

# Update Notice

## Handbook AS-805-D, Information Security Network Connectivity Process May 2004

This online version of Handbook AS-805-D, *Information Security Network Connectivity Process*, published in May 2004, is updated through July 6, 2006, with the following *Postal Bulletin* articles:

This chapter, sub-chapter, part, or section...	titled...	was updated to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
<b>Transmittal Letter</b>				
C	Distribution	revise the link for the Postal Service Intranet.	22184	7-6-2006
D	Comments and Questions	revise the e-mail address for information security.	22184	7-6-2006
D	Comments and Questions	correct the e-mail address that has changed since the handbook was first published.	22143	12-9-2004
<b>Chapter 1, Introduction</b>				
1-4	Postal Service Standard Networked Infrastructure	add the standards and exceptions for the Postal Service network infrastructure.	22143	12-9-2004
1-5	Network Connectivity Review Board	renumber this section from 1-4 to 1-5 and all subsequent sections.	22143	12-9-2004
1-5.2	NCRB Process Overview	change steps 2, 3, 5, 6, and 8 since handbook was first published.	22143	12-9-2004
<b>Chapter 2, Roles and Responsibilities</b>				
2-1	General	update the online source for connectivity request forms.	22184	7-6-2006
2-5	Chairperson, Network Connectivity Review Board	delete subsection j.	22143	12-9-2004
2-6	Network Connectivity Review Board	correct verb in item c.	22184	7-6-2006
2-7	Executive Sponsors	add new subsection f and g and reletter all subsequent sections.	22143	12-9-2004

Information Security Network Connectivity Process

This chapter, subchapter, part, or section...	titled...	was updated to...	in <i>Postal Bulletin</i> issue number...	with an issue date of...
<b>Chapter 2, Roles and Responsibilities</b>				
2-8	Business Partners	revise item 8, instructions for getting connectivity request forms online.	22184	7-6-2006
		revise the Note about instructions for getting connectivity request forms online.	22184	7-6-2006
2.10	Information Systems Security Officers	add new section about Information Systems Security Officers.	22184	7-6-2006
<b>Chapter 3, Network Connectivity Process</b>				
3-1.1	Types of Connectivity Requiring Review by the NCRB	add new subsection j and k.	22143	12-9-2004
3-1.2	Documentation Requirements for the Connectivity Request Package	revise the instructions for getting connectivity request forms online.	22184	7-6-2006
		revise the Site Security Review row in table.	22184	7-6-2006
		add new required support documentation standard into table to include facility and inspection service approvals.	22143	12-9-2004
3-5	Approval	update approval language since the handbook was first published.	22143	12-9-2004
3-6	Scheduling/ Pre-Implementation Review	update scheduling and implementation language since the handbook was first published.	22143	12-9-2004
3-8	Confirmation	update confirmation language since the handbook was first published.	22143	12-9-2004
<b>Chapter 4, Connectivity Request Documentation Requirements</b>				
4-5	Facilities and Postal Inspection Service Approvals	add approval criteria for Facilities and Postal Inspection Service connectivity and renumbered subsequent subchapters.	22143	12-9-2004
4-7	Site Security Review	revise site security review procedures.	22184	7-6-2006
4-8	NCRB Request Form	revise title and instructions for getting connectivity request forms online.	22184	7-6-2006

## Information Security Network Connectivity Process

Handbook AS-805-D

May 2004  
Transmittal Letter

### A. Purpose

The Postal Service's Transformation Plan serves as a blueprint to the activities we are pursuing to enable us to carry out our long-standing mission of providing affordable, universal service to the people of America. It is more important than ever that each of us be aware of the latest policies, regulations, and procedures of the Postal Service whether these policies concern mail processing, delivery, or in this case information technology. Only if Postal Service employees are familiar with the policy and procedures of the Postal Service *and* the goals of the Transformation Plan can we effectively implement the Plan. This handbook sets forth the procedures for requesting connectivity to the Postal Service network infrastructure and to establish the framework for the Postal Service Network Connectivity Review Board (NCRB). The NCRB oversees the implementation of Postal Service policies and procedures related to the connection of specified Postal and non-Postal Service systems or networks to the Postal Service network infrastructure.

### B. Content

This handbook describes the following:

- The types of connectivity.
- The process for requesting connectivity.
- The associated roles and responsibilities.
- The connectivity request business case required to support a connectivity request.
- How to obtain assistance and whom to contact for further information.

### C. Distribution

This document is available on the Postal Service Intranet at  
<http://blue.usps.gov/cpim/hbkid.htm>.

**D. Comments and Questions**

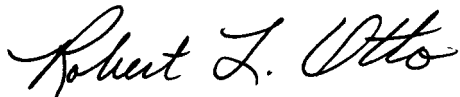
Address comments and questions to:

CORPORATE INFORMATION SECURITY OFFICE  
UNITED STATES POSTAL SERVICE  
4200 WAKE FOREST ROAD  
RALEIGH NC 27668-1510

Comments may also be sent by email to: *information\_security@usps.gov*. Use  
"AS-805-D, Network Connectivity Process" in the subject header.

**E. Effective Date**

The information in this document is effective immediately.



Robert L. Otto  
Vice President  
Chief Technology Officer

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1-1	Policy	1
1-2	What This Handbook Contains	1
1-3	Objectives of the Network Connectivity Process	1
1-4	Postal Service Standard Networked Infrastructure	2
1-5	Network Connectivity Review Board	2
1-5.1	Purpose	2
1-5.2	NCRB Process Overview	3
1-5.3	NCRB Membership	4
<b>2</b>	<b>Roles and Responsibilities</b>	<b>5</b>
2-1	General	5
2-2	Manager, Corporate Information Security Office	5
2-3	Manager, Telecommunications Services	5
2-4	Manager, IT Governance	6
2-5	Chairperson, Network Connectivity Review Board	6
2-6	Network Connectivity Review Board	7
2-7	Executive Sponsors	7
2-8	Business Partners	9
2-9	Requesters of Connectivity to Externally Facing Applications	10
2-10	Information Systems Security Officers	11
<b>3</b>	<b>Network Connectivity Process</b>	<b>13</b>
3-1	Determination of Need for Connectivity Request	13
3-1.1	Types of Connectivity Requiring Review by the NCRB	13
3-1.2	Documentation Requirements for the Connectivity Request Package	14
3-1.3	Extending the Postal Service Internal Network Into A Remote Business Partner Site	14
3-2	Request Initiation	15
3-3	Preliminary Request Evaluation	15
3-4	NCRB Evaluation	16
3-5	Approval	16
3-6	Scheduling/Pre-Implementation Review	16
3-7	Implementation	16
3-8	Confirmation	17
3-9	Escalation Procedures	17
3-10	Monitoring	17

<b>4</b>	<b>Connectivity Request Documentation Requirements</b>	<b>19</b>
4-1	General	19
4-2	Connectivity Description	19
4-3	Architectural Diagrams	19
4-4	Business Case	20
4-5	Facilities and Postal Inspection Service Approvals	21
4-6	Configuration and Enforcement Strategy	21
4-7	Site Security Review	21
4-8	NCRB Request Form	21
4-9	PS Form 3037, Telecommunications Service Request	21
<b>5</b>	<b>Contact Information</b>	<b>23</b>

# 1 Introduction

## 1-1 Policy

---

The Postal Service is committed to creating and maintaining a cost-effective information security environment to safeguard the integrity, confidentiality, and availability of Postal Service information and to protect the interests of the Postal Service, its personnel, its business partners, and the general public. This includes protecting the network infrastructure at a level commensurate to its value to the Postal Service. Such protection covers implementation of physical, administrative, and technical security controls and processes that will safeguard the network infrastructure in accordance with Postal Service policies and procedures. These controls establish standards and processes for governance of connectivity to the Postal Service network infrastructure.

## 1-2 What This Handbook Contains

---

This handbook contains the process to be used for requesting connectivity to the Postal Service network infrastructure, the associated roles and responsibilities, and the role of the Network Connectivity Review Board (NCRB). Additional policies concerning Postal Service network infrastructure are documented in Handbook AS-805, *Information Security*.

## 1-3 Objectives of the Network Connectivity Process

---

The network connectivity process is intended to do the following:

- a. Control access to Postal Service computer systems and networks.
- b. Ensure compliance with Postal Service information system security policies and procedures.
- c. Ensure compliance with Postal Service information resource and communications standards.
- d. Identify preparatory and support activities that non-Postal Service connections will require.
- e. Keep requirements for Postal Service applications and network infrastructure capabilities up to date.

- f. Provide Postal Service customers with the network security requirements to ensure the contracts are compliant with network infrastructure services.
- g. Ensure that remote Business Partner (BP) privileged usage in the demilitarized zone (DMZ) and in secure enclaves uses two-factor authentication.
- h. Ensure that unauthorized connectivity of information resources is either brought into compliance or removed.

## 1-4 Postal Service Standard Networked Infrastructure

The standard enabling networked infrastructure for the Postal Service is the Advanced Computing Environment (ACE)–approved hardware and software configurations. All non-ACE network-enabled hardware and software must be assessed and approved by the NCRB prior to connecting to the Postal Service Intranet. Exceptions are:

- a. Nonroutable mail processing equipment and mail processing infrastructure (MPE/MPI) devices that are only connected to MPE local area networks (LANs).
- b. Initiatives under portfolio management that have been through the Integrated Solutions Methodology (ISM) process.

## 1-5 Network Connectivity Review Board

### 1-5.1 **Purpose**

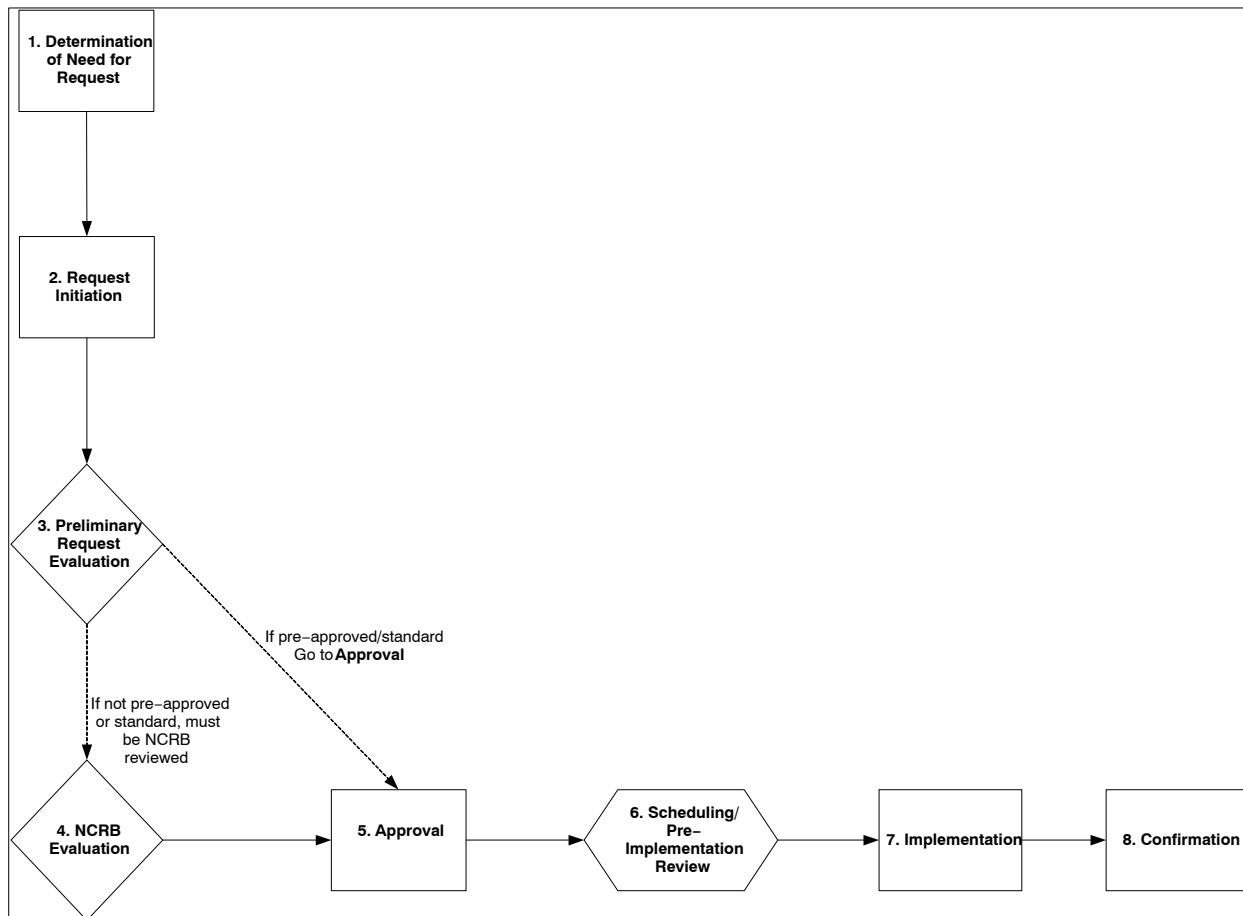
The NCRB oversees the implementation of policies and procedures relating to the connection of systems or networks to the Postal Service network infrastructure. The NCRB evaluates requests for connectivity to the Postal Service network for development, production, and internal networks in cases where connectivity requests do not comply with previously established connectivity standards. Requests that comply with the previously established connectivity standards may be sent directly to the appropriate network connectivity engineer for implementation. (See Chapter 3, Network Connectivity Process.)

The NCRB will evaluate and approve or deny any changes to Postal Service firewall configurations. No changes will be made to firewall configurations by Telecommunications Services personnel or their designees before the chairperson of the NCRB, his or her designee, or the NCRB as a whole (as applicable) has evaluated and approved the request.

**Note:** The manager, Corporate Information Security Office, is responsible for approving the configuration of all firewalls within the Postal Service infrastructure.

## 1-5.2 NCRB Process Overview

An overview of the NCRB process is presented below, followed by a short description of the steps.



### Step 1. Determination of Need for Connectivity Request

The requester and executive sponsor determine the need for connectivity to Postal Service network infrastructure.

### Step 2. Request Initiation

The requester and executive sponsor submit appropriate documentation (see section 3-1.2, Documentation Requirements for the Connectivity Package) with a requested completion date.

### Step 3. Preliminary Request Evaluation

The NCRB connectivity engineer reviews the request to ascertain feasibility, risk, and compliance; gathers all required information; performs research; and holds discussions with the requester, as required. A case number is assigned to the request. A determination will be made if the request follows pre-approved standards, or if it requires an NCRB review. If the request requires NCRB review, an e-mail is sent to the NCRB stakeholders and the requester is copied with the assigned case number and other information.

**Step 4. NCRB Evaluation**

The evaluated request is presented to the NCRB stakeholders and requesters in a decision making meeting.

**Step 5. Approval**

If approved, the requester is notified and the request is forwarded to the appropriate engineers for scheduling/pre-implementation review. If not approved, an alternative is usually suggested.

**Step 6. Scheduling Pre-Implementation Review**

The implementation engineers will review the implementation requirements of the request and schedule the change. The NCRB formally opens the change request based on the schedule for firewall updates.

**Step 7. Implementation**

The request is implemented based on the submitted change record and is completed by the appropriate group.

**Step 8. Confirmation**

A confirmation e-mail is sent to the requester notifying him or her of the completion of the request.

**1-5.3 NCRB Membership**

The NCRB consists of representatives from the Corporate Information Security Office, Telecommunications Services, and other Postal Service organizations (acting as ad-hoc experts).

# 2 Roles and Responsibilities

## 2-1 General

---

The development of policies and procedures governing protection of the Postal Service network falls under the purview of Information Technology. Roles and responsibilities associated with network connectivity are listed below. The connectivity request form is available from the NCRB Web page at <http://cto.usps.gov>; select *Support*, then *Corporate Information Security*, then under "Corporate Information Security," *Network Connectivity Review Board (NCRB)*.

## 2-2 Manager, Corporate Information Security Office

---

The manager, Corporate Information Security Office (CISO) is responsible for the following:

- a. Appointing representatives to the NCRB.
- b. Appointing the NCRB chair.
- c. Approving the configuration and management of all firewalls within the Postal Service intranet.
- d. Approving the configuration and management of all perimeter firewalls.
- e. Ensuring security controls are monitored or reviewed periodically to assure their effectiveness and reliability.

## 2-3 Manager, Telecommunications Services

---

The manager, Telecommunications Services, is responsible for the following:

- a. Appointing representatives to the NCRB.
- b. Administering all firewalls within the Postal Service network infrastructure.
- c. Managing networking devices that support the connectivity process, such as switches, load balancers, etc.
- d. Managing remote access, VPN, and dial-in connectivity.
- e. Designing and managing the Postal Service network infrastructure.

- f. Implementing NCRB-approved requests and notifying the NCRB upon implementation of the request.
- g. Ensuring that security controls are monitored or reviewed periodically to assure that they are still effective and reliable.
- h. Providing assistance regarding the design of proposed and future connectivity needs.

## 2-4 Manager, IT Governance

The manager, IT Governance, is responsible for adjudicating escalated requests for connectivity denied by the NCRB.

## 2-5 Chairperson, Network Connectivity Review Board

The chairperson, NCRB, is responsible for the following:

- a. Designating members of the NCRB other than those representing the organizations specified in section 1-5.3, NCRB Membership.
- b. Ensuring connectivity requests are submitted in the established format and in sufficient detail to be evaluated properly.
- c. Forwarding connectivity requests that require approval to the NCRB.
- d. Convening the NCRB in an appropriate and timely manner (e.g., in person or via conference calls, electronic mail, or bulletin board) as required to act on pending items.
- e. Presiding over NCRB meetings and coordinating NCRB functions.
- f. Ensuring that NCRB meetings and decisions are documented and that the minutes of the meetings are retained.
- g. Approving or rejecting requests based on NCRB analysis findings.
- h. Forwarding the approved connectivity request package to the implementation organizations, including Perimeter Security Services and the Network Protection Engineering Group.
- i. Providing technical guidance throughout the network connectivity process and closing all issues related to the connectivity request once service is installed.

## 2-6 Network Connectivity Review Board

---

The NCRB is responsible for the following:

- a. Developing system connectivity requirements for Postal Service connections to external systems, externally facing applications (e.g., FTP servers), and connections via the Internet to Postal Service development, production, and internal networks.
- b. Developing standard connectivity and documentation criteria to expedite approval of connectivity requests without additional board action.
- c. Determining the criteria for standard connectivity that will allow for requests to be pre-approved.
- d. Analyzing business cases and supporting documents for connectivity requests.
- e. Evaluating connectivity requests and approving or rejecting them based upon existing policy, best practices, and the level of risk associated with the request.
- f. Evaluating connectivity requests for Postal Service information resource secure enclave needs.
- g. Helping the requester identify alternative solutions for denied requests that are acceptable to the requester and the Postal Service.
- h. Evaluating firewall change requests and approving or rejecting them.
- i. Requesting additional information, security reviews, or audits regarding proposed or approved connections if deemed necessary.
- j. Reviewing new information resource, infrastructure, and network connections and their effects on overall Postal Service operations and information security.
- k. Recommending changes to the BP network. In situations where high risk factors exist, issuing mitigating requirements for connectivity.
- l. Ordering the disabling of an information resource or network connection that does not comply with Postal Service policies, procedures, and standards or which is found to pose a significantly greater risk than when originally assessed.

## 2-7 Executive Sponsors

---

Executive sponsors must provide appropriate funding for proposed connectivity, including BP connections. This funding includes costs associated with continued support for the life of the connection. Executive sponsors and/or assigned portfolio managers are also responsible for the following:

- a. Initiating the request for connectivity.
- b. Acting as liaison between the Postal Service and the BP requesting connectivity.

- c. Compiling the business case for BP justification (see 4-4, Business Case).
- d. Ensuring completion of a connectivity risk assessment (if required).
- e. Requesting and supporting a BP site risk assessment by the Postal Inspection Service or a designated Information Systems Security Officer (ISSO).
- f. Securing necessary approvals from the Facilities and Postal Inspection Service organizations for connecting physical access control and environmental systems to the Postal Service Intranet.
- g. Completing and submitting the appropriate NCRB documentation, including (as required) connectivity description, architectural diagrams, business case, Facilities and Postal Inspection Service approvals, configuration and enforcement strategy, site security review, and appropriate NCRB request forms.
- h. Ensuring completion and submission of a PS Form 3037, *Telecommunications Service Request*, if necessary.
- i. Coordinating with the BP and IT Telecommunication Services, Customer Care Operations, and CISO staff regarding all issues and actions necessary before establishing BP access to the Postal Service network infrastructure.
- j. Certifying that the connectivity and configuration are required and justified.
- k. Ensuring security controls are implemented to meet the information security requirements in Handbook AS-805, *Information Security*.
- l. Ensuring that the NCRB has approved any substantive configuration or procedural change before it is implemented.
- m. Obtaining the appropriate security clearances for all personnel with access to an information resource that uses the connection.
- n. Ensuring appropriate management of logon IDs.
- o. Funding two-factor authentication for privileged users under their sponsorship.
- p. Informing the NCRB of any changes affecting their sponsored connectivity.
- q. All activities performed over the requested connectivity.
- r. Ensuring prompt notification and escalation of any information security incident according to the Postal Service incident reporting process.
- s. Notifying the NCRB when the BP partner trading agreement ends or connectivity is no longer required.

## 2-8 Business Partners

---

Business partners (including alliances) are responsible for the following:

- a. Before connectivity approval:
  1. Initiating a request for access to the Postal Service network through the executive sponsor.
  2. Describing accurately the requirements for the proposed connection.
  3. Providing an architectural diagram of the connecting LAN/WAN (wide area network) showing all current and anticipated network connections.
  4. Providing configuration and enforcement strategy for the isolation of the connecting LAN.
  5. Cooperating in a connectivity risk assessment.
  6. Allowing a site security review by the Postal Inspection Service or providing an acceptable site risk assessment.
  7. Providing information required for development of the business case to the executive sponsor.
  8. Providing information to the executive sponsor as requested on the connectivity request form (available from the NCRB Web site at <http://cto.usps.gov>; select *Support*, then *Corporate Information Security*, then under "Corporate Information Security," *Network Connectivity Review Board (NCRB)*).
  9. Making required changes to the BP network to meet specific Postal Service network and information security policy requirements.
- b. After connectivity approval:
  1. Complying with all Postal Service information security policies and implementing mitigation strategies required by NCRB.
  2. Notifying the executive sponsor of connectivity completion.
  3. Informing the executive sponsor of any changes affecting the request for access or the connection.
  4. Allowing the Postal Service to have read access to all connecting LAN firewalls or similar compensating controls.
  5. Allowing the CISO staff to conduct security reviews.
  6. Allowing the Postal inspection Service or the ISSO to conduct site security reviews.
  7. Allowing the Office of the Inspector General to conduct audits.
  8. Correcting all security violations identified as a result of a Postal Service security review, audit, or information security incident within a contractually agreed-upon time period (for example, 30 calendar days after written notice has been received from the Postal Service).

9. Establishing reporting and recordkeeping procedures for all information security incidents.
10. Reporting any security incident to the Postal Service Computer Incident Response Team (CIRT) and the executive sponsor immediately and maintaining a point of contact with the CIRT.
11. Establishing change control, system maintenance, and auditing procedures that all comply with Postal Service policy.
12. Notifying the executive sponsor when connectivity is no longer required.

**Note:** The connectivity request form is available from the NCRB Web site at <http://cto.usps.gov>; select *Support*, then *Corporate Information Security*, then under “Corporate Information Security,” *Network Connectivity Review Board (NCRB)*.

## 2-9 Requesters of Connectivity to Externally Facing Applications

---

Anyone requesting connectivity to nonpublic externally facing Postal Service applications is responsible for the following:

- a. Before connectivity approval:
  1. Initiating a request for access to the Postal Service network through the executive sponsor.
  2. Describing accurately the requirements for the proposed connection.
  3. Providing an architectural diagram of the connecting LAN/WAN showing all current and anticipated network connections.
  4. Cooperating in a connectivity risk assessment.
  5. Providing information required for development of the business case to the executive sponsor.
  6. Providing information to the executive sponsor as requested on the connectivity request form.
  7. Making changes to the requester’s network to meet specific Postal Service network requirements.
  8. Ensuring appropriate management authorization for access.
- b. After connectivity approval:
  1. Complying with all Postal Service information security policies.
  2. Informing the executive sponsor of any changes affecting the request for access or the connection.
  3. Obtaining the appropriate security clearances for all personnel with access to the information resource that uses the connection.
  4. Allowing security reviews by CISO staff.

5. Allowing audits by the Office of the Inspector General.
6. Correcting all security violations identified as a result of a Postal Service security review, audit or information security incident within a contractually agreed-upon time period (for example, within 30 calendar days after written notice has been received from the Postal Service).
7. Establishing reporting and recordkeeping procedures for all information security incidents.
8. Reporting any security incident immediately to the Postal Service CIRT and the executive sponsor.
9. Establishing change control, system maintenance, and auditing procedures that comply with Postal Service policy.
10. Notifying the executive sponsor when connectivity is no longer required.

## 2-10 Information Systems Security Officers

---

Information Systems Security Officers (ISSOs) are responsible for the following:

- a. Coordinating the completion of the BIA to determine sensitivity and criticality of the information resource.
- b. Providing advice and consulting support to executive sponsors regarding the security requirements and controls necessary to protect the information resource, based on the resource's sensitivity and criticality designation.
- c. Providing guidance on potential threats and vulnerabilities to the information resource, appropriate choice of countermeasures, and the ISA process.
- d. Conducting site security reviews with the Inspection Service.

This page intentionally left blank

# 3 Network Connectivity Process

## 3-1 Determination of Need for Connectivity Request

### 3-1.1 **Types of Connectivity Requiring Review by the NCRB**

The following types of connectivity must be reviewed, evaluated, and approved by the NCRB:

- a. Connections of non-Postal Service systems or networks to the Postal Service network infrastructure, including dial-up or VPN.
- b. Nonstandard (not on the Postal network infrastructure contract) Postal-to-Postal connectivity.
- c. Connections via Internet, including Postal-to-Postal (e.g., cable or DSL).
- d. Extension of the Postal Service Intranet into a BP's remote site.
- e. Externally facing applications, such as FTP servers and Web applications.
- f. Perimeter firewall configurations and perimeter firewall change requests.
- g. Secure enclave firewall configurations and secure enclave firewall change requests.
- h. Wireless LANs, wireless access points, and wireless devices, such as PDAs.
- i. Applications accessing development, production, or internal Postal Service networks via the Internet.
- j. Non-ACE-supported infrastructure, including personally owned devices, physical access control devices such as key card devices and biometric devices, and environmental systems such as redundant power feed controllers; heating, ventilating, and air conditioning equipment; temperature and humidity controllers; fire suppression equipment; and water and sewer controllers.
- k. Any network device not managed by Telecommunications Services, IT.

### 3-1.2 Documentation Requirements for the Connectivity Request Package

Requests for network connectivity must include the documentation appropriate for the type of connectivity being requested. The documentation requirements for the types of connectivity listed below should be obtained through the executive sponsor and included in the request package. The connectivity request form is available from the NCRB Web site at <http://cto.usps.gov>; select *Support*, then *Corporate Information Security*, then under "Corporate Information Security," *Network Connectivity Review Board (NCRB)*.

Support Documentation Required with Request	Type of Connectivity Request		
	BP Requests for Leased Line Connectivity	BP Requests for VPN Connectivity	All Other Requests for Connectivity
Connectivity Description	X	X	X
Architecture Diagram	X	X	X
Business Case	X	X	X
Facility and Inspection Service Approvals	X	X	X
Configuration and Enforcement Strategy	X	X	X
Site Security Review	X	X	X
BP/MNS Access Request	X	X	X
BP Charge Back	X	X	
Secure Enclave Access Request			X
External Facing DMZ Request			X
External Facing IP Address and DNS Request			X
Pre-approved DMZ Access			X
VPN Access Request		X	If Applicable
PS Form 3037, Telecommunications Service Request	X		

### 3-1.3 Extending the Postal Service Internal Network Into A Remote Business Partner Site

BPs requesting an extension of the Postal Service internal network into a remote site must comply with the following minimum requirements:

- a. All connections to any remote BP site will be standalone (i.e., physically isolated from any other network infrastructure).
- b. All connections to any networks other than the Postal Service network infrastructure will be controlled by firewalls managed by the Postal Service.
- c. Network change control must obtain the approval of the CISO before any network changes are made for any network managed under the Postal Service network infrastructure contract.
- d. Description of the proposed connection must be provided.

- e. An architectural diagram of the connecting LAN/WAN showing all current and anticipated network connections must be provided.
- f. Configuration and enforcement strategy for the isolation of the connecting LAN must be provided.
- g. The manager, CISO (or his or her designee) must have the following:
  - 1. Unrestricted physical access to the network.
  - 2. Unrestricted network access to perform network-level intrusion detection.
  - 3. Unrestricted network access to perform network and host security vulnerability penetration testing and other network auditing functions.
- h. All equipment connected to the network infrastructure must meet current Postal Service security hardening standards.
- i. Passwords used to manage systems on the network infrastructure may not be used to manage other systems or networks. Passwords must meet the minimum password criteria designated in Handbook AS-805, *Information Security*. System administrators will use two-factor authentication.
- j. All remote site systems administrators must have an appropriate Postal Service security clearance.

## 3-2 Request Initiation

---

The requester is responsible for the following:

- a. Initiating the request through the executive sponsor.
- b. Completing the request in conjunction with the executive sponsor.

The executive sponsor is responsible for the following:

- a. Ensuring that the business need is justified, that all required documents have been provided, and that the connectivity request package is complete.
- b. Submitting the connectivity request package to the NCRB.

## 3-3 Preliminary Request Evaluation

---

The chairperson, NCRB, or his or her designee is responsible for the following:

- a. Ensuring that the connectivity request package contains the necessary documentation in the format required by the NCRB.
- b. Assigning a case number.
- c. Evaluating the request and determining whether it falls within the predetermined connectivity requirements.

- d. After making the determination, forwarding the package as follows:

<b>If . . .</b>	<b>Then . . .</b>
The request meets the standards,	The chairperson, NCRB, or his/her designee sends the package to the implementation organizations.
The request does not meet the standards,	The chairperson, NCRB, or his/her designee ensures that the request provides sufficient detail for proper evaluation and sends it to the NCRB for evaluation and approval.

### 3-4 NCRB Evaluation

---

For a connectivity request that falls outside predetermined standards, the NCRB does the following:

- a. Evaluates the request and seeks additional information, if necessary.
- b. Approves or denies the connectivity request.
- c. If the request is denied, works with the requester to identify alternative solutions acceptable to the requester and the Postal Service.
- d. Documents the decision associated with each request.

### 3-5 Approval

---

If the request is approved, the NCRB chairperson, or his or her designee notifies the executive sponsor of the decision, and the NCRB-approved connectivity request package is forwarded to the implementation organizations for scheduling/pre-implementation review.

If the request is not approved, the NCRB chairperson or his/her designee suggests an alternate solution compliant with Postal Service information security policy.

### 3-6 Scheduling/Pre-Implementation Review

---

The implementation engineers review the implementation requirements of the request and schedule the change. The NCRB formally opens the change request based on the schedule for firewall updates.

### 3-7 Implementation

---

The chairperson, NCRB, or his/her designee provides technical guidance throughout the network connectivity process and closes all issues related to the connectivity request once the service is installed. The request is implemented based on the submitted change record and is completed by the appropriate group.

## 3-8 Confirmation

---

A confirmation e-mail is sent to the executive sponsor of the establishment of connectivity.

## 3-9 Escalation Procedures

---

If a request is not approved, the executive sponsor can escalate it to the manager, IT Governance.

## 3-10 Monitoring

---

All extranet connections will be monitored to ensure the connection is not a threat to the Postal network infrastructure. See Handbook AS-805, *Information Security*, Chapter 14, Compliance and Monitoring.

This page intentionally left blank

# 4 Connectivity Request Documentation Requirements

## 4-1 General

---

The Postal Service requires justification for connecting to its network. An executive sponsor, business partner, or other party requesting network connectivity must provide the appropriate documentation.

## 4-2 Connectivity Description

---

The connectivity description should include the following:

- a. A list of the system or network component names.
- b. Hardware or software being used to provide high availability services and backups.
- c. If data is encrypted at any point in the data flow, identify the type of encryption used. If encryption or a tunnel is used, specify that mechanism and both the encryption and key exchange protocols that are being encrypted.
- d. Where data is stored, that data should be identified based on data type and the defined sensitivity and criticality levels of that data.
- e. If user authentication is required for the use of this application, explain how that is accomplished and where the authentication database resides.
- f. A list of all protocols used by the host system, including transport, routing, and application-specific protocols.
- g. A list of all ports required and an explanation of the services running on those ports.

## 4-3 Architectural Diagrams

---

An architectural diagram (e.g., hardware, communications, security devices, and interconnected resources) must be attached. The architectural diagram should include (on that diagram or on separate attached diagrams) all connectivity, data flow, business flow, and supporting functions. Data flow

descriptions should include the proposed servers, protocols, networks, and projected data repositories.

The network component diagram(s) should include, but are not limited to, the following:

- a. End-user workstations and other applicable devices.
- b. Servers, including hardware type, operating system level, and hosted applications.
- c. Firewalls, including details on interfaces, ports, proxies, and protocols.
- d. Routers, including interfaces, access control lists (ACLs), and configurations.
- e. Switches (VLAN information).
- f. Intrusion detection system (IDS); include vendor, release levels, and whether it is host- or network-based.
- g. Network monitoring equipment, include vendor and release levels.
- h. If multiple IDSs and/or firewalls exist and are centrally managed, the location(s) of the management station(s) should be identified.

## 4-4 Business Case

---

The business case must clearly identify the business partner or requesting party, and the key contacts of that organization and must describe exactly how and when resources would be accessed. The business case should also specify the following:

- a. The Postal Service resources that need to be accessed and for what purpose.
- b. Whether sensitive or business-controlled sensitive data will be transmitted.
- c. The period of time for which the connection should be available. Specify the start and end dates.
- d. The time of day during which the connection will be actively used.
- e. The number of users estimated or expected to send and receive data across the connection.
- f. The type of usage (e.g., interactive queries, transactions, or large-volume data transfers).
- g. Where access will be needed and what Postal Service sites will be affected.
- h. Data communications requirements, including devices and services needed.

## 4-5 Facilities and Postal Inspection Service Approvals

Connection of physical access control and environmental systems to the Postal Service Intranet must be approved by the Facilities and Postal Inspection Service organizations prior to requesting connectivity from the NCRB. Attach copies of the approvals.

## 4-6 Configuration and Enforcement Strategy

The configuration and enforcement strategy should indicate how the business partner will ensure that the connectivity requirements defined by the NCRB are maintained, how the added protection features will continue to work, and how the isolation presented in the architecture diagram will be maintained.

## 4-7 Site Security Review

All business partner sites connecting to a Postal Service information infrastructure require a site security review performed by the manager CISO and the Chief Inspector, or their designees. A site security review must be conducted if a facility is hosting sensitive, critical, business-controlled sensitivity, or business-controlled criticality information resources and the facility has not undergone a site security review in the last 3 years.

## 4-8 NCRB Request Form

A Network Connectivity Review Board (NCRB) Request form must be completed for all NCRB requests. This form is used to request all new or changed connectivity including Corporate VPN, Wireless, Enclave, Business Partners, DNS, IP, DMZ, Switchports, and Load Balancing. The connectivity request form is available from the NCRB Web site at <http://cto.usps.gov>; select *Support*, then *Corporate Information Security*, then under "Corporate Information Security," *Network Connectivity Review Board (NCRB)*.

## 4-9 PS Form 3037, Telecommunications Service Request

This form should be completed to request the leased line for BP connectivity.

This page intentionally left blank

# 5 Contact Information

For information regarding Postal Service network connectivity, send an e-mail to *NCRB@email.usps.gov*.

This page intentionally left blank