versions of the Application BIA Questionnaire is attached as Appendix A. The significant difference between the automated and the manual versions is the time required to generate the associated application requirements. In the automated version, the business rules are applied to the responses by the BIA application to generate the security requirements. In the hardcopy version, the ISSO must review the responses, apply the business roles, and manually mark the appropriate security requirements.

The Business Impact Assessment (BIA) 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, and sharing.

4 *Determination of Sensitivity* – establishes the sensitivity level associated with integrity (i.e., the correctness of application operation and the consistency and accuracy of information) and confidentiality (i.e., the sensitivity of the data collected and importance of each application relative to disclosure).

5 *Determination of Criticality* – establishes the criticality level associated with integrity and unavailability (i.e., the importance of each application relative to the overall mission of the Postal Service).

6 *General Application Data* – identifies information concerning the application that will help determine security requirements.

7 *Information Security Requirements To Be Implemented* – documents the baseline and mandatory (and requirements treated as mandatory) information security requirements for adequately securing the application.

8 *Acceptance of Responsibility* – documents acceptance of responsibility for implementing security controls which will satisfy the information security requirements for the application.

9 *Verification of Completion* – documents the Privacy Official who reviewed the BIA and the ISSO who coordinated the completion of the BIA and presented the information security requirements to the portfolio manager for inclusion in the Integrated Solutions Methodology (ISM) requirements document for implementation during the development/integration process.

Instructions for completing each section of the Application 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*.

### SECTION 2 PRIVACY COMPLIANCE

In Section 2:

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

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

c. The CPO will review the completed Application BIA Questionnaire, and if there are issues regarding privacy compliance or the application 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, *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 SENSITIVITY

Complete Section 4-1, *Data Element Sensitivity Designation*, by checking the elements in Section 4-1.1, *Personal Data*, and Section 4-1.2, *Business Data*, which are included in the application.

**Note:** In the *Business-Controlled Sensitive* portion of Section 4-1.1, *Personal Data*, the checked blocks with an asterisk will be considered business-controlled 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 business-controlled sensitive if it can be associated with a name or other personal identifier.

Complete Section 4-2, *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 dollar fraud would have little impact unless the incident hits the newspaper. Associated with each impact box is the resulting sensitivity determination: NS = Nonsensitive, BCS = Business-Controlled Sensitive, S = Sensitive.

Complete Section 4-3, *Sensitivity Determination Summary*, as follows:

a. Section 4-1, *Data Element Sensitivity Designation*, and Section 4-2, *Impact of Unauthorized Use*, should be considered together to determine application designation.

b. There may be instances where questions will elicit answers with different designations; i.e., sensitive and business-controlled sensitive. In most cases, where sensitive data elements and business-controlled sensitive are checked, the final designation will be sensitive. In most cases, where business-controlled sensitive and non-sensitive data elements are checked, the final designation will be business-controlled sensitive. Exceptions require approval of the CPO.

c. Also, keep in mind that the combination of data elements, in conjunction with their usage in the application and the purpose of the application itself, may make a higher sensitivity designation appropriate, even though a lower designation would apply if the elements were taken alone or in a smaller configuration. For example, an application with many data elements that are business-controlled sensitive may be considered a sensitive application due to the extent of data aggregation.

d. If there are questions, contact the CPO as needed for assistance in making the determination.

**Note:** Passwords, shared secrets, and application and information resource security audit logs, and network configuration information must be protected under the information security policies defined in Handbook AS-805, *Information Security*.

## SECTION 5 DETERMINATION OF CRITICALITY

Complete Section 5 by checking the box that best reflects the impact to the Postal Service if the application were to become unavailable.

a. Complete Section 5-1, *Criticality Determination Summary*, as follows:

   1. If the answer to the CRITICAL question was "Yes," mark the *Critical* box.

   2. If the answer to the BUSINESS-CONTROLLED CRITICAL question was "Yes," mark the *Business-Controlled Critical* box.

   3. If both the CRITICAL and BUSINESS-CONTROLLED CRITICAL questions were answered as "No," mark the *Noncritical* box.

b. Complete Section 5-2*, Determine Internal and External Dependencies,* by entering the dependent application that provide required input to, or receive required input from, the application. An application is dependent if it CANNOT function without the input of another application. Applications that are dependent upon one another must have plans with recovery strategies based on similar recovery time objective. If not, the executive sponsor must negotiate changing the recovery time objective of the application(s) providing or receiving input as appropriate.

**Note:** See Exhibit 1, *Preliminary Recovery Strategies and Associated Costs*, for a graphical representation of recovery strategies and the estimated costs to implement those recovery strategy.

## SECTION 6 GENERAL APPLICATION DATA

In Section 6-1, *System Description*:

a. Enter the information requested to provide a brief system description of the application.

b. Enter a *Projected Deployment Date*.

In Section 6-2, *Development and Deployment Characteristics*:

a. Answer the questions about the development and deployment of the application by checking the appropriate boxes.

b. The responses to these questions will be used to determine additional security requirements.

In Section 6-3, *Network Connectivity Characteristics*:

a. Answer the questions about the network connectivity of the application by checking the appropriate boxes.

b. The responses to these questions will be used to determine whether approval for the proposed connectivity is required by the Network Connectivity Review Board (NCRB). If the answers to any of the questions is "yes", the ISSO will alert the NCRB by sending an e-mail to ncrb@ usps.gov.

In Section 6-4, *Independent Processes*, check the appropriate boxes relative to the need for independent processes.

**Note:** Independent processes are evaluations conducted by independent personnel, contractors, or vendors for the purpose of applying rigorous evaluation standards to applications. 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 application and strictly adheres to the separation of duties policy.

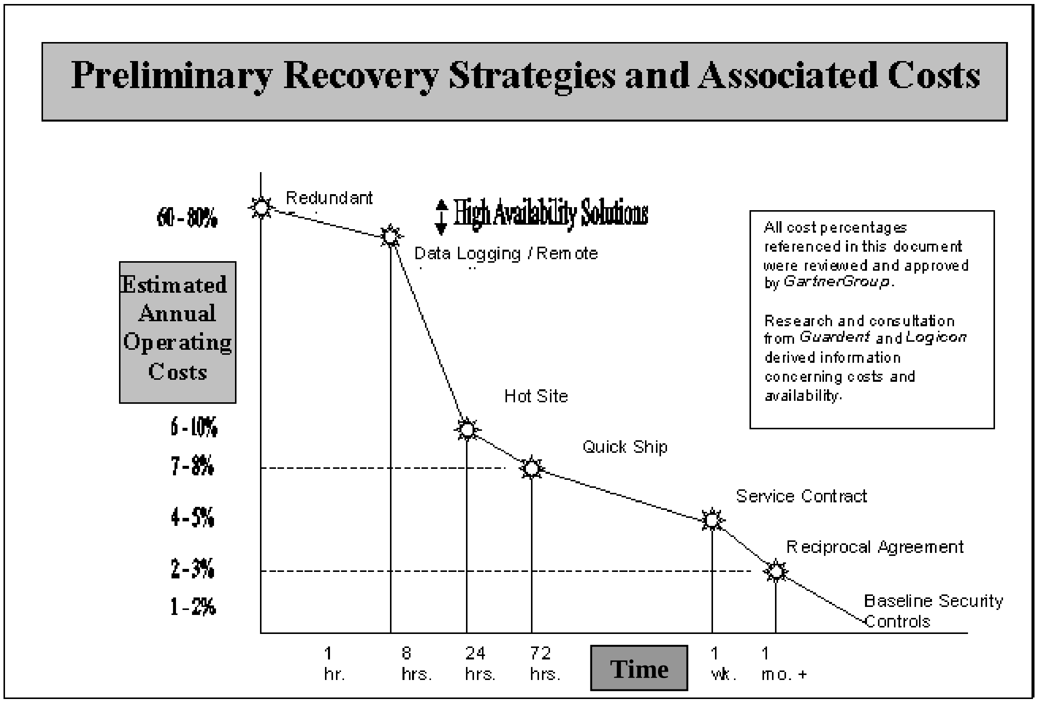
## SECTION 7 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED

The baseline security requirements for all applications are pre-marked with an "X" in the BAS column.

The ISSO marks the mandatory security requirements with an "X" in the MAN column.

The ISSO posts the security requirements to be treated as "mandatory" with an "X" in the MAN column. The four security requirements that could become "mandatory" are requirement numbers 4-2, 8-9, 8-10, and 8-15.

### EXHIBIT 1. PRELIMINARY RECOVERY STRATEGIES AND ASSOCIATED COSTS



**Preliminary Recovery Strategies and Associated Costs**

All cost percentages referenced in this document were reviewed and approved by *GartnerGroup*.

Research and consultation from *Guardent* and *Logicon* derived information concerning costs and availability.

**Recovery Strategy Options and Definitions**

- **Annual Operating Costs:** Costs involved with the purchase and ongoing support of information resources.
- **High Availability Solutions**
  - **Redundant Systems**
    An alternate computer facility that receives simultaneous database and file updates that allows instantaneous operations following a disaster.
  - **Data Logging / Remote Journaling**
    An alternate computer facility that receives delayed database and file updates. Provides for continuity of operations within 8 hours following a disaster.
- **Hot Site:** A back up computer facility with compatible equipment and network connectivity to restore critical processing.
- **Quick Ship:** An agreement with a hardware or recovery vendor that ensures emergency shipment of replacement equipment. Equipment may also be purchased and maintained for emergency shipment.
- **Service Contract:** A pre-purchase agreement with a hardware vendor that guarantees restoration of critical systems (usually within 5 days).
- **Reciprocal Agreement:** An agreement between two organizations whereby each is willing to share their computing facilities during a disaster.

**Note:** Nonsensitive and noncritical applications must implement controls that will satisfy the baseline security requirements and any mandatory security requirements identified in Section 6-2, *Development and Deployment Characteristics*, or in Section 6-4, *Independent Processes*.

**Note:** Business-controlled, sensitive and critical applications must implement controls that will satisfy the baseline security requirements and the checked mandatory security requirements.

### APPLICATION MODULE REQUIREMENTS GENERATOR

Some applications may consist of a parent module and several subordinate modules. Modules may reside on different servers. When completing the BIA Questionnaire, all of the modules must be taken in to account and the classification for the parent application must be set at the highest sensitivity and criticality designation. Also all of the modules must be taken in to account when completing Section 2, *Privacy Compliance.*

For each module where the security requirements may be different than the parent, complete Appendix B, Application Module Requirements Generator (Appendix B). The security requirements for the module will be based on the sensitivity and criticality for that module and the responses to the questions.

### SECTION 8 ACCEPTANCE OF RESPONSIBILITY

The portfolio manager signs and enters today’s date.

### SECTION 9 VERIFICATION

The Privacy Official signs and enters today's date.

The ISSO signs, enters today’s date, and presents the information security requirements to the portfolio manager for inclusion in the Integrated Solutions Methodology (ISM) requirements document and subsequent implementation during the development/integration process.

## BIA WRAP UP

1. File the Application BIA Questionnaire with the ISA documentation package.
2. Forward a copy of the completed and signed BIA Questionnaire to the CPO, CISO, and ISSO at the following addresses:

   Chief Privacy Officer
   U.S. Postal Service
   475 L’Enfant Plaza SW, Room 10407
   Washington, DC 20260-2200

   Information Security Services
   ATTN: ISSO
   4200 Wake Forest Road
   Raleigh, NC 27668-9040

   Corporate Information Security Office
   ATTN: ISA Program Manager
   475 L’Enfant Plaza SW, Room 2441
   Washington, DC 20260-2441

3. If the application is designated as sensitive, business-controlled sensitive, critical, or business-controlled critical, proceed with Phase 2 of the ISA Process.
4. Phase 2 of the ISA Process and beyond does not apply to an application designated as nonsensitive and noncritical. The executive sponsor is responsible for ensuring the baseline security requirements are met throughout the life of the nonsensitive and noncritical application.

# APPENDIX A - APPLICATION BIA QUESTIONNAIRE

# Application Business Impact Assessment (BIA) Questionnaire

APPLICATION NAME: ____________________

EIR NUMBER: ____________________

APPLICATION FINANCE NUMBER: ____________________

SENSITIVITY: ____________________

CRITICALITY: ____________________

DATE: ____________________

## *TABLE OF CONTENTS*

1 PROJECT IDENTIFICATION .......... A–2

2 PRIVACY COMPLIANCE .......... A–3

3 GENERAL DATA ATTRIBUTES .......... A–8

4 DETERMINATION OF SENSITIVITY .......... A–9

5 DETERMINATION OF CRITICALITY .......... A–11

6 GENERAL APPLICATION DATA .......... A–12

7 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED .......... A–14

8 ACCEPTANCE OF RESPONSIBILITY .......... A–17

9 VERIFICATION .......... A–17

Version 3.83

September 1, 2006

# 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: | |
| **Program Manager:** | | **Project Manager:** | |
| Telephone Number: | | Telephone Number: | |
| Email Address: | | Email Address: | |
| **ISSO:** | | **ISSR:** | |
| Telephone Number: | | Telephone Number: | |
| Email Address: | | Email Address: | |
| **Privacy Office Designee:** | | | |
| Telephone Number: | | | |
| Email Address: | | | |

| | |
|---|---|
| **DEVELOPMENT AND PRODUCTION INFORMATION** | |
| **Development Organization:** | |
| **Development Site:** | |
| **Production Site(s):** | |
| **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 maintain in a 'system of records.' A system of records (SOR) is a file or application 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 and the Freedom of Information Act*. (See HBK AS-353, Appendix.)

| | | |
|---|---|---|
| **a.** | **Does the application 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 2-4.) | □ 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 application comply with, all data mgmt practices in the SOR?** | |
| □ | No | □ Yes |
| **e.** | **When is the application expected to be operational?** | |
| | (mm/dd/yyyy) | |
| **f.** | **What is the data retention period for records associated with this application?** | |
| | (specify): | |
| | **What is the process for purging records at the end of that period?** | |
| | (specify): | |
| **g.** | **Will the application 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 application 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. (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. | **Is a privacy notice provided?** | | | | | |
| | □ No (skip to 2-3 and contact Privacy Office.) | □ Yes | | | | |
| d. | **How is a privacy notice provided?** | | | | | |
| □ | **Individual customer** | | | | | |
| | If online, is usps.com privacy policy link on each page of application? | □ Yes | □ No | | | |
| | If by other than usps.com: Does the privacy notice include the following elements? | | | | | |
| | 1. Proximity & Timing: notice provided at time & point of data collection. | □ Yes | □ No | | | |
| | 2. Purpose: describes principal purpose(s) for use of information. | □ Yes | □ No | | | |
| | 3. Authority: specifies legal authority allowing information collection. | □ Yes | □ No | | | |
| | 4. Conditions: says if providing info is voluntary, & effects, if any, of not doing so. | □ Yes | □ No | | | |
| | 5. Disclosures: lists routine use(s) that may be made of information. | □ Yes | □ No | | | |
| □ | **Business customer** | | | | | |
| | 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): | | | | |
| | Does the privacy notice include the following elements? | | | | | |
| | 1. Proximity & Timing: notice provided at time & point of data collection. | □ Yes | □ No | | | |
| | 2. Purpose: describes principal purpose(s) for use of information. | □ Yes | □ No | | | |
| | 3. Authority: specifies legal authority allowing information collection. | □ Yes | □ No | | | |
| | 4. Conditions: says if providing info is voluntary, & effects, if any, of not doing so. | □ Yes | □ No | | | |
| | 5. Disclosures: specifies routine use(s) that may be made of information. | □ Yes | □ No | | | |

## 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 application 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** | *Application must provide method for customer to express consent for secondary use (opt-in).* |
| | How will application provide a mechanism for opt-in? | □ usps.com registration |
| | □ Other (explain): | |
| □ | **Business customers** | *Application must provide method for customer to take affirmative step to prevent secondary use (opt-out).* |
| | How will application provide a mechanism for opt-out? | □ usps.com registration |
| | □ Other (explain): | |
| □ | **Employees (and applicants)** | |
| | Will application 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 application 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

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

| | | | |
|---|---|---|---|
| **a.** | **Are contractors or business partners employed regarding the application?** | | |
| □ | No (skip to 2-7.) | □ Yes | |
| **b.** | **Do contractors/partners have access to customer or employee information?** | | |
| □ | No | □ Yes | |
| **c.** | **Do 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 contractors /partners below.**<br>**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?**<br>**(Check all applicable boxes)** | | | |
| □ | No (skip to d.) | □ blue.usps.gov | □ usps.com | □ Other (URL): |
| **b.** | **Check all 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 application 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 application that operates online?** | |
| □ | No (skip to 2-10.) | □ Yes |
| **b.** | **Does the application obtain age information or birth dates?** | |
| □ | No | □ Yes |
| **c.** | **Do you know, or have reason to expect, that the application will collect information from children under the age of 13?** | |
| □ | No | □ Yes |
| **d.** | **If yes was checked for b. or c., have you read, and will the application comply with, the usps.com privacy policy related to collecting information from children?** | |
| □ | No | □ Yes |

## 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 application 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.** | **Have you considered, or has the application 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 application?** | |
| □ | No (skip to section 3.) | |
| □ | Yes (describe): | |
| | | |
| **d.** | **Have efforts been made to mitigate privacy risks and/or impacts related to the application?** | |
| □ | No | |
| □ | Yes (describe): | |
| | | |

# 3 GENERAL DATA ATTRIBUTES

## 3-1 Data Types

What type of data is being collected, or who does the data apply to? Please check all that apply.

| | |
|---|---|
| □ | Customer (external, non-vendor customer as defined by Section 2, *Privacy Compliance*) |
| □ | USPS Employee |
| □ | USPS Employment Applicant |
| □ | Supplier or Business Partner |
| □ | Mail operations-related data |
| □ | Other (specify): |

## 3-2 Data Sources

Please check all the data sources that apply.

| DATA SOURCES | |
|---|---|
| □ | Customer (external, non-vendor customer) |
| □ | USPS Employee |
| □ | USPS Employment Applicant |
| □ | Supplier or Business Partner |
| □ | Other USPS Data Source |
| □ | 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.

| DATA ACCESS | |
|---|---|
| □ | Customer (external, non-vendor customer) |
| □ | USPS Employees |
| □ | USPS Managers |
| □ | Supplier or Business Partner |
| □ | Other (specify): |

## 3-4 Data Sharing

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

| DATA SHARING | |
|---|---|
| □ | 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 SENSITIVITY

## 4-1 Data Element Sensitivity Designation

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 those data elements in the appropriate table below.

### 4-1.1 PERSONAL DATA

| **Sensitive** | | | |
|---|---|---|---|
| □ Full Social Security Number | □ Fingerprints | □ Biometric Data | □ USPS Personnel Records |
| □ USPS Applicant or Employee Medical Information | □ Information compiled for law enforcement purposes | □ Change of Address with court ordered non-disclosure | □ Other: |

| **Business-Controlled Sensitive** | | | |
|---|---|---|---|
| □ Home Street Address* | □ Home Phone Number* | □ Personal Cell Number* | □ Birth Date/Age* |
| □ Partial Social Security Number* | □ Driver's License Number | □ Credit Card Number (Full or Partial) | □ Race/National Origin* |
| □ Change of Home Address* | □ Other Account Number | □ Marital Status* | □ Family Information |
| □ Customer Obtained Demographic info.* | □ Externally Obtained Demographic Info.* | □ Buying Habits* | □ Web Navigation Habits* |
| □ Bill Payee Name | □ Bill Payee Address | □ Bill Payee Phone Number | □ Bill Payee Acct Number |
| □ Bank Routing Number | □ Bank Account Number | □ Personal Email Address | □ Personal Clubs and Affiliations* |
| □ Income/Assets: | □ Photographs | □ USPS Employee ID Number* | □ Other: |

**Data element with a name or personal identifier is business-controlled sensitive. Data element without a name or personal identifier is nonsensitive.*

| **Nonsensitive** | | | |
|---|---|---|---|
| □ 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 | □ IP Address | □ Gender | □ USPS Employee Title (position) |
| □ Other: | | | |

### 4-1.2 BUSINESS DATA

| **Sensitive** | | | |
|---|---|---|---|
| □ National Security Related Information | □ Communications Protected by Legal Privileges[1] | □ USPS Restricted Financial/Trade Secrets/Proprietary | □ Other: |

| **Business-Controlled Sensitive** | | |
|---|---|---|
| □ Not Publicly Available USPS Documents (withholdable under FOIA) | □ Not Publicly Available Information from Business Partners | □ Other |

| **Non-Sensitive** | | |
|---|---|---|
| □ Publicly Available USPS Information | □ Publicly Available Information from Business Partners | □ Other: |

## 4-2 Impact of Unauthorized Use

| | | |
|---|---|---|
| **1.** | **Is the data subject to potential fraud or manipulation for financial gain? Check one.** | |
| □ | Information has little or no potential to be used for financial gain through fraud or manipulation. | NS |
| □ | Information has moderate potential to be used for financial gain through fraud or manipulation. | BCS |
| □ | Information has significant potential to be used for financial gain through fraud or manipulation. | S |
| **2.** | **What is the impact on USPS of unauthorized disclosure or misuse of the information? Check one.** (Includes revenue denied due to loss of business or market share, civil and legal penalties, impact to brand.) | |
| □ | Unauthorized disclosure or misuse of the information would result in little or no financial loss or negative impact to brand. | NS |
| □ | Unauthorized disclosure or misuse of the information would result in moderate financial loss or negative impact to brand. | BCS |
| □ | Unauthorized disclosure or misuse of the information would result in significant financial loss or negative impact to brand. | S |
| **3.** | **What is the impact on the individual on whom information is maintained if unauthorized disclosure or misuse of information occurs? Check one.** | |
| □ | Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual. | NS |
| □ | Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual. | BCS |
| □ | Results in significant harm, embarrassment, inconvenience, or unfairness to the individual. | S |

## 4-3 Sensitivity Determination Summary

Based on an evaluation of the responses and the type of information being collected, this application is designated as (check one):

| | | |
|---|---|---|
| □ **Nonsensitive** | □ **Business-Controlled Sensitive** | □ **Sensitive** |

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

# 5 DETERMINATION OF CRITICALITY

| CRITICAL | | Yes | No |
|---|---|---|---|
| | Would the nonavailability of your application have a negative impact on customer or employee life, safety, or health; a significant negative impact on the movement of mail; a significant negative impact on financial activities related to cash flow; or provide required input which is required for the continued operation of a critical application and there are no other alternatives available? | | |
| **BUSINESS-CONTROLLED CRITICAL** | | **Yes** | **No** |
| | Would the nonavailability of your application have a moderate negative impact on the movement of mail; a moderate negative impact on financial activities related to cash flow; provide required input which is required for the continued operation of a business-controlled critical application and there are no other alternatives available; result in a substantial or enduring negative impact on public confidence, brand, or image; result in substantial additional expenses, increased costs, or penalties; result in substantial potential for fraud or diversion of goods; result in a substantial violation of regulatory or contractual requirements, or USPS standards; or result in a substantial negative impact on real-time decision making and there are no other alternatives available? | | |
| | **NONCRITICAL** | | |
| | Your application is noncritical if it is not critical or business-controlled critical. | | |

## 5-1 Criticality Determination Summary

Based on an evaluation of the responses, this application is designated as (check one):

| | | |
|---|---|---|
| □ **Noncritical** | □ **Business-Controlled Critical** | □ **Critical** |

## 5-2 Determine Internal or External Dependencies

In the table below, identify dependent applications that provide input to or receive support from the application. A system is dependent if it **CANNOT** function without the input or link of the other system or portal. Applications that are dependent upon one another must have plans with recovery strategies based on the same RTO. (Continue the list on a separate page if necessary.)

**Note**: Go to the Enterprise Information Repository (EIR) at http://eir/ to identify the RTO for an application.

| | Name of Application | External or Internal (E or I) | EIR Number | Provides Input to This Application (Y or N) | Receives Support from this Application (Y or N) | RTO (If Known) | Criticality (C, BCC, or NC) |
|---|---|---|---|---|---|---|---|
| 1. | | | | | | | |
| 2. | | | | | | | |
| 3. | | | | | | | |
| 4. | | | | | | | |

# 6 GENERAL APPLICATION DATA

## 6-1 System Description

| | |
|---|---|
| **Supporting Application Software:** | |
| **Operating System:** | |
| **Data or Database:** | |
| **Hardware:** | |
| **Network:** | |
| **Communications:** | |
| **Security Software:** | |
| **Other:** | |
| **Projected Production Date:** | |

## 6-2 Development and Deployment Characteristics

| | **Question** | **Yes** | **No** |
|---|---|---|---|
| 1. | Will the application be publicly accessible? | | |
| 2. | Will the application be developed offsite primarily by non-Postal Service personnel? | | |
| 3. | Will the application be hosted at a non-Postal Service site? | | |
| 4. | Will the application be managed primarily by non-Postal Service personnel? | | |
| 5. | Will the application have high visibility or high impact if there is security incident? | | |
| 6. | Does the COTS product contain custom programming or scripts? | | |
| 7. | Is the application an externally-facing application containing custom programming (HTML, XML, Java, JavaScript, CGI, ActiveX, etc.)? | | |
| 8. | Does the application transmit 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? | | |
| 9. | Is credit card information stored in a secure, access controlled location? | | |

| Question | | Yes | No |
|---|---|---|---|
| 10. | Will access to this information increase the opportunity for theft, collusion, fraud, blackmail, or prevent the timely performance of Postal Service operations? | | |
| 11. | Is there an opportunity for disclosure, unavailability, modification or damage to the application, or prevention of timely performance of Postal Service operations if operational training is not provided? | | |
| 12. | Does application contain Active Content or CGI code? | | |
| 13. | Is the data collected, stored, analyzed, or maintained by this application available in another form or from another source? | | |
| 14. | Would the unavailability of this application prevent the timely performance of Postal Service operations? | | |

## 6-3 Network Connectivity Characteristics

| Question | | Yes | No |
|---|---|---|---|
| 1. | Will the application utilize connections of non-Postal systems or networks to the Postal Service Intranet infrastructure including dial-up or VPN? | | |
| 2. | Will the application utilize nonstandard (not on the Postal network infrastructure) Postal-to-Postal connectivity? | | |
| 3. | Will the application utilize connections via Internet including Postal-to-Postal (e.g., cable or DSL)? | | |
| 4. | Will the application extend the Postal Intranet into a remote site of a business partner? | | |
| 5. | Will the application require a change to a perimeter firewall configuration? | | |
| 6. | Will the application require a change to a secure enclave firewall configuration? | | |
| 7. | Will the application utilize a wireless LAN, wireless access point, or wireless devices such as PDAs? | | |
| 8. | Will the application access development, production, or internal Postal networks via the Internet or Internet connectivity? | | |

## 6-4 Independent Processes

| Determination of the Need for Independent Processes | Yes | No |
|---|---|---|
| Has the VP/CTO, Manager Corporate Information Security Office (CISO), or Vice-President of the functional business area designated the application as requiring an: | [redacted] | [redacted] |
| 1. Independent risk assessment? | | |
| 2. Independent code review? | | |
| 3. Independent validation of security testing? | | |

# 7 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED

***LEGEND:* *BAS*: *Baseline,* *MAN*: *Mandatory***

| REQ. NO. | INFORMATION SECURITY REQUIREMENT<br>(HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE) | BAS | MAN |
|---|---|---|---|
| 1-1 | Identify application, business requirements, and related roles and responsibilities (AS-805: 1-1) | X | |
| 3-4 | Label hardcopy and storage media as “restricted information” (AS-805: 3-5.1) | ■ | |
| 3-5 | Label login/password screen or welcome screen as "Information within this application is designated as sensitive or business-controlled sensitive and should be protected from unauthorized access or disclosure" (AS-805: 3-5.1) | ■ | |
| 3-6 | Protect sensitive and business-controlled sensitive information (both digital and hardcopy) from unauthorized access and disclosure. Protect critical and business-controlled critical information from unauthorized access (AS-805: 3-5.2) | ■ | |
| 3-7 | Implement appropriate disposal and destruction procedures (AS-805: 3-5.6); eradicate information on hardware and electronic media prior to re-use by another program or being released for maintenance (AS-805: 3-5.6.2, 3-5.5.4) | X | |
| 3-9 | Release information on clean, virus-free media (AS-805: 3-5.5.3) | X | |
| 4-1 | Complete an application risk assessment or an abbreviated application risk assessment (AS-805: 4-1, 4-4.1) | ■ | |
| 4-3 | Complete a site security review (AS-805: 4-6.1) | ■ | |
| 5-2 | Evaluate the use of cookies and other user tracking mechanisms (AS-805: 5-9.3.1, 5-9.3.2) | X | |
| 5-5 | Notify customers before transfer to an external site not under Postal Service control (AS-805: 5-9.3.3) | X | |
| 6-1 | Request clearance or background screening for applicable personnel (AS-805: 6-5) | ■ | |
| 6-2 | Implement appropriate separation of duties and responsibilities (AS-805: 6-3.1) | ■ | |
| 6-4 | Implement application operational security training. The training should address how to protect application information throughout the lifecycle (AS-805: 6-6.3) | ■ | |
| 6-5 | Submit eAccess changes and collect keys, badges, smart cards, and sensitive materials when personnel transfer or terminate (AS-805: 9-7.4.2, 6-7) | X | |
| 7-2 | Locate application (e.g., server, process controller) in a controlled area (room level security) (AS-805: 7-3.1.1, 7-3.1.2) | ■ | |
| 7-13 | Protect applications being removed from a secure environment and sensitive and business-controlled sensitive information residing on them (AS-805: 7-3.2) | ■ | |
| 8-1 | Develop and maintain an application security plan or abbreviated application security plan (AS-805-A: 4-2.4.6) | ■ | |
| 8-2 | Develop and execute an application security test and evaluation [ST&E] plan ( AS-805-A: 4-3.4.1, 4-3.4.2) | ■ | |
| 8-4 | Provide high-level architectural diagrams (AS-805-A: 4-1.4.4); submit documentation for secure enclave assessment (AS-805:11-5.8) | X | |
| 8-6 | Document application security settings, perform timely application maintenance, and control tools, techniques, and mechanisms used to conduct application system maintenance (AS-805: 8-6.5.1) | ■ | |
| 8-7 | Include information security in service level agreements [SLA] (internal and external systems) and trading partner agreements [TPA] (external systems only) (AS-805-A: 4-1.4.5) | X | |
| 8-11 | Conduct penetration tests and vulnerability scans (AS-805: 5-3) | ■ | |

| REQ. NO. | INFORMATION SECURITY REQUIREMENT (HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE) | BAS | MAN |
|---|---|---|---|
| 8-12 | Comply with Postal Service testing environment restriction policies (AS-805: 8-3.6) | X | |
| 8-15 | Conduct security code review (AS-805-A: 4-3.4.4) | ■ | |
| 9-1 | Protect data from modification or deletion by unauthorized users (AS-805: 9-9.2) | X | |
| 9-2 | Uniquely identify and authenticate each user (AS-805: 9-6, 9-7); comply with authentication requirements established in Postal Service policies (AS-805: 9-7) | X | |
| 9-3 | Restrict supervisory and administrative privileges (AS-805: 9-5.3.2) | X | |
| 9-4 | Implement session management including timeouts and screen savers where the platform permits (AS-805: 9-7.9) | X | |
| 9-6 | Implement logical access security (AS-805: 9-11) | ■ | |
| 9-7 | Authorize access based on need-to-know and least privilege (AS-805: 9-4.1.2, 9-4.1.4) | X | |
| 9-8 | Encrypt appropriate information transmitted over untrusted networks (AS-805: 9-8.2.1, 3-5.4.1) based on Postal Service encryption and key recovery policies (AS-805: 9-8.2, 5-6.3) | ■ | |
| 9-9 | Encrypt information stored in a non-secure location (AS-805: 9-8.2.2, 3-5.4.2) based on Postal Service encryption and key recovery policies (AS-805: 9-8.2, 5-6.3) | ■ | |
| 9-10 | Encrypt information stored in a secure location (onsite and offsite) (AS-805: 9-8.2.2, 3-5.4.2) based on Postal Service encryption and key recovery policies (AS-805: 9-8.2, 5-6.3) | ■ | |
| 9-12 | Implement application level auditing and logging (AS-805: 9-12) | X | |
| 9-14 | Protect, review, retain, and maintain application audit logs (AS-805: 9-12) | X | |
| 10-1 | Implement virus protection (AS-805: 10-7) | X | |
| 10-2 | Establish and maintain baseline information resource configurations and inventories (including hardware, software, firmware, and documentation) (AS-805: 10-4.2, 10-3.5) | X | |
| 10-3 | Implement application on a server hardened to Postal Service standards (AS-805: 10-5.3.1) | X | |
| 10-4 | Install patches in a timely manner (AS-805: 10-4.5) | X | |
| 10-5 | Evaluate Active content or CGI code (AS-805: 10-7.2.2) | ■ | |
| 10-7 | Implement appropriate database security (AS-805: 10-6.6.2) | X | |
| 11-6 | Acquire approval in advance for modem access to and from Postal Service networks and implement protection measures in accordance with Postal Service remote access security policies (AS-805: 11-12.3) | X | |
| 12-1 | Develop and test an application disaster recovery plan [ADRP] (AS-805: 12-5) | ■ | |
| 12-4 | Implement backup and recovery procedures (AS-805: 12-8) | X | |
| 12-5 | Implement off-site storage of backup media (AS-805: 12-8.5) | ■ | |
| 12-6 | Utilize secondary storage device (network attached or, RAID storage); implement redundancy (redundant components, servers, infrastructures); implement fault-tolerant systems; implement a mirrored site (AS-805: 9-10); and maintain an inventory of backup media offsite (AS-805: 12-8.3) | ■ | |
| 13-1 | Report incidents in accordance with Postal Service policies (AS-805: 13-6.1) | X | |
| 14-1 | Implement authorized warning banner (AS-805: 14-5.5) | X | |

| REQ. NO. | INFORMATION SECURITY REQUIREMENT<br>(HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE) | BAS | MAN |
|---|---|---|---|
| 4-2 | Conduct an independent risk assessment (AS-805-A: 5-2)<br>□ Requested by VP/CTO, Manager CISO, or Function VP<br>□ Application will be publicly accessible<br>□ Application will be developed offsite by non-Postal Service personnel<br>□ Application will be hosted at a non-Postal Service site<br>□ Application will be managed primarily by non-Postal Service personnel<br>□ Application will have high visibility and impact will be high if something negative happens | ▨ | |
| 8-9 | Conduct independent validation of security testing (AS-805-A: 5-4)<br>□ Requested by VP/CTO, Manager CISO, or Function VP<br>□ Application will be publicly accessible | ▨ | |
| 8-10 | Conduct independent security code review (AS-805-A: 5-1)<br>□ Requested by VP/CTO, Manager CISO, or Function VP<br>□ Application will be publicly accessible<br>□ Application will be developed offsite by non-Postal Service personnel | ▨ | |

## 8 ACCEPTANCE OF RESPONSIBILITY

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

| | |
|---|---|
| **Portfolio Manager (as Executive Sponsor designee)** | **Date (MM/DD/YYYY)** |

## 9 VERIFICATION

I reviewed this BIA for privacy compliance and sensitivity determination.

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

I coordinated the completion of this BIA and submitted the resulting information security requirements to the Portfolio Manager for inclusion in the Integrated Solutions Methodology (ISM) requirements document and subsequent implementation during the development/integration process.

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

# APPENDIX B - APPLICATION MODULE REQUIREMENTS GENERATOR

UNITED STATES POSTAL SERVICE™

# Application Module Requirements Generator

*Some applications may consist of a parent module and several subordinate modules. Modules may reside on different servers. When completing the BIA Questionnaire, all of the modules must be taken in to account and the classification for the parent application must be set at the highest sensitivity and criticality designation.*

*For each module where the security requirements may be different than the parent, enter the information requested below. The security requirements for the module will be based on the sensitivity and criticality for that module and the responses to the questions below.*

**MODULE NAME:** Module Name

**EIR NUMBER:** ______________________

**SENSITIVITY:** ______________________

**CRITICALITY:** ______________________

**BRIEF DESCRIPTION:**

## 1 DETERMINATION OF CRITICALITY

| CRITICAL | Yes | No |
|---|---|---|
| Would the nonavailability of your application have a negative impact on customer or employee life, safety, or health; a significant negative impact on the movement of mail; a significant negative impact on financial activities related to cash flow; or provide required input which is required for the continued operation of a critical application and there are no other alternatives available? | | |
| **BUSINESS-CONTROLLED CRITICAL** | **Yes** | **No** |
| Would the nonavailability of your application have a moderate negative impact on the movement of mail; a moderate negative impact on financial activities related to cash flow; provide required input which is required for the continued operation of a business-controlled critical application and there are no other alternatives available; result in a substantial or enduring negative impact on public confidence, brand, or image; result in substantial additional expenses, increased costs, or penalties; result in substantial potential for fraud or diversion of goods; result in a substantial violation of regulatory or contractual requirements, or USPS standards; or result in a substantial negative impact on real-time decision making and there are no other alternatives available? | | |
| **NONCRITICAL** | | |
| Your application is noncritical if it is not critical or business-controlled critical. | | |

## 1-1 Criticality Determination Summary

Based on an evaluation of the responses, this application is designated as (check one):

| | | |
|---|---|---|
| □ **Noncritical** | □ **Business-Controlled Critical** | □ **Critical** |

# 2 DETERMINATION OF SENSITIVITY

## 2-1 Data Element Sensitivity Designation

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 those data elements in the appropriate table below.

### 2-1.1 PERSONAL DATA

| **Sensitive** | | | |
|---|---|---|---|
| □ Full Social Security Number | □ Fingerprints | □ Biometric Data | □ USPS Personnel Records |
| □ USPS Applicant or Employee Medical Information | □ Information compiled for law enforcement purposes | □ Change of Address with court ordered non-disclosure | □ Other: |

| **Business-Controlled Sensitive** | | | |
|---|---|---|---|
| □ Home Street Address* | □ Home Phone Number* | □ Personal Cell Number* | □ Birth Date/Age* |
| □ Partial Social Security Number* | □ Driver's License Number | □ Credit Card Number (Full or Partial) | □ Race/National Origin* |
| □ Change of Home Address* | □ Other Account Number | □ Marital Status* | □ Family Information |
| □ Customer Obtained Demographic info.* | □ Externally Obtained Demographic Info.* | □ Buying Habits* | □ Web Navigation Habits* |
| □ Bill Payee Name | □ Bill Payee Address | □ Bill Payee Phone Number | □ Bill Payee Acct Number |
| □ Bank Routing Number | □ Bank Account Number | □ Personal Email Address | □ Personal Clubs and Affiliations* |
| □ Income/Assets: | □ Photographs | □ USPS Employee ID Number | □ Other: |

**Data element with a name or personal identifier is business-controlled sensitive. Data element without a name or personal identifier is nonsensitive.*

| **Nonsensitive** | | | |
|---|---|---|---|
| □ 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 | □ IP Address | □ Gender | □ USPS Employee Title (position) |
| □ Other: | | | |

### 2-1.2 BUSINESS DATA

| **Sensitive** | | | |
|---|---|---|---|
| □ National Security Related Information | □ Communications Protected by Legal Privileges[2] | □ USPS Restricted Financial/Trade Secrets/Proprietary | □ Other: |

| **Business-Controlled Sensitive** | | |
|---|---|---|
| □ Not Publicly Available USPS Documents (withholdable under FOIA) | □ Not Publicly Available Information from Business Partners | □ Other |

| **Non-Sensitive** | | |
|---|---|---|
| □ Publicly Available USPS Information | □ Publicly Available Information from Business Partners | □ Other: |

## 2-2 Impact of Unauthorized Use

| **1.** | **Is the data subject to potential fraud or manipulation for financial gain? Check one.** | |
|---|---|---|
| □ | Information has little or no potential to be used for financial gain through fraud or manipulation. | NS |
| □ | Information has moderate potential to be used for financial gain through fraud or manipulation. | BCS |
| □ | Information has significant potential to be used for financial gain through fraud or manipulation. | S |
| **2.** | **What is the impact on USPS of unauthorized disclosure or misuse of the information? Check one.** (Includes revenue denied due to loss of business or market share, civil and legal penalties, impact to brand.) | |
| □ | Unauthorized disclosure or misuse of the information would result in little or no financial loss or negative impact to brand. | NS |
| □ | Unauthorized disclosure or misuse of the information would result in moderate financial loss or negative impact to brand. | BCS |
| □ | Unauthorized disclosure or misuse of the information would result in significant financial loss or negative impact to brand. | S |
| **3.** | **What is the impact on the individual on whom information is maintained if unauthorized disclosure or misuse of information occurs? Check one.** | |
| □ | Results in little or no harm, embarrassment, inconvenience, or unfairness to the individual. | NS |
| □ | Results in moderate harm, embarrassment, inconvenience, or unfairness to the individual. | BCS |
| □ | Results in significant harm, embarrassment, inconvenience, or unfairness to the individual. | S |

## 2-3 Sensitivity Determination Summary

Based on an evaluation of the responses and the type of information being collected, this application is designated as (check one):

| | | |
|---|---|---|
| □ **Nonsensitive** | □ **Business-Controlled Sensitive** | □ **Sensitive** |

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

# 3 DEVELOPMENT AND DEPLOYMENT CHARACTERISTICS

| Question | | Yes | No |
|---|---|---|---|
| 1. | Will the application be publicly accessible? | | |
| 2. | Will the application be developed offsite primarily by non-Postal Service personnel? | | |
| 3. | Will the application be hosted at a non-Postal Service site? | | |
| 4. | Will the application be managed primarily by non-Postal Service personnel? | | |
| 5. | Will the application have high visibility or high impact if there is security incident? | | |
| 6. | Does the COTS product contain custom programming or scripts? | | |
| 7. | Is the application an externally-facing application containing custom programming (HTML, XML, Java, JavaScript, CGI, ActiveX, etc.)? | | |
| 8. | Does the application transmit 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? | | |
| 9. | Is credit card information stored in a secure, access controlled location? | | |
| 10. | Will access to this information increase the opportunity for theft, collusion, fraud, blackmail, or prevent the timely performance of Postal Service operations? | | |
| 11. | Is there an opportunity for disclosure, unavailability, modification or damage to the application, or prevention of timely performance of Postal Service operations if operational training is not provided? | | |
| 12. | Does application contain Active Content or CGI code? | | |
| 13. | Is the data collected, stored, analyzed, or maintained by this application available in another form or from another source? | | |
| 14. | Would the unavailability of this application prevent the timely performance of Postal Service operations? | | |

# 4 INFORMATION SECURITY REQUIREMENTS TO BE IMPLEMENTED

***LEGEND: BAS**: Baseline, **MAN**: Mandatory*

| REQ. NO. | INFORMATION SECURITY REQUIREMENT (HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE) | BAS | MAN |
|---|---|---|---|
| 1-1 | Identify application, business requirements, and related roles and responsibilities (AS-805: 1-1) | X | |
| 3-4 | Label hardcopy and storage media as "restricted information" (AS-805: 3-5.1) | ▨ | |
| 3-5 | Label login/password screen or welcome screen as "Information within this application is designated as sensitive or business-controlled sensitive and should be protected from unauthorized access or disclosure" (AS-805: 3-5.1) | ▨ | |
| 3-6 | Protect sensitive and business-controlled sensitive information (both digital and hardcopy) from unauthorized access and disclosure. Protect critical and business-controlled critical information from unauthorized access (AS-805: 3-5.2) | ▨ | |
| 3-7 | Implement appropriate disposal and destruction procedures (AS-805: 3-5.6); eradicate information on hardware and electronic media prior to re-use by another program or being released for maintenance (AS-805: 3-5.6.2, 3-5.5.4) | X | |
| 3-9 | Release information on clean, virus-free media (AS-805: 3-5.5.3) | X | |
| 4-1 | Complete an application risk assessment or an abbreviated application risk assessment (AS-805: 4-1, 4-4.1) | ▨ | |
| 4-3 | Complete a site security review (AS-805: 4-6.1) | ▨ | |
| 5-2 | Evaluate the use of cookies and other user tracking mechanisms (AS-805: 5-9.3.1, 5-9.3.2) | X | |
| 5-5 | Notify customers before transfer to an external site not under Postal Service control (AS-805: 5-9.3.3) | X | |
| 6-1 | Request clearance or background screening for applicable personnel (AS-805: 6-5) | ▨ | |
| 6-2 | Implement appropriate separation of duties and responsibilities (AS-805: 6-3.1) | ▨ | |
| 6-4 | Implement application operational security training. The training should address how to protect application information throughout the lifecycle (AS-805: 6-6.3) | ▨ | |
| 6-5 | Submit eAccess changes and collect keys, badges, smart cards, and sensitive materials when personnel transfer or terminate (AS-805: 9-4.2.7, 6-7) | X | |
| 7-2 | Locate application (e.g., server, process controller) in a controlled area (room level security) (AS-805: 7-3.1.1, 7-3.1.2) | ▨ | |
| 7-13 | Protect applications being removed from a secure environment and sensitive and business-controlled sensitive information residing on them (AS-805: 7-3.2) | ▨ | |
| 8-1 | Develop and maintain an application security plan or abbreviated application security plan (AS-805-A: 4-2.4.6) | ▨ | |
| 8-2 | Develop and execute an application security test and evaluation [ST&E] plan ( AS-805-A: 4-3.4.1, 4-3.4.2) | ▨ | |
| 8-4 | Provide high-level architectural diagrams (AS-805-A: 4-1.4.4); submit documentation for secure enclave assessment (AS-805: 11-5.8) | X | |
| 8-6 | Document application security settings, perform timely application maintenance, and control tools, techniques, and mechanisms used to conduct application system maintenance (AS-805: 8-6.5.1) | ▨ | |
| 8-7 | Include information security in service level agreements [SLA] (internal and external systems) and trading partner agreements [TPA] (external systems only) (AS-805-A: 4-1.4.5) | X | |
| 8-11 | Conduct penetration tests and vulnerability scans (AS-805-A: 5-3) | ▨ | |

| **REQ. NO.** | **INFORMATION SECURITY REQUIREMENT (HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE)** | **BAS** | **MAN** |
|---|---|---|---|
| 8-12 | Comply with Postal Service testing environment restriction policies (AS-805: 8-3.6) | X | |
| 8-15 | Conduct security code review (AS-805-A: 4-3.4.4) | ▨ | |
| 9-1 | Protect data from modification or deletion by unauthorized users (AS-805: 9-9.2) | X | |
| 9-2 | Uniquely identify and authenticate each user (AS-805: 9-6, 9-7); comply with authentication requirements established in Postal Service policies (AS-805: 9-7) | X | |
| 9-3 | Restrict supervisory and administrative privileges (AS-805: 9-5.3.2) | X | |
| 9-4 | Implement session management including timeouts and screen savers where the platform permits (AS-805: 9-7.9) | X | |
| 9-6 | Implement logical access security (AS-805: 9-11) | ▨ | |
| 9-7 | Authorize access based on need-to-know and least privilege (AS-805: 9-4.1.2, 9-4.1.4) | X | |
| 9-8 | Encrypt appropriate information transmitted over untrusted networks (AS-805: 9-8.2.1, 3-5.4.1) based on Postal Service encryption and key recovery policies (AS-805: 9-8.2, 5-6.3) | ▨ | |
| 9-9 | Encrypt information stored in a non-secure location (AS-805: 9-8.2.2, 3-5.4.2) based on Postal Service encryption and key recovery policies (AS-805: 9-8.2, 5-6.3) | ▨ | |
| 9-10 | Encrypt information stored in a secure location (onsite and offsite) (AS-805: 9-8.2.2, 3-5.4.2) based on Postal Service encryption and key recovery policies (AS-805: 9-8.2, 5-6.3) | ▨ | |
| 9-12 | Implement application level auditing and logging (AS-805: 9-12) | X | |
| 9-14 | Protect, review, retain, and maintain application audit logs (AS-805: 9-12) | X | |
| 10-1 | Implement virus protection (AS-805: 10-7) | X | |
| 10-2 | Establish and maintain baseline information resource configurations and inventories (including hardware, software, firmware, and documentation) (AS-805: 10-4.2, 10-3.5) | X | |
| 10-3 | Implement application on a server hardened to Postal Service standards (AS-805: 10-5.3.1) | X | |
| 10-4 | Install patches in a timely manner (AS-805: 10-4.5) | X | |
| 10-5 | Evaluate Active content or CGI code (AS-805: 10-7.2.2) | ▨ | |
| 10-7 | Implement appropriate database security (AS-805: 10-6.6.2) | X | |
| 11-6 | Acquire approval in advance for modem access to and from Postal Service networks and implement protection measures in accordance with Postal Service remote access security policies (AS-805: 11-12.3) | X | |
| 12-1 | Develop and test an application disaster recovery plan [ADRP] (AS-805: 12-5) | ▨ | |
| 12-4 | Implement backup and recovery procedures (AS-805: 12-8) | X | |
| 12-5 | Implement off-site storage of backup media (AS-805: 12-8.5) | ▨ | |
| 12-6 | Utilize secondary storage device (network attached or, RAID storage); implement redundancy (redundant components, servers, infrastructures); implement fault-tolerant systems; implement a mirrored site (AS-805: 9-10); and maintain an inventory of backup media offsite (AS-805: 12-8.3) | ▨ | |
| 13-1 | Report incidents in accordance with Postal Service policies (AS-805: 13-6.1) | X | |
| 14-1 | Implement authorized warning banner (AS-805: 14-5.5) | X | |

| REQ. No. | Information Security Requirement<br>(Handbook AS-805, *Information Security*, or Handbook AS-805-A, *Application Information Security Assurance Process*, Reference) | B<br>A<br>S | M<br>A<br>N |
|---|---|---|---|
| 4-2 | Conduct an independent risk assessment (AS-805-A: 5-2)<br>□ Requested by VP/CTO, Manager CISO, or Function VP<br>□ Application will be publicly accessible<br>□ Application will be developed offsite by non-Postal Service personnel<br>□ Application will be hosted at a non-Postal Service site<br>□ Application will be managed primarily by non-Postal Service personnel<br>□ Application will have high visibility and impact will be high if something negative happens | | |
| 8-9 | Conduct independent validation of security testing (AS-805-A: 5-4)<br>□ Requested by VP/CTO, Manager CISO, or Function VP<br>□ Application will be publicly accessible | | |
| 8-10 | Conduct independent security code review (AS-805-A: 5-1)<br>□ Requested by VP/CTO, Manager CISO, or Function VP<br>□ Application will be publicly accessible<br>□ Application will be developed offsite by non-Postal Service personnel | | |

# 5 ACCEPTANCE OF RESPONSIBILITY

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

| | |
|---|---|
| **Portfolio Manager (as Executive Sponsor designee)** | **Date (MM/DD/YYYY)** |

# 6 VERIFICATION

I reviewed this BIA for privacy compliance and sensitivity determination.

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

I coordinated the completion of this BIA and submitted the resulting information security requirements to the Portfolio Manager for inclusion in the Integrated Solutions Methodology (ISM) requirements document and subsequent implementation during the development/integration process.

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

# APPENDIX C - GOOD BUSINESS PRACTICES

UNITED STATES POSTAL SERVICE™

# Good Business Practices for Information Security

Version 3.0
December 24, 2002

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

The requirements for the protection of Postal Service applications are a combination of information security requirements championed by the Corporate Information Security Office (CISO) and requirements championed by other Postal Service organizations. For the purpose of this document, these latter requirements are described as good business practices. Good business practices apply to all Postal Service applications. The following good business practices have been identified to support a secure computing environment:

| REQ No. | Security Requirement |
|---|---|
| 2-2 | **Comply with applicable laws, regulations and policies** (e.g., Privacy Act, Freedom of Information Act, Gramm-Leach-Bliley Act, PDD 63, PDD 67, ASM, Handbook AS 805, Handbook AS-805-A) |
| 3-1 | **Update Enterprise Information Repository (EIR)** – EIR entry needs to be accurate and up-to-date with complete information. |
| 3-6 | **Implement appropriate data retention procedures** – Ensure that data is retained for the appropriate period as specified in Postal Service policy (see ASM, subchapter 35 for information). In addition, the Records Office can provide further guidance. |
| 5-1 | **Comply with software licensing agreements** – All software used at Postal Service must be procured in accordance with Postal Service policies and procedures and be licensed and registered in the name of the Postal Service. All personnel must abide by software copyright laws and must not obtain, install, replicate, or use software except as permitted by the software licensing agreement. |
| 5-3 | **Obtain all hardware and software from Official Postal Service Sources** – All hardware and software must be obtained from official Postal Service sources. |
| 5-4 | **Protect privacy-related data of customers and personnel in accordance with Postal Service privacy policy** – Ensure that any privacy data that is used for design/development purposes or created in production environment is secured when it is not in use or is used only by those with a need to know that information. When information is no longer needed, ensure that hard copies are shredded and electronic copies are eradicated using zero bit formatting or another acceptable eradication procedure. |
| 6-3 | **Implement appropriate hiring procedures** – Postal Service hiring procedures must be followed for FTE and well as for contractor support personnel. |
| 8-5 | **Implement change/version control and configuration management** – All applications, whether developed in-house, outsourced, or acquired must be developed following rigorous change control, version control, and configuration management procedures to reduce the risks introduced by undocumented and untested changes (see Postal Service CCM process for further information). |
| 8-6 | **Develop and maintain Standard Operating Procedures (SOPs)** – SOPs support the confidentiality, integrity, and availability of an application by ensuring that roles, responsibilities, and security processes are clearly defined. |
| 8-14 | **Utilize formal system development methodology (SDM) for application development** – Sensitive, critical, and business-controlled application development must utilize a formal system development methodology. Security must be addressed throughout the application life cycle process, and must include risk management, quality assurance, configuration management and change control, separation of duties, and testing. |

| REQ No. | Security Requirement |
|---|---|
| 9-13 | **Integrate security into the capacity planning process** – Capability planning and scalability must be considered for the application, the hosting information resource, and network connections. Whenever technically feasible, scalable applications and information resources should be considered that require little or no change to the configuration or the application when adding additional hardware or data storage. |
| 10-8 | **Submit new COTS software for approval through Enterprise Architecture Committee (EAC)** – COTS software must be acquired and distributed from a Postal Service approved source. The EAC approves software for use within the Postal Service computing environment. |
| 10-9 | **Implement eCommerce requirements when processing financial transactions** – Financial security requirements must be implemented when processing eCommerce financial transactions. (These requirements are set by the dominant financial institutions.) |
| 11-1 | **Implement remote access security** – All information resources must implement remote access security. Personnel outside the Postal Service firewalls must authenticate at the perimeter and use an encrypted session (such as VPN or SSL) if transmitting sensitive or business-controlled sensitive information. Remote access should have strong authentication on application or network connections. |
| 11-4 | **Submit network connectivity requests** – The Network Connectivity Review Board (NCRB) must approve, in advance, the establishment of network connectivity to an information resource. Any connectivity to the Postal Service network must allow monitoring. |