GENERAL LOCKBOX NETWORK
Invitation for Expressions of Interest

IEI ATTACHMENTS

Attachment __A___	Notice of Intention to Respond Form
Attachment __B___	Financial Institution Performance Questionnaire
Attachment __C___	Paper Check Conversion Standard Operating Procedures ((PCC SOP)
Attachment __D___	Summary Account Analysis Statement
Attachment __E___	Account Summary Information
Attachment __F___	Detailed Account Analysis Statement
Attachment __G___	Security Certification Statement
Attachment __H___	Facility Security Plan Outline
Attachment __I___	Occupant Emergency Plan Criteria
Attachment __J___	Suitability Factors
Attachment __K__	ISSO Designation Template
Attachment __L__	Related Web Sites

ATTACHMENT A

General Lockbox Network
Invitation for Expressions of Interest
Notice of Intention to Respond

This Notice of Intention to Respond serves as notice of [Financial Institution Name] intent to submit a response to the Invitation for Expressions of Interest (IEI) released by the U.S. Department of Treasury, Financial Management Service (FMS) on August 15, 2003, for the purpose of being considered for selection as a Qualified Lockbox Provider (QLP) under FMS' General Lockbox Network (GLN).

I, _____, do hereby certify that:

A. I am a duly authorized representative or officer of _____, hereinafter referred as "Financial Institution," who is authorized to submit and bind Financial Institution to the terms of this Notice and hereby do so;

B. I have read and thoroughly understand the requirements of the GLN IEI referenced above;

C. Financial Institution intends to submit a response to the IEI in accordance with the requirements specified in the IEI;

D. Financial Institution has been, or is eligible to be, designated by FMS as depositary and financial agent of the United States in accordance with 31 C.F.R. Part 202, and that Financial Institution also meets the following threshold requirements to participate in the IEI competition:

1. Financial Institution is in compliance with existing Treasury regulations and procedures concerning the handling of government financial transactions;
2. Financial Institution is not on the Federal Debarment and/or Suspension list and is not delinquent on any debts owed to the U.S. Government;
3. Financial Institution is capable of performing the required services specified in the IEI;
4. If selected as a QLP at the conclusion of the IEI competition, Financial Institution warrants that it shall provide GLN services, as required by FMS under the terms of the IEI, the Financial Institution's response to the IEI, and associated documents referenced in the IEI, including, but not limited to, the Designation and Authorization of Financial Agent Agreement and applicable Memoranda of Understanding;
5. To the extent Financial Institution presently provides services to FMS in its capacity as a depositary and financial agent of the United States:

    a. Financial Institution is not currently on probationary status with FMS, and, if placed on probationary status in the past, has addressed and resolved any deficiencies in performance identified by FMS; and

b. Financial Institution has completed and submitted to FMS all required internal and external audit information required in connection with providing such services;

6. If selected as a QLP, Financial Institution warrants that it shall address, to the satisfaction of FMS, any potential personnel or organizational conflicts of interest as between itself or any subsidiaries or contractors;
7. Financial Institution will be able to partner with other financial agents, when determined by FMS to be in the best interest of the government; and
8. Financial Institution warrants that it shall comply fully with all security requirements detailed in the GLN IEI, including, but not limited to, the requirement that all financial institution permanent employees, temporary employees (and employees of any subcontractor) performing GLN work be either U.S. citizens or lawful permanent residents.

E. Financial Institution understands the threshold requirements listed in Sec. D above are continuing requirements. Financial Institution is responsible for notifying FMS immediately if it no longer meets all threshold requirements;

F. Financial Institution hereby designates __[Name and Title]__ as its sole authorized point of contact with FMS to represent Financial Institution for the duration of the IEI selection process. This point of contact is authorized to make commitments on behalf of the Financial Institution involving and related to the IEI selection process and required GLN services. The sole point of contact may be reached at:

Name: _____
Title: _____
Business Address: _____
_____
Business Phone: _____
Business Email Address: _____
Business Fax Number: _____

G. Financial Institution submits the following information to FMS on its top ten (10) largest lockbox clients (based on transaction information). Financial Institution authorizes FMS to contact these references and to use the information collected in accordance with the established IEI past performance evaluation criteria:

(*For those Financial Institutions currently performing Federal agency lockbox work on behalf of FMS, at least four of the provided client references must be Federal agencies; for those Financial Institutions not currently performing Federal lockbox work on behalf of FMS, Financial Institution is requested to provide client references from state or local government customers or large decentralized corporations*)

1. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

2. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

3. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

4. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

5. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

6. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

7. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

8. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

9. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

10. Client Company or Agency Name: _____
Name of Contact: _____
Contact's Title: _____
Business Address: _____
_____
Business Phone: _____
Contact Email Address: _____

H. Financial Institution understands that it may elect to withdraw from the IEI competition before the date FMS selects QLPs.

This Notice was executed by the undersigned on _[Insert Date]__ in accordance with IEI, Sec. 3.1.1.

_____
Name of Financial Institution

_____
Printed Name and Title of Authorized Financial Institution Representative or Officer Submitting Notice

_____
Signature of Authorized Financial Institution Representative or Officer Submitting Notice

ATTACHMENT B

GENERAL LOCKBOX NETWORK
PERFORMANCE QUESTIONNAIRE
For Completion by Bidding Financial Institution

The following questionnaire has been prepared to obtain responses to effectively evaluate your financial institution's ability to provide lockbox services. This questionnaire must be completed and included along with your response to the 2003 Invitation for Expression of Interest (IEI) for the General Lockbox Network. Each question must be answered in the order presented herein, listing the question first and followed by the answer.

---

1. Provide a brief history of your financial institution as it relates to lockbox processing including the following:

    a Year of organization
    b. Year of initiation of lockbox processing
    c. Nature of relationships with affiliated companies or joint ventures

2. Has your financial institution ever been terminated, sanctioned or penalized for failure to perform any duty described in any agreement, Memorandum of Understanding or contract for lockbox services? If so, please provide dates and circumstances.

3. Do you subscribe to the Phoenix Hecht Quality Index report? If so, please provide your latest rating.

4. Do you send questionnaires to your customers on an annual basis to rate your financial institution's performance? If so, please provide a summary of the results from all customers.

5. Describe examples of your financial institution's commitment to innovation in lockbox services. Include the number and experience of employees dedicated to this processing, approach to check conversion/truncation, and any other significant information.

6. Discuss the overall business objectives of your financial institution with respect to general lockbox transaction processing. Comment on any present or planned areas of emphasis over the next three to five years.

7. Describe the approach to account administration, e.g., account team, client account executives, support by administrative units. Elaborate on the support staff, size of the staff, and hours of availability.

8. Provide the number of commercial and government accounts for which your financial institution provides lockbox services, and the volume of transactions processed by your financial institution. How have these volumes changed over the last three years?

9. Discuss services currently provided to commercial or Federal government clients similar to those required in this IEI. A brief description of current deposit reporting services, customer service capabilities, and response and down time statistics with existing services must be included.

10. Briefly describe what distinguishes your financial institution from competitors.

GENERAL LOCKBOX NETWORK

Certification Page

PERFORMANCE QUESTIONNAIRE

For Completion by Bidding Financial Institutions

This questionnaire is submitted by [Financial Institution Name] to FMS in response to the 2003 Invitation for Expression of Interest in the General Lockbox Network.

The undersigned, on behalf of [Financial Institution Name] agrees/certifies:

1. That all factual statements made in the attached response are true and correct;
2. To provide General Lockbox services set out in the Invitation's Technical Requirements in accordance with this IEI,
3. To accept terms and conditions as outlined in the Invitation's Designation and Authorization of Financial Agent (DFA); and
4. That the undersigned possesses authority to make these representations on behalf of the undersigned's financial institution.

Name: _____

Title: _____

Financial Institution: _____

Date: _____

ATTACHMENT C

United States Treasury

Financial Management Service

Paper Check Conversion

Standard Operating Procedures

and

User's Manual

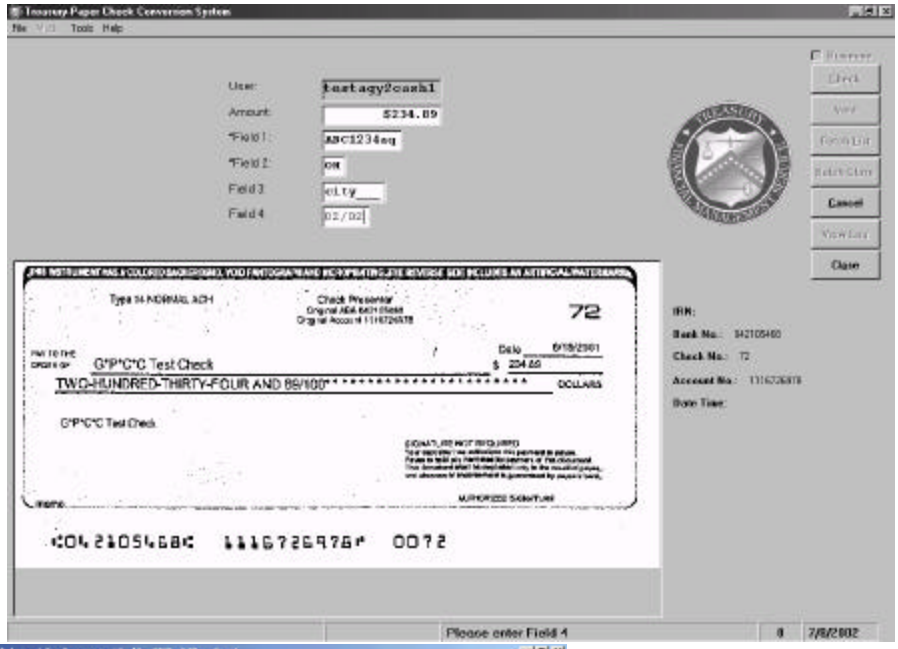
Accounts Receivable/Lockbox

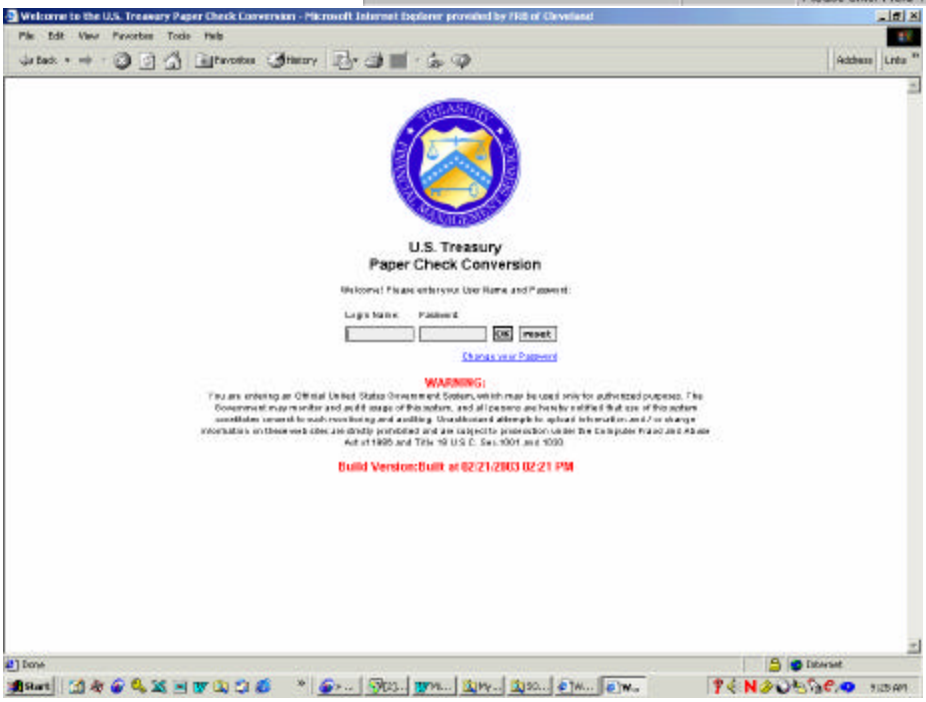
Revised May 22, 2003

United States Treasury

Check Point of Sale and

Central Image & Research Archive Installation & User Guide





Manual Contents

Section Title	Responsible Party
Installation and Configuration	System Administrator
Daily Processing Step-By-Step User Guide	System Administrator, Cashier
Central Image & Research Archive (CIRA)	System Administrator, Administration
Reporting and Balancing with CA$HLINK II	System Administrator, Cashier
Personnel Change Over	System Administrator, Cashier
Troubleshooting	System Administrator, Cashier
Appendix	System Administrator, Cashier

INTRODUCTION

What is Paper Check Conversion (PCC)?

Paper Check Conversion (PCC) is the process of converting paper checks presented to agencies into electronic ACH debits to the check writer's account. The process works as a Point of Sale (POS) when the consumer presents a physical check to the cashier for payment, or as an Accounts Receivable/Lockbox when the check is received through the mail as payment and the writer of the check is not present. The cashier takes the completed check and inserts it into the Point-of-Sale scanner that reads the MICR line on the bottom of the check and captures the image of the check into the POS computer. The check image is forwarded and stored in a central database called the Central Image and Research Archive (CIRA). When processing as a POS, the cashier returns the cancelled check to the consumer on the spot with the transaction information. The financial information captured from the MICR line is transmitted to the Federal Reserve Bank of Cleveland (FRBC). FRBC settles the transaction through the ACH network, makes CA$HLINK II entries, and provides electronic deposit ticket and debit voucher (SF215 and SF5515) reporting back to the collection site.

The PCC process involves the following major components:

Point of Sale (POS)

The software to capture and forward the image of the check and the information from the transaction is called the POS. Depending on the respective agency's needs, the POS will also collect relative payment information. The agency will determine on an overall agency basis which information is necessary. Refer to the Installation and Configuration section for setup and configuration of the POS using the PCCSAT and PCCPOS systems and setup of the POS scanner. Refer to the Daily Processing sections for POS operating instructions.

Accounts Receivable/Lockbox

Accounts Receivable/Lockbox is a processing mode that is used when checks are mailed and the writer of the check is not present. For more information, refer to the Installation and Configuration and Daily Processing sections of this manual.

Central Image and Research Archive (CIRA)

The POS application transmits all the image transaction information to Central Image and Research Archive (CIRA). The CIRA online repository of all transactions processed electronically is used to perform research on a specific item or on a group of items. The CIRA is part of the Master Verification Database (MVD), which provides the POS system information to ensure a presented check is acceptable. The CIRA can only be accessed by authorized people within the agency as well as authorized staff at the Federal Reserve Bank of Cleveland (FRBC). Refer to the CIRA section for information on accessing and researching transactions through the web site.

Settlement and Reporting

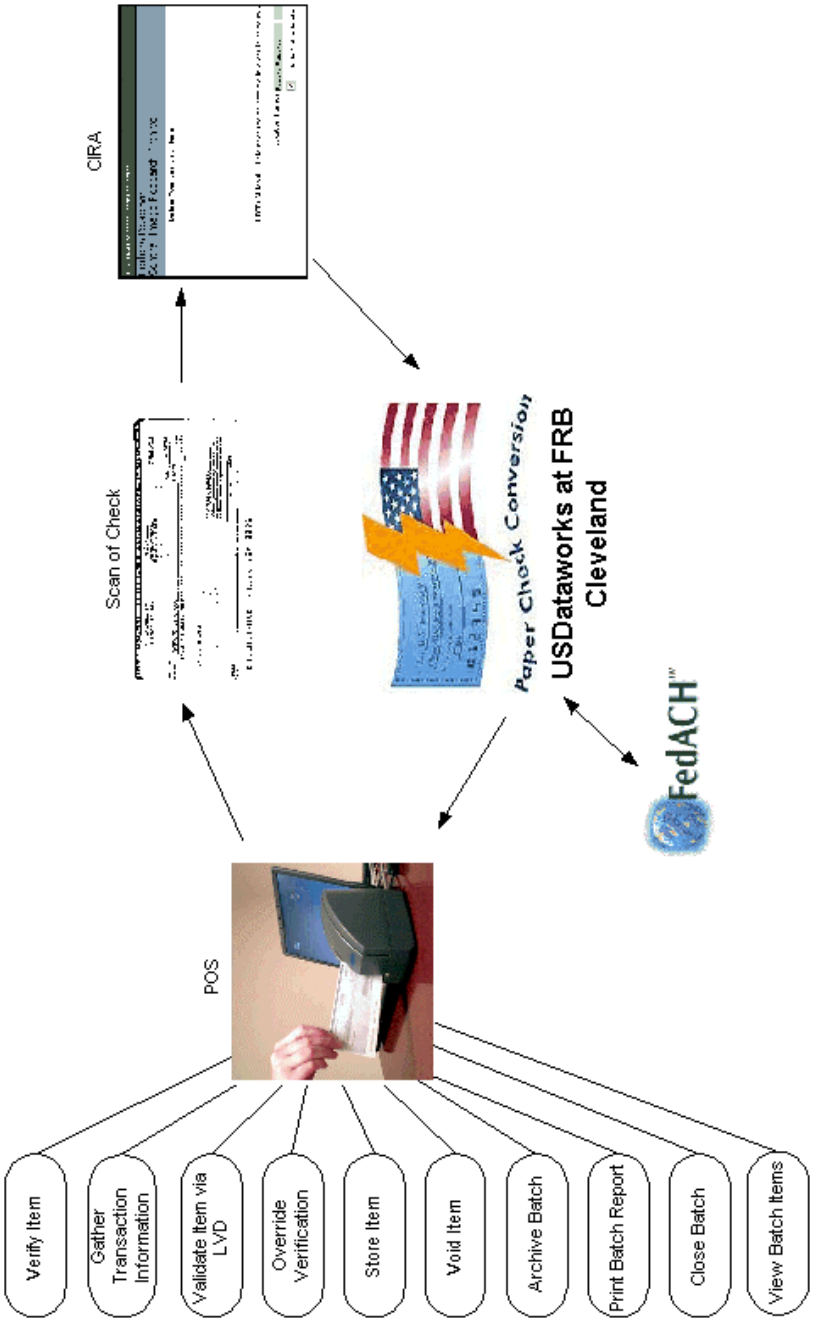
The Federal Reserve Bank of Cleveland will convert the financial information captured from each check that was forwarded to the CIRA to an electronic Automated Clearing House (ACH) item. The FedACH system is used by the Federal Reserve to settle ACH items between financial institutions. (As this system is internal to the Federal Reserve Bank, no further reference will be provided in this manual.)

CA$HLINK II

The CA$HLINK II system is used to settle and report transactions for the U.S. Government. This system will reflect deposits for all checks processed as well as debits for checks that are returned. Each day the Disbursing Officer will receive a report via email that details transactions that have posted to CA$HLINK II. Refer to the Reporting and Balancing with CA$HLINK II section for more information.

POS Diagram

The following diagram depicts the flow of transactions through the Paper Check Conversion process conducted through the POS:



ATTACHMENT D

Summary Account Analysis Statement

(Name of Site) Summary Data for Month Ending: (Date)		
Earnings Rate	0.000%	
Average Monthly Ledger Balance	$0.00	
Less average float	$0.00	
Avg Collected Balance	$0.00	
Less 10% reserves	$0.00	
Avail Bal for Earnings Credit	$0.00	
Earnings on Collected Balance After Reserve		$0.00
Service Charge Summary	$0.00	
Adjustments	$0.00	
Total Service Charges	$0.00	
Total Monthly Expenses		$0.00
Net Profit (or Loss) on Account		**$0.00**

ATTACHMENT E

Account Summary
(Name of Site)
Month Ending:
(Date)
Page: 1 of X

Account Name	DDA Number	Volume	Standard Charges	Basic Charges	Ancillary charges	Total Charges
X	X	X	$X	$X	$X	$X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
X	X	X	X	X	X	X
	TOTAL	XX	XX	XX	XX	$XX.XX

ATTACHMENT F

Detailed Account Analysis Statement
(Name of Agency)

DDA Number:
XXXXXXXXXX
Month Ending: (Date)
Page: 1 of X

Service Charge Summary

Standard Charges:	**$X.XX**
Basic Charges:	**$X.XX**
Ancillary Charges:	**$X.XX**
Total Service Charges:	**$XX.XX**

TMA Code	TMA Description	Service Type	Lockbox Number	Volume	Price Per Item	Service Charge
XX XX XX	XXXXX	Standard (S)	XXXXXX	XXX	$X.XX	$X.XX
		Basic (B)	XXXXXX	XXX	$X.XX	$X.XX
		Ancillary (A)	XXXXXX	XXX	$X.XX	$X.XX
		X	XXXXXX	X	$X.XX	$X.XX
		X	XXXXXX	XX	$X.XX	$X.XX
					TOTAL	$XXXX.XX

ATTACHMENT G

GENERAL LOCKBOX NETWORK
SECURITY CERTIFICATION STATEMENT
FOR FINANCIAL AGENTS

This security certification statement is attached in response to the 2003 Invitation for Expressions of Interest in the General Lockbox Network.

I, _____, authorized representative of _____
Name Financial Institution
hereby certify that, if _____ is selected as a QLP, it will satisfy the
Financial Institution
mandatory technical requirements specified in IEI, Section 4.0, including, but not limited to, the security requirement detailed in IEI, Section 4.10 (physical and personnel security) and Section 4.11 (information technology), within 30 days of signing the DFA.

The undersigned agrees:

1. Physical security requirements inclusive of surveillance cameras, Closed Circuit Television monitoring, digital video recording, intrusion detection systems, security guard coverage, and required access control measures have been or will be implemented.

2. Security guards are used or will be used to control access into the facility or are/will be dedicated to the general lockbox processing floor.

3. Entrances to the lockbox facility and the general lockbox processing floor are or will be controlled and monitored via camera surveillance.

4. Personnel security and background investigation requirements will be applied to all Qualified Lockbox Provider (QLP) employees and contractor employees performing general lockbox duties (i.e., have staff-like access to general lockbox processing floors, information systems, sensitive but unclassified information, and/or who in any way handle lockbox remittances and associated data), regardless of their tenure.

5. QLP employees and contractor employees will undergo background checks in accordance with the general lockbox investigative requirements prior to being granted access to remittances and associated data or within 75 days from the date of selection.

6. QLP employees and contractor employees will meet citizenship or lawful permanent resident status requirements contained in the general lockbox security requirements.

7. Personnel security files are or will be kept at the processing facility, and the results of background investigations will be adjudicated according to Suitability Factors (see IEI Attachment J), or the equivalent.

8. That the undersigned possess the authority necessary to make these representations on behalf of the QLP.

Name:_____

Authorized Signature:_____

Title:_____

Name of Financial Institution:_____

Date:_____

ATTACHMENT H

FACILITY SECURITY PLAN
Outline

1.0 Overview

- 1.1 Purpose
- 1.2 Scope
- 1.3 Assumptions
- 1.4 General Overview of the Threat
- 1.5 General Overview of Risks
- 1.6 Plan Responsibilities
  - 1.6.1 Security/Compliance Management Official
  - 1.6.2 Corporate Security
  - 1.6.3 Guard Force Manager
  - 1.6.4 Guard Force Training
  - 1.6.5 Guard Force Oversight
- 1.7 Coordination with Local Law Enforcement and Emergency Management Officials
  - 1.7.1 Law Enforcement Liaison
  - 1.7.2 FBI Liaison
  - 1.7.3 Emergency Response by Local Utilities (e.g., water, electric, telephone, power)
- 1.8 Reporting Requirements
  - 1.8.1 Local Security Incidents
  - 1.8.2 Event/Incident Reporting
  - 1.8.3 FMS Alerting Plan
- 1.9 Training Requirements
  - 1.9.1 Initial Security Awareness Training
  - 1.9.2 Annual Security Awareness Training
  - 1.9.3 Specialized Security Awareness Training (Agency Specific)

2.0 Intrusion Detection Equipment

- 2.1 System Description (including location of sensors and areas of protection)
- 2.2 Motion Sensors (type/model; location)
- 2.3 Glass Break Sensors (type/model; location)
- 2.4 Door Alarms (i.e., Door Contacts)
- 2.5 Remote Alarm Service - Local Law Enforcement Coordination and Response
- 2.6 Loss of Alarm System Coverage
- 2.7 Maintenance and Service Calls

3.0 Access Control

3.1 Access Control System

3.1.1 System Description (discussion of type of access control system, e.g., proximity card, swipe card, turnstiles in conjunction with card readers, PIN's biometrics, revolving doors, portals used in concert with card access or biometrics, etc.)

3.1.2 Alarm monitoring, panels and reports

3.1.3 Accountability and control procedures for proximity and swipe cards

3.1.4 Location of All Access Control devices (e.g., location of card readers)

3.1.5 Unauthorized Access/Unauthorized Access Attempts

3.2 Facility Access (General Population)

3.2.1 General Access Rules

3.2.2 Examination of Property

3.2.3 Removal from Premise

3.2.4 Protocol for Facility Access After Normal Business Hours

3.3 Visitor Registration, Escort and Control

3.3.1 Visitor Registration

3.3.2 Escort Authority and Responsibilities

3.3.3 Escort Procedures

3.3.4 Maintenance Personnel and Cleaning Personnel

3.3.5 Service Repairmen (e.g., electricians, plumbers,

4.0 Closed Circuit Television System Operation and Surveillance Cameras

4.1 System Description

4.2 Security of Head End and Recording Equipment

4.3 CCTV Monitoring

4.4 Loss of Camera Coverage

4.5 Maintenance and Service Calls

4.6 Size/model of CCTV Monitors

4.7 Matrix switchers

4.8 Sequential switchers

4.9 Quad Splitters

4.10 Description of exterior cameras and camera coverage (fixed and Pan/Tilt/Zoom cameras)

4.11 Description of interior cameras and camera coverage (fixed and Pan/Tilt/Zoom cameras)

5.0 Video Recording System

5.1 System Description (including type of video recorders, multiplexers, digital vs. analog, time lapse)

5.2 Security of Head End and Recording Equipment

5.3 Method used for image recording (e.g., VHS tapes, DAT tapes, CD, hard drive, etc.)

5.4 Security and Retention of Tapes

5.5 Maintenance and Service Calls

6.0 Key and Lock Control

6.1 Key Control

6.1.1 Inventory (i.e., Use of Key Register documenting the total number of keys by quantity and type)

6.1.2 Key Inventory Procedures

6.1.3 Key Sign In/Out Procedures

6.1.4 Locksmith Services

6.1.5 Responding to Lockouts

6.2 Cipher Lock operations

6.2.1 Combination Settings

6.2.2 Maintenance

6.2.3 Key Access

7.0 Guard Force Operations

7.1 General Guard Force Responsibilities

7.2 Perimeter Patrol

7.3 Operation and Use of PA (Public Address) System

7.4 Guard Post Orders (For each post in support of the LB operation)

7.5 Internal Patrol

7.6 Responding to Alarms or Incidents

7.7 Use of Force

7.8 Response to Alarms

7.9 Response to Emergencies

8.0 Courier Service and Deliveries

8.1 Courier Services

8.1.1 Schedule

8.1.2 Courier Delivery Procedures

8.1.3 Courier Pick Up Procedures

8.1.4 Courier Emergencies

8.2 Deliveries

8.2.1 Schedule(s)

8.2.2 Protocol/Delivery procedures

8.2.3 Unscheduled or Emergency Deliveries

8.3 Mail Service

8.3.1 Schedule of mail drops

8.3.2 Procedure for incoming/outgoing Express Mail

8.3.3 Procedure for incoming/outgoing Certified Mail

8.4 FedEx (Federal Express)/UPS (United Parcel Service) Deliveries

8.4.1 Schedule

8.4.1 Procedures

9.0 Emergency Actions

9.1 Overview of actions taken in emergency (i.e., life/health/safety) situations
9.2 Bomb Threat
    9.2.1 Detection
    9.2.2 Reporting
    9.2.3 Coordination with Local Law Enforcement
    9.2.4 Area or Facility Evacuation
9.3 Civil Disturbance
9.4 Medical Emergency
    9.4.1 Responding to a Medical Emergency
    9.4.2 Assistance to Local Medical Personnel
9.5 Power Outage
    9.5.1 UPS or battery back up for IDS equipment
    9.5.2 UPS or battery back up for surveillance cameras, CCTV and video recording equipment
9.6 Severe Weather
9.7 Suspicious Package and Suspected Contaminated Mail
9.8 Threats to the Facility or Personnel
9.9 Workplace Violence
9.10 Hazardous Material (HAZMAT) Response

ATTACHMENT I

OCCUPANT EMERGENCY PLAN (OEP) OUTLINE

February 4, 2003

Version 1.0, October 18, 1999

OCCUPANT EMERGENCY PLAN (OEP)

The OEP should consist of detailed procedures, supplemented by training and visual aids (placards, signs, etc), that are designed to assist occupants in dealing with emergencies within the facility, and mitigate the impact of events or incidents that may occur in the workplace.

1.0 Preparatory Actions

- 1.1 Purpose
- 1.2 Scope
- 1.3 Management Review and Approval of OEP
- 1.4 Training Requirements
- 1.5 Coordination with Local Emergency Management Agencies
  - 1.5.1 Emergency Management Response Protocol
  - 1.5.2 Law Enforcement
  - 1.5.3 Fire Department
  - 1.5.4 Hazardous Material (HAZMAT) Unit (If not within the Fire Department)
  - 1.5.5 Emergency Medical Services

2.0 Emergency Actions

- 2.1 Incident Reporting
  - 2.1.1 Internal Notifications
  - 2.1.2 Corporate Security
  - 2.1.3 Use of 911
- 2.2 Public Address System
  - 2.2.1 Routine Use
  - 2.2.2 Emergency Notification Scripts (Facility Evacuation, Section Isolation, etc.)
  - 2.2.3 Alternate Notification Schema (Runners/Signs/Telephone, etc.)
- 2.3 Facility Evacuation
  - 2.3.1 Egress Routes
  - 2.3.2 Handicapped Assistance
  - 2.3.3 Assembly Point
  - 2.3.4 Accountability and Reporting

3.0 Bomb Threat

- 3.1 Immediate Actions
- 3.2 Reporting
- 3.3 Facility Inspection
- 3.4 Law Enforcement/Fire Department liaison

4.0 Fire

- 4.1 Location and Use of Fire Alarm System
- 4.2 Location and Use of Fire Extinguishers

ATTACHMENT J

SUITABILITY FACTORS

[5CFR 731.202 (b)]

Suitability is defined as identifiable character traits and conduct sufficient to determine whether an individual is likely or not likely to be able to carry out the duties of a Federal job with appropriate integrity, efficiency, and effectiveness

SUITABILITY FACTORS	GENERAL APPLICATIONS/DISCUSSION
(1) MISCONDUCT OR NEGLIGENCE IN EMPLOYMENT,	* Misconduct involves doing something wrong in the employer's which would estimation, while negligence is the failure to do something expected by the employer. * May or may not have resulted in dismissal. If dismissed, primary emphasis should be on the act or conduct which prompted the dismissal. For military misconduct, the nature of the conduct is the governing factor, rather than the type of discharge. * Includes: poor attendance without cause, insubordination, or other suitability issues that occur in employment, such as theft, etc. * Does not include performance (i.e., an inability to perform) or other qualification issues. * Misconduct or negligence in current Federal employment is not generally included unless it is part of a pattern of conduct. (Instead, 5 CFR 315 or 752 would normally apply for post-appointment misconduct issues.)
(2) CRIMINAL or DISHONEST CONDUCT	Criminal Conduct: * Primary emphasis is on the nature of the criminal conduct, which may or may not have resulted in a conviction: details/reasons for dismissal of the offense must be considered; expungement of/pardon for an offense would not nullify the conduct, unless granted on the basis of the person's innocence. * Pending charges (of a nature that would potentially be disqualifying) cannot be adjudicated until case is disposed. Dishonest Conduct: * Dishonest conduct includes deliberate lies, fraud, or deceit for personal benefit (e.g., theft, acceptance of a bribe, falsification or records, falsification of employment documents, deliberate financial irresponsibility with continuing, valid debts of a significant nature.)
(3) MATERIAL INTENTIONAL FALSE STATEMENT or DECEPTION or FRAUD IN EXAMINATION OR APPOINTMENT	* A "Material" statement (as used in the phrase "material, intentional false statement") is one that is capable of influencing, or has a natural tendency to affect an official decision. The test of materiality does not rest on whether the agency actually relied on the statement. * A deliberate attempt to withhold information, or furnish false information, that would have a material bearing on suitability or qualifications for employment, or gain the person an advantage over other applicants, which occurs during the examination, application, or appointment process. * Material false answers to questions on appointment documents concerning one or more recent, serious criminal offenses, employment termination's, etc., or failure to admit a series of minor issues which demonstrate a pattern of misconduct, or omission of information clearly related to the position sought, such as a performance discharge from the same type of job, a conviction for drug use when applying for a job in the medical field, etc. * Falsifying qualifications needed for the job. * Impersonation/collusion, altering scores, etc.

SUITABILITY FACTORS

[5CFR 731.202 (b)]

SUITABILITY FACTORS	GENERAL APPLICATIONS/DISCUSSION
(4) REFUSAL TO FURNISH TESTIMONY as required by section 5.4	Per Civil Service Rule 5.4 (5 CFR, Part 5, Section 5.4), all competitive service applicants and employees are required to give OPM, MSPB, or the Special Counsel, or their authorized representatives, all information, testimony, documents, and material requested in regard to matters inquired of under the Civil Service laws, rules, and regulations, the disclosure of which is not otherwise prohibited by law or regulation.
(5) ALCOHOL ABUSE of a nature and duration which suggests that the applicant or appointee would be prevented from performing the duties of the position in question or would constitute a direct threat to the property or safety of others.	Current continuing abuse would ordinarily be disqualifying. Rehabilitation must be carefully considered (clear, lengthy break in pattern of abuse/strong evidence the abuse will not occur again).
(6) ILLEGAL USE OF NARCOTICS DRUGS, OR OTHER CONTROLLED SUBSTANCES, without evidence of substantial rehabilitation.	Current or recent use or possession of a serious nature would ordinarily be disqualifying. Rehabilitation claims must be clearly established. See comments for Alcohol abuse. Criminal conduct would also be an applicable factor to consider.
(7) KNOWING AND WILFUL ENGAGEMENT IN ACTS OR ACTIVITIES DESIGNED TO OVERTHROW THE U.S. GOVERNMENT BY FORCE	* Must be an overt act. * Membership in organizations, alone, is not disqualifying.
(8) Any STATUTORY or REGULATORY BAR which prevents the lawful employment of the person involved in the position in question.	Specific legal restrictions to employment.

ADDITIONAL CONSIDERATIONS

[5CFR 731.202 (c)]

ADDITIONAL CONSIDERATIONS	DISCUSSION
The Nature of the POSITION for which the person is applying or in which the person is employed.	The more authority, responsibility, sensitivity and public trust associated with the position, the higher the risks involved and the more potential adverse impact there is to the efficiency and integrity of the service; thus the misconduct becomes more serious as a potentially disqualifying issue. However, certain kinds of conduct may result in disqualification regardless of the position.
(2) The NATURE AND SERIOUSNESS of the conduct.	The more serious the conduct, the greater the potential for disqualification.
(3) The CIRCUMSTANCES surrounding the conduct.	Full facts and circumstances are essential to insure justice to the person and to protect the interests of the Government.
(4) The RECENCY of the conduct.	The more recent the conduct is, the greater the potential for disqualification.
(5) The AGE of the person at the time of the conduct.	Offenses committed as a minor are treated as less serious than those committed as an adult, unless the offense is very recent, part of a pattern, or particularly heinous.
(6) Contributing SOCIETAL CONDITIONS.	Economic and cultural conditions might be a mitigating factor if the conditions are now removed. Generally considered in cases with relatively minor issues.
(7) The absense or presence of REHABILITATION or efforts toward rehabilitation.	Clear, affirmative evidence of rehabilitation is required for a favorable adjudication. Rehabilitation is a consideration in all cases, not just those involving alcohol and drug abuse. While formal counseling or treatment may be a consideration, other factors such as the individual's employment record, etc. May also be indications of rehabilitation.

ATTACHMENT J

ATTACHMENT K

ISSO DESIGNATION TEMPLATE

APPENDIX A

ASSIGNMENT OF RESPONSIBILITY

1. **Instructions for Completing the Assignment of Responsibility**
2. **Assignment of Responsibility Memorandum Template**

Instructions for Completing the Assignment of Responsibility

Complete the Information System Security Officer assignment memorandum by filling in the names as appropriate. The signed letter shall be maintained as an attachment to the Security Plan and a copy shall be forwarded to the Financial Management Service (FMS) for their files. At any time during the life cycle of the application if the ISSO position is reassigned, a new assignment letter shall be completed and included in the Security Plan attachment, and a copy shall be forwarded to FMS.

Date:

To: <Name of Qualified Lockbox Provider ISSO Designee>

From: <Director>
Financial Services Division

Subject: [General Lockbox Network] IT System Security Officer Appointment

In accordance with the Financial Management Service (FMS) Information Technology (IT) Security Program you are being appointed as the General Lockbox Network (GLN) Security Officer.

As the GLN ISSO, you help ensure that all IT security requirements relevant to this application are implemented and maintained. Your specific responsibilities with regard to the GLN and the IT Security Program are:

- Complete and maintain the Security Plan for the application,
- Provide assistance in the scheduling of the periodic risk assessments,
- Provide assistance in the system security acceptance tests,
- Provide assistance in the completion and the maintenance of the Contingency Plan for the application,
- Provide assistance in the completion of the waiver requests when one is required, and
- Perform the procedures for managing the accounts of authorized application users, i.e., maintain a current list of authorized application users, maintain all completed system access request forms, etc.

If you have any questions concerning any of your IT security responsibilities, you should contact FMS' Financial Services Division at 202-874-6717.

Please acknowledge your understanding of your duties and responsibilities by signing below and returning a copy of this letter to me.

_____ _____

Qualified Lockbox Provider ISSO Signature Date

ATTACHMENT L

Related Web Addresses

www.fms.treas.gov	FMS Home Page
www.fms.treas.gov/cashlink	CA$HLINK II
www.fms.treas.gov/cashmanagement/frbdeposits	Deposits at FRB & TGA Depositaries
www.fms.treas.gov/eft	Electronic Funds Transfer
www.fms.treas.gov.pcn	Plastic Card Network
www.fms.treas.gov/tfm	Treasury Financial Manual
www.paygov	Pay.gov
www.pcc.gov	Paper Check Conversion
www.gpoaccess.gov/uscode/	United States Code
www.gpoaccess.gov/cfr/ or www.access.gpo.gov/nara/cfr	Code of Federal Regulations
http://csrc.nist.gov/publications/nistpubs/index.html	NIST Publications
http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf	National Information Assurance Certification and Accreditation Process
http://csrc.nist.gov/publications/nistpubs/index.html	Security Self-Assessment Guide for Information Technology Systems
www.fms.treas.gov/rebids	FMS Rebids Website