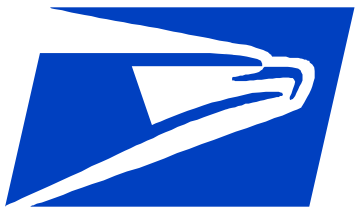

UNITED STATES POSTAL SERVICE™

Field Application

Business Impact Assessment

Version 1.64

September 16, 2005

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

TABLE OF CONTENTS

1 INTRODUCTION

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

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

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

1-1 WHAT ARE FIELD APPLICATIONS

Characteristics of field applications are as follows:

a. Field applications are not national applications.
b. Field applications are hosted on a server located in the FIS Server Farm at Eagan.
c. Field applications are classified as noncritical and can never be critical or business-controlled criticality.
d. Field applications facilitate the completion of one or more specific tasks, establish a unique session with each visitor; and allow a user to make permanent changes to stored data.
e. A field application is coherent -- it is a set of web pages designed to work together. It is focused -- the goal is completion of a specific task or set of tasks. It is user-centric -- differentiation of user input is generally critical. It is data-driven -- users (depending on level of access) can create/edit/delete stored data.
f. A field application is not static web pages, generic feedback forms, "mailto" email links, hit counters, stand-alone reports pages where the data is merely displayed and not altered, or Excel macros.

Categories of local field applications are as follows:

a. New - Local field applications being developed today. These applications must be registered in the Enterprise Information Repository (EIR) http://fcco/eir and require the completion of a Field Application Business Impact Assessment (BIA).
b. Replicated Stand Alone - Multiple copies of the same local non-web application. Requires Area Vice President approval and sponsorship. (e.g., emailed Access databases). The application must be registered in the EIR using the same application name but attaching your district number to the front of the name. No Field Application BIA is needed.

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

c. Shared Local - Web applications that are shared and can be expanded for use across districts and areas. Requires Area Vice President approval and sponsorship prior to expansion to additional areas or districts. (e.g., Mail Arrival Quality (MAQ); Plant Arrival Quality (PAQ); Leadership Skills Bank (LSB)). The application must be registered in the EIR using the same application name but attaching your district number to the front of the name. No Field Application BIA is needed.
d. National Duplicate - Local applications whose functionality is already included in a national application. Retirement of the local application requires Area Vice President approval and sponsorship. (e.g., Asset Configuration Management System (ACMS); Telephone Directory).
e. National Incorporated - Local applications whose functionality could be incorporated into an existing national application. Requires approval from the Area Vice President, Portfolio Manager and National Sponsor. (e.g., FLASH System).

f. Field Shareable - Single instance of a web application that has been identified for use across the field, sponsored by Field Information Systems (FIS), approved by the Manager of Field Customer Care Operations (FCCO) and sanctioned by the Manager of Distributed Computing Environment (DCE). Determination and final approval will be from FIS. (e.g., Web Content Administrative Tool (WebCAT); Report Engine). The application must be registered in the EIR using the same application name but attaching your district number to the front of the name. No Field Application BIA is needed.

1-2 What the Field Application BIA Applies To

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

1-3 What Field Applications Are Affected

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

1-4 Purpose

The purpose of the Field Application BIA is to determine compliance with the privacy requirements, determine sensitivity, and identify the appropriate security requirements to protect the application based on its sensitivity and criticality.

1-4.1 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 sensitivity, and nonsensitive.
- **Criticality**
  Criticality determines the need for continuous availability of the information. The levels of criticality are: critical, business-controlled criticality, and noncritical. By definition field applications are defined as noncritical.

1-4.2 Determination of Compliance with Privacy Requirements

The BIA ensures that applications 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 Field Application BIA Questionnaire.

1-4.3 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 a field application are categorized as baseline, mandatory, and requirements treated as mandatory. The security requirements will vary with the application's sensitivity designation and the responses to the questions in the Field Application 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 B, *Good Business Practices*, for a list of these requirements.

- **BASELINE**
  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 Field Application BIA Questionnaire.

- **MANDATORY**
  Mandatory security requirements are requirements that must be implemented based on the sensitivity designation of the Postal Service applications. In the automated Field Application 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 Field 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 Field 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 Field Application 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 Field 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** and **business-controlled sensitivity** applications, the appropriate controls must be implemented to satisfy the baseline security requirements and the mandatory security requirements.

1-5 WHEN TO COMPLETE THE FIELD APPLICATION BIA

Significant Change— A change that calls into question the security of an application and the accuracy of previous ISA documentation.

A Field 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.

1-6 BIA PROCESS METRICS

Following are the criteria for official classification of field 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 Business Owner and Field Information Systems Manager together.
c. The Business Owner, FIS Manager, Corporate FIS Manager, Privacy Officer and ISSO all sign BIA within 10 days.
d. After the document is signed by the Business Owner, FIS Manager, Corporate FIS Manager, Privacy Officer and ISSO, the ISSO enters the field application sensitivity and criticality designations in EIR within 48 business hours.
e. The field 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.

1-7 BENEFITS OF THE FIELD APPLICATION 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 designation.
d. Determination of application dependencies.
e. The focusing of security requirements on application sensitivity, function, and environment.
f. A risk-based approach that empowers business owners to implement controls to satisfy the discretionary requirements where the business risk justifies such practices.
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 BUSINESS OWNER

Business owners (e.g., Area Vice President, IT Manager, District Manager, or BMC Manager) have 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. Providing financial and personnel resources to complete the BIA processes.

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.

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.

2-2 FIELD INFORMATION SYSTEMS MANAGERS

Field information systems managers are responsible for the following:

a. Functioning as the liaison between business owners and the information technology providers.
b. Supporting the business owner in the completion of the BIA.

2-3 INFORMATION SYSTEMS SECURITY REPRESENTATIVES

An information systems security representative (ISSR) may be assigned by the business manager or field information systems 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 business manager or field information systems 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 business manager or field information systems managers regarding the BIA processes.
b. Facilitating the completion of the BIA.
c. Selecting appropriate discretionary security requirements.

2-5 BUSINESS OWNER DESIGNEES

Business owners may designate in writing Postal Service employees to perform security-related activities on their behalf. However, ultimate accountability and responsibility reside with the business owner.

2-6 FIELD INFORMATION SYSTEMS MANAGER DESIGNEES

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

2-7 PROGRAM MANAGERS

Field information systems managers may designate in writing program managers to perform security-related activities on their behalf in support of the business owner.

2-8 PROJECT MANAGERS

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

2-9 CHIEF PRIVACY OFFICER

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

a. Providing guidance on completing the privacy compliance section of the Field 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 version of the Field 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 Field Application 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 importance of the data collected relative to disclosure).
5 *Determination of Criticality* – documents 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 information security requirements for adequately securing the application.
8 *Acceptance of Responsibility* – documents acceptance of responsibility for implementing information security requirements for the application.
9 *Verification of Completion* – documents the ISSO who coordinated the completion of the BIA and submitted the information security requirements to the field information systems manager for implementation.

Instructions for completing each section of the Field 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 privacy official if there are any questions regarding this section. The privacy official is available to provide guidance via email or telephone.
c. The privacy official will review the completed Field Application BIA Questionnaire, and if there are issues regarding privacy compliance or the application sensitivity designation, the privacy official will contact the ISSO to get clarification or to arrange a teleconference with the business owner.

SECTION 3 GENERAL DATA ATTRIBUTES

Complete Section 3-1, *Data Types*, by describing the types of data collected.

Complete Section 3-2, *Data Sources*, by describing the sources for the data.

Complete Section 3-3, *Data Access*, by describing who has access to the data.

Complete Section 3-4, *Data Sharing*, by describing if the data is shared externally and with whom.

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 Sensitivity* portion of Section 4-1.1, *Personal Data*, the checked blocks with an asterisk will be considered business-controlled sensitivity 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 sensitivity 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 Sensitivity, 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 sensitivity. In most cases, where sensitive data elements and business-controlled sensitivity are checked, the final designation will be sensitive. In most cases, where business-controlled sensitivity and non-sensitive data elements are checked, the final designation will be business-controlled sensitivity. Exceptions require approval of the privacy official.
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 sensitivity may be considered a sensitive application due to the extent of data aggregation.
d. If there are questions, contact the privacy official 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

No action required. By definition field applications are noncritical.

SECTION 6 GENERAL APPLICATION DATA

In Section 6-1.1, *General Information*, enter the requested information.

In Section 6-1.2, *Technical Information*, enter the requested information.

In Section 6-1.3, *HCS Information*, enter the requested information.

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 security requirements and whether independent processes (risk assessment, code review, validation of security testing, and vulnerability scans) will be recommended by the ISSO.

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 are "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 in the BAS column.

The ISSO posts the mandatory security requirements in the MAN column.

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

SECTION 8 ACCEPTANCE OF RESPONSIBILITY

The business owner or designee signs and enters today's date.

The BIA should be emailed to the Corporate FIS Manager along with a scanned copy of the acceptance of responsibility signature page.

SECTION 9 VERIFICATION

The Privacy Official signs and enters today's date.

The ISSO signs, enters today's date, and sends the information security requirements to the field information systems manager.

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: Sensitive and business-controlled sensitivity applications must implement controls that will satisfy the baseline security requirements, and the checked mandatory security requirements. It is recommended that sensitive and business-controlled sensitivity applications implement controls that will satisfy the checked discretionary security requirements.

BIA WRAP UP

1. File the Field 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

RESTRICTED INFORMATION

ATTN: ISA Program Manager
475 L'Enfant Plaza SW, Room 2441
Washington, DC 20260-2441

APPENDIX A – FIELD APPLICATION BIA QUESTIONNAIRE

RESTRICTED INFORMATION

UNITED STATES POSTAL SERVICE™

Field Application Business Impact Assessment (BIA) Questionnaire

APPLICATION NAME: _____

EIR NUMBER: _____

APPLICATION FINANCE NUMBER: _____

SENSITIVITY: _____

CRITICALITY: Noncritical

DATE: _____

TABLE OF CONTENTS

Version 1.63

September 16, 2005

RESTRICTED INFORMATION

1 PROJECT IDENTIFICATION

CONTACT INFORMATION			
Area/District Manager:		**Corporate FIS Manager:**	Carole D. Koehler
Telephone Number:		Telephone Number:	(919) 501-9638
Email Address:		Email Address:	carole.d.koehler@usps.gov
FCCO Manager:	Cheryl A. Dill	**Other:**	
Telephone Number:	919-501-9404	Telephone Number:	
Email Address:	cheryl.a.dill@usps.gov	Email Address:	
ITPC Manager:		**Other:**	
Telephone Number:		Telephone Number:	
Email Address:		Email Address:	
ISSO:	Phillip R. Nicholson	**Other:**	
Telephone Number:	202-268-3589	Telephone Number:	
Email Address:	phillip.r.nicholson@usps.gov	Email Address:	
Privacy Official:	Deborah A. Kendall	**Other:**	
Telephone Number:	202-268-3323	Telephone Number:	
Email Address:	deborah a. kendall@usps.gov	Email Address:	

DEVELOPMENT AND PRODUCTION INFORMATION	
Development Organization:	
Development Site:	
Production Site(s):	
Brief Description (include purpose and key business functions)**:**	
Production Date	

2 PRIVACY COMPLIANCE

2-1	SYSTEM OF RECORDS – Data Management	Yes	No
	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?		
2-2	**NOTICE**	**Yes**	**No**
	Is information collected directly from a customer or employee?		

RESTRICTED INFORMATION

2-3	CHOICE	Yes	No
	Do you intend to use customer information 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?		
2-4	**SUPPLIERS**	**Yes**	**No**
	Are contractors or business partners: 1) employed regarding the application OR 2) helping design, build, or operate a customer-facing web site?		
2-5	**WEB SITES**	**Yes**	**No**
	Does the application include a customer-facing web site not on usps.com?		
2-6	**CHILDREN'S ONLINE PRIVACY PROTECTION ACT**	**Yes**	**No**
	If an online customer site, does it identify ages or is it directed to persons under 13?		
2-7	**GRAMM–LEACH-BLILEY ACT – Financial Services**	**Yes**	**No**
	Does the application provide a financial service? Examples include banking activities or functions; wire/monetary transfers; printing, selling, or cashing checks; providing USPS credit services. It does NOT include payment by check or credit card issued by another entity.		
2-8	**PRIVACY RISKS**	**Yes**	**No**
	Does the program or application collect or store information related to customers or employees; involve a customer web site; or use technology that can track customer behavior?		

2-9	DESCRIPTION of INFORMATION MANAGEMENT PRACTICES
	If "YES" was checked for any of the above, please provide a brief explanation for each "YES" item below.

3 GENERAL DATA ATTRIBUTES

3-1	DATA TYPES:
	What data is being collected? (customer, employee, employee applicant, supplier, business partner, product/service related, etc.)
3-2	**DATA SOURCES:**
	Who provides the data?
3-3	**DATA ACCESS:**
	Who has access to the data?
3-4	**DATA SHARING:**
	Will the data be shared externally? If so, with whom?

RESTRICTED INFORMATION

4 DETERMINATION OF SENSITIVITY

4-1 Data Element Sensitivity Designation. Check all that apply.

4-1.1 Personal Data						
	SENSITIVE					
	full Social Security number		fingerprints		info held for law enforcement purposes	
	biometric data		medical information		address change w/court ordered non-disc.	
	other					
	BUSINESS-CONTROLLED SENSITIVITY					
	home street address*		home phone number *		personal cell phone number *	
	birth date/age*		partial Social Security number *		driver's license number	
	credit card # (full or partial)		race/national origin*		change of home address*	
	other account number		marital status*		customer obtained demographic info.*	
	family information		buying habits*		externally obtained demographic info.*	
	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 & affiliations*	
	income/assets:		photographs		other:	
	**Data element with a name or personal identifier is business-controlled sensitivity.* *Data element without a name or personal identifier is nonsensitive.*					
	NONSENSITIVE					
	Name		city, state, & zip (H or W)		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 ID number		USPS empl. position (title)		other:	
4-1.2 Business Data						
	SENSITIVE					
	national security related information		communications protected by legal privileges		USPS restricted financial/trade secrets/proprietary	
	other:					
	BUSINESS-CONTROLLED SENSITIVITY					
	not publicly available USPS documents		not publicly available info from business partners		other:	
	NONSENSITIVE					
	publicly available USPS information		publicly available info 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.		
	Info has little or no potential to be used for financial gain through fraud or manipulation.	**NS**
	Info has moderate potential to be used for financial gain through fraud or manipulation.	**BCS**
	Info 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?		
	Unauthorized disclosure/misuse of info would result in little or no financial loss/negative impact to brand.	**NS**
	Unauthorized disclosure/misuse of info would result in moderate financial loss/negative impact to brand.	**BCS**
	Unauthorized disclosure/misuse of info would result in significant financial loss/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 individual.	**NS**
	Results in moderate harm, embarrassment, inconvenience, or unfairness to individual.	**BCS**
	Results in significant harm, embarrassment, inconvenience, or unfairness to individual.	**S**

RESTRICTED INFORMATION

4-3 SENSITIVITY DETERMINATION SUMMARY					
Based on the responses and type of info being collected, the application is designated as (check one):					
	Nonsensitive		**Business-Controlled Sensitivity**		**Sensitive**

5 DETERMINATION OF CRITICALITY

5-1 CRITICALITY DETERMINATION SUMMARY					
By definition this application is:					
X	**Noncritical**		**Business-Controlled Criticality**		**Critical**

6 GENERAL APPLICATION DATA

6-1.1 General Information	
URL of website (if applicable)	
IP address(s)	
Hostname(s)	
Governing Office:	
Webmaster:	
Reason for Application	

6-1.2 Technical Information	
Application Software (Version & Service Pack)	
Operating System (Version & Service Pack)	
HTTP Server Software (Type & Version)	
Database (Type & Version)	
Dynamic HTML? (Type & Version)	
Remote Management?	
508 Compliant?	
External links, Ad Banners?	
Login/Password required?	

6-2 Development and Deployment Characteristics

	Question	Yes	No
1.	Will the application be developed offsite primarily by non-Postal Service personnel?		
2.	Is a COTS product a significant feature or portion of the application?		
3.	Does the COTS product contain custom programming or scripts?		
4.	Is the application an externally-facing application containing custom programming (HTML, XML, Java, JavaScript, CGI, ActiveX, etc.)?		
5.	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?		
6.	Could unrestricted access to hardcopy information and storage media result in the disclosure of business-controlled sensitivity information?		
7.	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?		
8.	Could unrestricted access to computer screens result in the disclosure of business-controlled sensitivity information?		
9.	Will access to this information increase the opportunity for theft, collusion, fraud, blackmail, or prevent the timely performance of Postal Service operations?		
10.	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?		
11.	Does application contain Active Content or CGI code?		
12.	Is the data collected, stored, analyzed, or maintained by this application available in another form or from another source?		

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 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?		

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:			
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 (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 sensitivity and should be protected from unauthorized access or disclosure" (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)		
4-3	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)		
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 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 (AS-805: 11-5.8)	X	

RESTRICTED INFORMATION

REQ. NO.	INFORMATION SECURITY REQUIREMENT (HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE)	BAS	MAN
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	
8-11	Conduct penetration tests and vulnerability scans (AS-805: 5-3)		
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)	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 (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)		

RESTRICTED INFORMATION

REQ. NO.	INFORMATION SECURITY REQUIREMENT (HANDBOOK AS-805, *INFORMATION SECURITY*, OR HANDBOOK AS-805-A, *APPLICATION INFORMATION SECURITY ASSURANCE PROCESS*, REFERENCE)	BAS	MAN
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	
4-2	Conduct an independent risk assessment (AS-805-A: 5-2) ☐ Requested by VP/CTO, Manager CISO, or Function VP ☐ Application will be developed offsite by non-Postal Service personnel ☐ 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) ☐ Requested by VP/CTO, Manager CISO, or Function VP ☐ Application will be publicly accessible		
8-10	Conduct independent security code review (AS-805-A: 5-1) ☐ Requested by VP/CTO, Manager CISO, or Function VP ☐ Application will be publicly accessible ☐ 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.

_____ _____

Business Owner Date (MM/DD/YYYY)

_____ _____

FIS Manager Date (MM/DD/YYYY)

_____ _____

Corporate FIS Manager 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 information security requirements to the Field Information Systems Manager for implementation.

_____ _____

ISSO Date (MM/DD/YYYY)

APPENDIX B - GOOD BUSINESS PRACTICES

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 fifteen 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.
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.

REQ No.	Security Requirement
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 sensitivity 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.