



# Business Impact Assessment (BIA) Questionnaire

APPLICATION NAME: \_\_\_\_\_

EIR NUMBER: \_\_\_\_\_

APPLICATION FINANCE  
NUMBER: \_\_\_\_\_

SENSITIVITY: \_\_\_\_\_

CRITICALITY: \_\_\_\_\_

DATE: \_\_\_\_\_

## TABLE OF CONTENTS

1	PROJECT IDENTIFICATION .....	1
2	PRIVACY COMPLIANCE .....	2
3	GENERAL DATA ATTRIBUTES .....	8
4	DETERMINATION OF SENSITIVITY .....	10
5	DETERMINATION OF CRITICALITY .....	12
6	DETERMINATION OF RECOVERY TIME OBJECTIVE (RTO) .....	14
7	GENERAL APPLICATION DATA .....	16
8	DECLARATION OF INFORMATION SECURITY REQUIREMENTS .....	17

April 28, 2004

# 1 PROJECT IDENTIFICATION

<b>IDENTIFICATION INFORMATION</b>			
<b>PROGRAM OR APPLICATION NAME:</b>			
<b>APPLICATION FINANCE No:</b>		<b>EIR NUMBER:</b>	
<b>CONTACT INFORMATION FOR SOLE OR DEVELOPING ORGANIZATION</b>			
<b>Functional Vice President:</b>		<b>Other:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>Executive Sponsor:</b>		<b>Executive Sponsor Designee:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>Portfolio Manager:</b>		<b>Portfolio Manager Designee:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>Program Manager:</b>		<b>Project Manager:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>ISSO:</b>		<b>ISSR:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>Privacy Office Designee:</b>			
Telephone Number:			
Email Address:			
<b>CONTACT INFORMATION FOR RECEIVING ORGANIZATION (if applicable)</b>			
<b>Vice President:</b>		<b>Other:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>Executive Sponsor:</b>		<b>Executive Sponsor Designee:</b>	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
<b>DEVELOPMENT AND PRODUCTION INFORMATION</b>			
<b>Development Organization:</b>			
<b>Development Site:</b>			
<b>Production Site(s):</b>			
<b>Brief Description of Business Function</b> (include purpose and key business functions):			

## 2 PRIVACY COMPLIANCE

The purpose of this section of the questionnaire is to ensure compliance with privacy requirements, including applicable laws and USPS policy. Questions or comments regarding this section 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 or customer information that the USPS or its supplier maintains 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, such as how data is collected, managed, and disclosed, 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, 3-3.)

<b>a.</b>	<b>Does the program or application collect or store information related to a customer or employee where data is retrieved by name, unique number, symbol, or other identifier assigned to the customer or employee?</b>
<input type="checkbox"/>	No (skip to 2-6.)
<input type="checkbox"/>	Yes (Privacy Act system of records (SOR) is required.)
<b>b.</b>	<b>Does an existing Privacy Act system of records (SOR) apply?</b>
<input type="checkbox"/>	No (skip to 'e' and contact Privacy Office to develop new SOR.)
<input type="checkbox"/>	Yes (provide name of SOR): _____ (For assistance, contact Privacy Office.)
<b>c.</b>	<b>Does the existing SOR need to be modified?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes (skip to 'e' and contact Privacy Office.)
<b>d.</b>	<b>Have you read, and will the application comply with, all data management practices in the SOR?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<b>e.</b>	<b>When is the application expected to be operational?</b>
	(mm/dd/yyyy)
<b>f.</b>	<b>What is the data retention period for the application?</b>
	(specify):
	<b>What is the process for purging records at the end of that period?</b>
	(specify):
<b>g.</b>	<b>Will the application meet all of the following? (Check all applicable boxes.)</b>
<input type="checkbox"/>	Information is processed and maintained only for the purposes for which it was collected.
<input type="checkbox"/>	Information is reliable for its intended use.
<input type="checkbox"/>	Information is accurate.
<input type="checkbox"/>	Information is complete.
<input type="checkbox"/>	Information is current.

<b>h.</b>	<b>Will the application collect only the minimum information required for functional operation?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes

## 2-2 NOTICE

The Privacy Act of 1974 and USPS policy requires a privacy notice to be provided to the customer or employee when information is collected directly from them. A privacy notice describes the purpose of collection and data protections that apply to the information. (See HBK AS-353, 3-2.)

<b>a.</b>	<b>Is information collected from a customer or employee that can be used to identify them?</b>
<input type="checkbox"/>	No (skip to 2-3.)
<input type="checkbox"/>	Yes (privacy notice is required.)
<b>b.</b>	<b>Check all sources from which information will be collected.</b>
<input type="checkbox"/>	Employees (including applicants)
<input type="checkbox"/>	Individual customers
<input type="checkbox"/>	Business customers
<b>c.</b>	<b>Check all channels/methods that will be used to collect information.</b>
<input type="checkbox"/>	In-person <input type="checkbox"/> verbal <input type="checkbox"/> hard-copy form <input type="checkbox"/> telephone <input type="checkbox"/> fax <input type="checkbox"/> e-mail <input type="checkbox"/> online
<b>d.</b>	<b>If information is collected online from a customer (either individual or business), is there a link to the usps.com privacy policy on each page of the application?</b>
<input type="checkbox"/>	Not applicable, as information will not be collected online from individual or business customers.
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<b>e.</b>	<b>If information is collected online from an employee, how is a privacy notice provided?</b>
<input type="checkbox"/>	Not applicable, as information will not be collected online from employees.
<input type="checkbox"/>	Notice is available on the screen near where data is collected.
<input type="checkbox"/>	Via link
<input type="checkbox"/>	Other (specify):
<b>f.</b>	<b>If information is collected from an individual customer other than from usps.com, or from an employee by any channel, does the privacy notice include the following elements? (Check all applicable boxes.)</b>
<input type="checkbox"/>	Not applicable, as information will not be so collected.
<input type="checkbox"/>	1. Proximity and Timing: the notice is provided at the time and point of data collection.
<input type="checkbox"/>	2. Purpose: describes the principal purpose(s) for which the information will be used.
<input type="checkbox"/>	3. Authority: specifies the legal authority that allows the information to be collected.
<input type="checkbox"/>	4. Conditions: specifies if providing information is voluntary, and effects, if any, of not providing it.
<input type="checkbox"/>	5. Disclosures: specifies routine use(s) that may be made of the information.
<b>g.</b>	<b>If information is collected from a business customer by fax, email, form, or mail, how is a privacy notice provided?</b>
<input type="checkbox"/>	Not applicable, as information will not be so collected.
<input type="checkbox"/>	Via statement on the document, e.g., "See our privacy policy on usps.com." or "For information regarding our privacy policies visit us at usps.com."

<input type="checkbox"/>	Other (specify):
--------------------------	------------------

## 2-3 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. Customers must be given a choice as to whether their information may be used for a secondary marketing use, such as to up-sell or cross-sell to the customer, or to share the customer's information with third parties for marketing purposes. Answer 'a' through 'c' if the application collects or manages customer information; answer 'd' if it collects or manages employee information. (See HBK AS-353, 3-2.3.)

<b>a.</b>	<b>Do you intend to use customer information for a secondary use?</b>
<input type="checkbox"/>	No (skip to 2-4.)
<input type="checkbox"/>	Yes
<b>b.</b>	<b>If information is collected from an individual customer, they must provide express consent for any secondary use of their information (opt-in). How will the application provide a mechanism for opt-in?</b>
<input type="checkbox"/>	Not applicable, as information will not be collected from individual customers.
<input type="checkbox"/>	Application will use usps.com registration.
<input type="checkbox"/>	Application will use other method (explain):
<b>c.</b>	<b>If information is collected from a business customer, they must take an affirmative step to prevent any secondary use of their information (opt-out). How will the application provide a mechanism for opt-out?</b>
<input type="checkbox"/>	Not applicable, as information will not be collected from business customers.
<input type="checkbox"/>	Application will use usps.com registration.
<input type="checkbox"/>	Application will use other method (explain):
<b>d.</b>	<b>Do you intend to use employee information for a secondary use?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes (contact Privacy Office to determine if amendment to applicable Privacy Act SOR is needed).

## 2-4 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.)

<b>a.</b>	<b>How does the application provide customers or employees with instructions for accessing or amending data related to them that is maintained by the USPS? (Check all applicable boxes.)</b>
<input type="checkbox"/>	The application will provide a link that leads to their information.
<input type="checkbox"/>	The application will provide, via link or where data is collected, written instructions on how to access/amend their information.
<input type="checkbox"/>	The application will provide a phone number of a USPS representative who will provide instructions.
<input type="checkbox"/>	The application will use other method (explain):

--	--

## 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.)

<b>a.</b>	<b>How does the application enable customers to submit questions or inquiries about USPS privacy policies or use of their data?</b>
<input type="checkbox"/>	Not applicable, as information will not be collected from customers.
<input type="checkbox"/>	The application will provide a link or reference to usps.com privacy policy.
<input type="checkbox"/>	The application will use 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, 3-8.)

<b>a.</b>	<b>Are contractors or business partners employed regarding the application?</b>
<input type="checkbox"/>	No (skip to 2-7.)
<input type="checkbox"/>	Yes
<b>b.</b>	<b>Do contractors/partners have access to customer or employee information?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<b>c.</b>	<b>Do contractors/partners help design, build, or operate a customer-facing web site?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<b>d.</b>	<b>If yes was checked for 'b' or 'c' above, list all contractors and partners below, and contact Privacy Office or Law Department to coordinate with Supply Management to ensure inclusion of appropriate privacy and confidentiality clauses in contract.</b>

## 2-7 ONLINE AND OTHER TECHNOLOGIES - Customer Systems

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

<b>a.</b>	<b>Does the application collect any information relating to customer behavior?</b>
<input type="checkbox"/>	No (skip to 2-8.)
<input type="checkbox"/>	Yes (describe):

<b>b.</b>	<b>What channel(s) does the application use? (Check all applicable boxes.)</b>
<input type="checkbox"/>	The application operates entirely on blue.usps.gov. (skip to 2-8.)
<input type="checkbox"/>	Offline only (skip to 'g.')
<input type="checkbox"/>	Online only
<input type="checkbox"/>	Both Offline and Online
<b>c.</b>	<b>Does the application operate on usps.com?</b>
<input type="checkbox"/>	No (provide url):
<input type="checkbox"/>	Yes (provide url on usps.com):
<b>d.</b>	<b>If online, will the application use web analysis tools in any way that exceeds the limits of the usps.com privacy policy? See the usps.com privacy policy for authorized uses of web analysis tools. For example, persistent cookies, web beacons, and other tools (except for session cookies) must be specifically authorized by the policy and CPO.</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes (describe):
<b>e.</b>	<b>Will the application include links to any type of external site(s)?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<input type="checkbox"/>	If yes, check box if links comply with the usps.com privacy policy relating to links.
<b>f.</b>	<b>Will the application include any type of ad banners?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<input type="checkbox"/>	If yes, check box if banners comply with usps.com privacy policy relating to banners.
<b>g.</b>	<b>If offline, will the application use any technology to identify or track customers?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	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 banking activities or functions; 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, 2-2.4.)

<b>a.</b>	<b>Does the application provide a financial service?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	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, 2-2.5.)

<b>a.</b>	<b>Does the application operate online?</b>
<input type="checkbox"/>	No (skip to 2-10.)
<input type="checkbox"/>	Yes
<b>b.</b>	<b>Does the application obtain age information or birth dates?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<b>c.</b>	<b>Do you know, or have reason to expect, that the application will collect information from children under the age of 13?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes
<b>d.</b>	<b>If yes was checked for 'b' or 'c' above, have you read, and will the application comply with, the usps.com privacy policy related to collecting information from children?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes

## 2-10 PRIVACY RISKS

In accordance with the Privacy Act, the 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, 2-2.)

<b>a.</b>	<b>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?</b>
<input type="checkbox"/>	No (skip to section 3.)
<input type="checkbox"/>	Yes
<b>b.</b>	<b>Have you considered or has the application been reviewed for any possible privacy risks or impacts?</b>
<input type="checkbox"/>	No (skip to section 3.)
<input type="checkbox"/>	Yes
<b>c.</b>	<b>Has the review identified any privacy risks and/or impacts related to the application?</b>
<input type="checkbox"/>	No (skip to section 3.)
<input type="checkbox"/>	Yes (describe):
<b>d.</b>	<b>Have efforts been made to mitigate privacy risks and/or impacts related to the application?</b>
<input type="checkbox"/>	No
<input type="checkbox"/>	Yes (describe):

### 3 GENERAL DATA ATTRIBUTES

This section will be used later in the Information Security Assurance (ISA) process to assess the adequacy of security controls that are implemented to protect the application.

#### 3-1 Data Types

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

<input type="checkbox"/> Customer (external, non-vendor customer as defined by Section 2, <i>Privacy Compliance</i> )
<input type="checkbox"/> USPS Employee
<input type="checkbox"/> USPS Employment Applicant
<input type="checkbox"/> Supplier or Business Partner
<input type="checkbox"/> Other (specify):

#### 3-2 Data Sources

Please check all the data sources that apply.

DATA SOURCES
<input type="checkbox"/> Customer (external, non-vendor customer)
<input type="checkbox"/> USPS Employee
<input type="checkbox"/> USPS Employment Applicant
<input type="checkbox"/> Supplier or Business Partner
<input type="checkbox"/> Other USPS Data Source
<input type="checkbox"/> Other Government Data Source
<input type="checkbox"/> Consumer Reporting Agency
<input type="checkbox"/> Law Enforcement Agency
<input type="checkbox"/> Commercial source or database (specify):
<input type="checkbox"/> Other (specify):

#### 3-3 Data Access

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

DATA ACCESS
<input type="checkbox"/> Customer (external, non-vendor customer)
<input type="checkbox"/> USPS Employees
<input type="checkbox"/> USPS Managers
<input type="checkbox"/> Supplier or Business Partner
<input type="checkbox"/> 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).

<b>DATA SHARING</b>	
<input type="checkbox"/>	Customer (external, non-vendor customer)
<input type="checkbox"/>	Supplier, Business Partner, or other business entity
<input type="checkbox"/>	Other government agency(s) (federal, state, or local) (specify):
<input type="checkbox"/>	Law Enforcement Agency (specify):
<input type="checkbox"/>	Other (specify):
<input type="checkbox"/>	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			
<input type="checkbox"/> Full Social Security Number	<input type="checkbox"/> Fingerprints	<input type="checkbox"/> Biometric Data	<input type="checkbox"/> USPS Personnel Records
<input type="checkbox"/> USPS Applicant or Employee Medical Information	<input type="checkbox"/> Information compiled for law enforcement purposes	<input type="checkbox"/> Change of Address with court ordered non-disclosure	<input type="checkbox"/> Other:

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

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

Nonsensitive			
<input type="checkbox"/> Name	<input type="checkbox"/> City, State, and ZIP (Home or Work)	<input type="checkbox"/> Work Street Address	<input type="checkbox"/> Work Phone Number
<input type="checkbox"/> Work Fax Number	<input type="checkbox"/> Work Cell Number	<input type="checkbox"/> Work Pager Number	<input type="checkbox"/> Work Email Address
<input type="checkbox"/> Occupation	<input type="checkbox"/> Job Description	<input type="checkbox"/> USPS Salary	<input type="checkbox"/> Professional Affiliations
<input type="checkbox"/> ICQ/Chat Address	<input type="checkbox"/> IP Address	<input type="checkbox"/> Gender	<input type="checkbox"/> USPS Employee ID Number
<input type="checkbox"/> USPS Employee Title (position)	<input type="checkbox"/> Other:		

### 4-1.2 BUSINESS DATA

Sensitive			
<input type="checkbox"/> National Security Related Information	<input type="checkbox"/> Communications Protected by Legal Privileges <sup>1</sup>	<input type="checkbox"/> USPS Restricted Financial/Trade Secrets/Proprietary	<input type="checkbox"/> Other:

Business-Controlled Sensitivity		
<input type="checkbox"/> Not Publicly Available USPS Documents (withholdable under FOIA)	<input type="checkbox"/> Not Publicly Available Information from Business Partners	<input type="checkbox"/> Other

Non-Sensitive		
<input type="checkbox"/> Publicly Available USPS Information	<input type="checkbox"/> Publicly Available Information from Business Partners	<input type="checkbox"/> Other:

### 4-2 Impact of Unauthorized Use

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

<input type="checkbox"/> Nonsensitive	<input type="checkbox"/> Business-Controlled Sensitivity	<input type="checkbox"/> Sensitive
---------------------------------------	--	------------------------------------

<sup>1</sup> Such as the deliberate process privilege, attorney-client privilege, and attorney work product doctrine.

## 5 DETERMINATION OF CRITICALITY

### 5-1 Critical Impact of Application Unavailability Determination

Check the box for each of the items below that best reflects the impact to the Postal Service if the application were to become unavailable.

<b>1. CUSTOMER OR EMPLOYEE HEALTH AND SAFETY</b> (Negative impact on life, safety, or health.)		
<input type="checkbox"/>	Little or no relationship to customer or employee life, safety, or health.	NC
<input type="checkbox"/>	Would result in a negative impact on customer or employee life, safety, or health.	C
<b>2. MOVEMENT OF THE MAIL</b> (Negative impact on customer or mail service.)		
<input type="checkbox"/>	Little or no negative impact to customer or mail service. May result in inconvenience to customers but would have an inconsequential impact on customers or core business activities.	NC
<input type="checkbox"/>	Would have a moderate negative impact on customers or impedes the movement of the mail.	BCC
<input type="checkbox"/>	Would have a significant negative impact on customers or halts the movement of the mail.	C
<b>3. FINANCIAL IMPACT</b> (Negative impact on cash flow; e.g., not able to take advantage of significant discounts or loss of incoming cash including revenue denied due to loss of business or market share.)		
<input type="checkbox"/>	Little or no impact. May result in an inconvenience but would have a trivial impact on USPS financial activities related to cash flow.	NC
<input type="checkbox"/>	Would have a moderate negative impact on USPS financial activities related to cash flow.	BCC
<input type="checkbox"/>	Would have a significant negative impact or prevent USPS financial activities related to cash flow.	C
<b>1. PROVIDES REQUIRED CRITICAL INPUT FOR A CRITICAL APPLICATION</b> (Input must be both required and critical; i.e., it CANNOT function without the input.)		
<input type="checkbox"/>	Provides no required input which is critical for the continued operation of a critical or business-controlled criticality application.	NC
<input type="checkbox"/>	Provides required input which is critical for the continued operation of a <u>business-controlled criticality</u> application and there are no other alternatives available.	BCC
<input type="checkbox"/>	Provides required input which is critical for the continued operation of a <u>critical</u> application and there are no other alternatives available.	C
<b>5. PUBLIC CONFIDENCE, BRAND, OR IMAGE</b> (Loss of customers, reduced competitiveness, or delay of new ventures and services.)		
<input type="checkbox"/>	May result in a minimal or temporary negative impact on public confidence, brand, or image.	NC
<input type="checkbox"/>	Would result in a substantial or enduring negative impact on public confidence, brand, or image.	BCC

<b>6. ADDITIONAL EXPENSE RESULTING FROM CONDUCTING BUSINESS MANUALLY, OTHER LABOR-RELATED COSTS</b> (Such as overtime, penalties, or legal liabilities.)		
<input type="checkbox"/>	Would result in less than substantial additional expense or penalties. May result in additional costs, but substantial additional expense and penalties would not be incurred.	NC
<input type="checkbox"/>	Would result in substantial additional expenses, increased costs, or penalties.	BCC
<b>7. FRAUD OR THEFT RESULTING FROM THE DIVERSION (OR CONCEALING) OF GOODS OR FUNDS BY INTERNAL OR EXTERNAL ENTITIES</b> (Such as loss of a surveillance camera.)		
<input type="checkbox"/>	Would result in less than substantial potential for fraud or diversion of goods. May result in a minor opportunity for fraud or diversion of goods.	NC
<input type="checkbox"/>	Would result in substantial potential for fraud or diversion of goods.	BCC
<b>8. AVAILABILITY DETERMINED BY REGULATORY REQUIREMENTS, CONTRACTUAL REQUIREMENTS, OR USPS STANDARDS</b>		
<input type="checkbox"/>	Would result in less than substantial violation of regulatory or contractual requirements, or USPS standards. Requirements or standards may be non-existent or subject to exemption.	NC
<input type="checkbox"/>	Would result in substantial violation of regulatory or contractual requirements, or USPS standards.	BCC
<b>9. AVAILABILITY AFFECTS REAL-TIME DECISION MAKING</b>		
<input type="checkbox"/>	Would result in less than substantial negative impact on real-time decision making. Application provides no or little information for real-time decision making or there are alternatives available.	NC
<input type="checkbox"/>	Would result in substantial negative impact on real-time decision making and there are no other alternatives available.	BCC

## 5-2 Criticality Determination Summary

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

<input type="checkbox"/> Noncritical	<input type="checkbox"/> Business-Controlled Criticality	<input type="checkbox"/> Critical
--------------------------------------	--	-----------------------------------

## 5-3 Relationship of Criticality and RTO

The level of criticality should be appropriately reflected in the RTO. If there is a significant mismatch between the criticality designation and RTO, the criticality designation and RTO should be reviewed.

**Note:** If the application is designated as critical or business-controlled criticality, continue with Section 6, *Determination of Recovery Time Objective (RTO)*. Otherwise, go directly to Section 7, *General Application Data*.

## 6 DETERMINATION OF RECOVERY TIME OBJECTIVE (RTO)

Completion of this section of the BIA is only required for applications designated as **critical or business-controlled criticality**. This section provides a process for determining an appropriate recovery time objective (RTO) for an application. RTO is defined as the maximum length of time an application can be unavailable before the Postal Service begins to experience significant operational or business services losses.

IMPACT DEFINITIONS		
<b>N</b>	No or Negligible Impact	Has no or negligible impact on USPS operational or financial activities or the life, safety, or health of employees or customers.
<b>M</b>	Moderate Impact	Would have a moderate negative impact on USPS operational or financial activities or the life, safety, or health of employees or customers.
<b>H</b>	High Impact	Would have a significant negative impact on USPS operational or financial activities or the life, safety, or health of employees or customers.

### 6-1 Identification of Impacts Over Time

To calculate the RTO for your application, use the legend above and do the following:

- For each Impact Category, determine the degree of impact (N, M, or H) if the application were to become unavailable. Assume that the system becomes unavailable during your busiest processing cycle (e.g., end of quarter, holiday, etc.).
- Enter N, M, or H for each category in each time interval column.

Impact Categories	1 Hr	8 Hrs	24 Hrs	72 Hrs	1 Week	1 Month+
Affects Life, Safety or Health of Customers or Employees						
Affects Movement of the Mail (negative impact on customer or mail service)						
Affects Cash Flow (Loss of significant discounts or incoming cash)						
Affects Public Confidence, Brand, Image (Loss of customers or Reduced Competitiveness)						
Results in Significant Additional Expenses (such as overtime, penalties, liabilities, etc.)						
Fraud or Theft Resulting from Unauthorized Use or Unavailability of the Application						

- Total the number of "Moderates" and "Highs" from the above table and enter the totals in the table below.

Impact Level Totals for	1 Hr	8 Hrs	24 Hrs	72 Hrs	1 Week	1 Month +
<b>Moderate</b>						
<b>High</b>						

## 6-2 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 of the other system. 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 the 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.							

## 6-3 Recovery Time Objective Calculation

Complete Steps 1 – 6, below, to determine RTO.

Step	If you . . .	Then . . .	Time Interval	
1.	Recorded any High impacts in Section 6.1	Enter the lowest time interval for recorded Highs in the <i>Time Interval</i> column (e.g., 1 hr., 8 hrs., etc.).		
	Did not record any Highs	Skip to step 2.		
2.	Recorded any Moderates in Section 6.1	Add up the number of Moderates in each time interval. Enter the time interval with the highest frequency of Moderates in the <i>Time Interval</i> column.		
		<table border="1"> <tr> <th>If . . .</th> <th>Then . . .</th> </tr> <tr> <td>More than one time interval has the same frequency of Moderates</td> <td>Enter the time in the <i>Time Interval</i> column that best matches your estimate of RTO</td> </tr> </table>		If . . .
If . . .	Then . . .			
More than one time interval has the same frequency of Moderates	Enter the time in the <i>Time Interval</i> column that best matches your estimate of RTO			
3.	Recorded no Highs or Moderates in any category	Enter one month in the <i>Time Interval</i> column.		
4.	Recorded any dependencies and RTOs in Section 6.2	Enter the lowest RTO time interval indicated in 6.2 in the <i>Time Interval</i> column.		
5.	Recorded any time intervals in Steps 1, 2, and 4	Enter the lowest of the time intervals in the <i>Time Interval</i> column.	<b>Calculated RTO</b>	
6.	Select the RTO your organization will use to design your recovery strategy	Record the Selected RTO in the <i>Time Interval</i> column and explain briefly under Comments why you selected a higher or lower RTO than the Calculated RTO in the space below (budget, risk avoidance, etc.).	<b>Selected RTO</b>	
Comments:				

## 7 GENERAL APPLICATION DATA

### 7-1 System Description

<i>Brief System Description:</i>	
<i>Supporting Application Software:</i>	
<i>Operating System:</i>	
<i>Data or Database:</i>	
<i>Hardware:</i>	
<i>Network:</i>	
<i>Communications:</i>	
<i>Security Software:</i>	
<i>Other:</i>	
<b>Projected Production Date:</b>	

### 7-2 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.	Will the application be located in a Postal Service controlled access area?		
7.	Is a COTS product a significant feature or portion of the application?		
8.	Does the COTS product contain custom programming or scripts?		
9.	Is the application an externally-facing application containing custom programming (HTML, XML, Java, Javascript, CGI, ActiveX, etc.)?		
10.	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?		
11.	Will the information be stored in a secure location?		
12.	If stored in a secure location, is access controlled?		
13.	Could unrestricted access to hardcopy information and storage media result in the disclosure of business-controlled sensitivity information?		

14.	Could the aggregation of multiple business-controlled sensitivity information elements by unauthorized persons result in the violation of an individual's privacy or jeopardize Postal Service operations?		
15.	Could unrestricted access to computer screens result in the disclosure of business-controlled sensitivity information?		
16.	Will access to this information increase the opportunity for theft, collusion, fraud, blackmail, or prevent the timely performance of Postal Service operations?		
17.	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?		
18.	Does application contain Active Content or CGI code?		
19.	Is the data collected, stored, analyzed, or maintained by this application available in another form or from another source?		
20.	Would the unavailability of this application prevent the timely performance of Postal Service operations?		

### 7-3 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 be an externally-facing application such as an Internet accessible Web application?		
6.	Will the application require a change to a perimeter firewall configuration?		
7.	Will the application require a change to a secure enclave firewall configuration?		
8.	Will the application utilize a wireless LAN, wireless access point, or wireless devices such as PDAs?		
9.	Will the application access development, production, or internal Postal networks via the Internet or Internet connectivity?		

## 8 DECLARATION OF INFORMATION SECURITY REQUIREMENTS

### 8-1 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:		
1. Independent risk assessment?		
2. Independent code review?		
3. Independent validation of security testing?		
4. Independent penetration testing and vulnerability scans?		

## 8-2 Information Security Requirements To Be Implemented

**LEGEND:** *BAS*: Baseline, *MAN*: Mandatory, *REC*: Recommended Discretionary, *ACC*: Accepted Discretionary

REQ. NO.	INFORMATION SECURITY REQUIREMENT (HANDBOOK AS-805, INFORMATION SECURITY, OR HANDBOOK AS-805-A, APPLICATION INFORMATION SECURITY ASSURANCE PROCESS, REFERENCE)	B A S	M A N	R E C	A C C
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	Add “restricted information” to computer screen display (AS-805: 3-5.1)				
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)				
4-2	Conduct an independent risk assessment (AS-805-A: 5-2)				
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 (AS-805: 6-6.3)				
7-2	Locate application 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 sensitivity 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 (11-5.8)	X			
8-7	Include information security in service level agreements [SLA] (internal and external systems) and trading partner agreements (external systems only) (AS-805-A: 4-1.4.5)	X			
8-9	Conduct independent validation of security testing (AS-805-A: 5-4)				
8-10	Conduct independent security code review (AS-805-A: 5-1)				
8-11	Conduct independent 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)	B A S	M A N	R E C	A C C
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 or 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)				
10-1	Implement virus protection (AS-805: 10-7)	X			
10-3	Implement application on a server hardened to Postal Service standards (AS-805: 10-5.3.1)	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: 12-7.1, 12-9)				
12-4	Implement backup and recovery procedures (AS-805: 12-5)	X			
12-5	Implement off-site storage of backup media (AS-805: 12-5.5)				
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: 12-7.3); and maintain an inventory of backup media offsite (AS-805: 12-5.4)				
13-1	Report incidents in accordance with Postal Service policies (AS-805: 13-4.1)	X			
14-1	Implement authorized warning banner (AS-805: 14-5.5)	X			

## 8-3 ACCEPTANCE OF RESPONSIBILITY AND ACKNOWLEDGEMENT OF ACCOUNTABILITY

### 8-3.1 Executive Sponsor

I am responsible for funding and procuring, developing, and integrating security controls that will satisfy the information security requirements (identified above) in accordance with the ISA process outlined in Handbook AS-805-A, *Application Information Security Assurance Process*, and, if applicable, Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment*. I understand that compliance with the ISA process may affect the development time and cost of this project and must be planned for accordingly. I will ensure that Postal Service information security policies, guidelines, and procedures are followed in the development, integration, and, if applicable, the operation and maintenance of this application.

<b>Executive Sponsor</b>		
<b>COMMENTS:</b>		
<b>Executive Sponsor</b>	<b>Title</b>	<b>Date (MM/DD/YYYY)</b>

=====**Start For Exception Where an Application is Developed by One Organization**=====  
 =====**and Transferred to Another Organization**=====

### 8-3.2 Executive Sponsor Developing Application

I am responsible for funding and procuring, developing, and integrating security controls that will satisfy the information security requirements (identified above) in accordance with the ISA process outlined in Handbook AS-805-A, *Application Information Security Assurance Process*, and, if applicable, Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment*. I understand that compliance with the ISA process may affect the development time and cost of this project and must be planned for accordingly. I will ensure that Postal Service information security policies, guidelines, and procedures are followed in the development and integration of this application.

<b>Executive Sponsor (developing organization)</b>		
<b>COMMENTS:</b>		
<b>Executive Sponsor (developing organization)</b>	<b>Title</b>	<b>Date (MM/DD/YYYY)</b>

<b>SCHEDULED TRANSFER DATE:</b>
<b>Date (MM/DD/YYYY)</b>

### 8-3.3 Executive Sponsor Receiving Application

I am responsible for funding and maintaining security controls in the operating environment that will satisfy the information security requirements (identified above) in accordance with the ISA process outlined in Handbook AS-805-A, *Application Information Security Assurance Process*, and, if applicable, Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment*. I understand that compliance with the ISA process may affect the operations cost of this project and must be planned for accordingly. I will ensure that Postal Service information security policies, guidelines, and procedures are followed in the operation and maintenance of this application.

<b>Executive Sponsor (receiving organization)</b>		
<b>COMMENTS:</b>		

<b>Executive Sponsor (receiving organization)</b>	<b>Title</b>	<b>Date (MM/DD/YYYY)</b>

**=====Stop For Exception Where an Application is Developed by One  
Organization=====**  
**=====and Transferred to Another  
Organization=====**

### 8-3.4 Portfolio Manager

I am responsible for coordinating the implementation of security controls that will satisfy compliance with the ISA outlined in Handbook AS-805-A, *Application Information Security Assurance Process*, and, if applicable, Handbook AS-805-G, *Information Security for Mail Processing Equipment/Mail Handling Equipment*. I understand that compliance with the ISA process may affect the development time and cost of this project and must plan for this accordingly with the Executive Sponsor.

<b>COMMENTS:</b>	
Portfolio Manager	Date (MM/DD/YYYY)

### 8-4 Verification of Completion of the BIA

<b>COMMENTS:</b>	
ISSO	Date (MM/DD/YYYY)
Privacy Official	Date (MM/DD/YYYY)

### BIA WRAP UP

File completed BIA Questionnaire with the ISA documentation package.

Send completed copies of this document to the Chief Privacy Officer, ISA Program Manager, and the Information Security Systems Officer at the following addresses:

Chief Privacy Officer  
 US Postal Service  
 475 L'Enfant Plaza SW, Room 10407  
 Washington, DC 20260-2200

Corporate Information Security Office  
 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