UNITED STATES POSTAL SERVICE

Information Security Network Connectivity Process

Handbook AS-805-D

September 2009
Transmittal Letter

A. Purpose

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.

This handbook sets forth the procedures for requesting connectivity to the Postal Service network infrastructure and for establishing 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:

- Types of connectivity.
- Process for requesting connectivity.
- Associated roles and responsibilities.
- Documentation required to support a connectivity request.
- Procedures for obtaining assistance and contacts for further information.

C. Availability

This handbook is available on the Postal Service PolicyNet Web site at *http://blue.usps.gov/cpim* and on the Postal Service Internet at *www.usps.com*.

D. Comments and Questions

Address comments and questions to:

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

Comments my also be sent by e-mail to: informationsecurity@usps.gov. Use "AS-805-D, Network Connectivity Process" in the subject header.

E. Effective Date

The information in this document is effective immediately.

Ross Philo
Executive Vice President
Chief Information Officer

Contents

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 commitment 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 Contents of This Handbook

This handbook describes the process 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 about the 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:

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 privileged usage in the de-militarized zone (DMZ) and in secure enclaves uses two-factor authentication.

h. Ensure that unauthorized connectivity of information resources are brought into compliance or removed.

1-4 Postal Service Standard Networked User Interface

The standard networked user interface for the Postal Service is the Advanced Computing Environment (ACE)-approved hardware and software configurations. The NCRB must assess and approve all non-ACE network-enabled hardware and software prior to connecting to the Postal Service intranet. The exception is nonroutable mail processing equipment and mail processing infrastructure (MPE/MPI) devices that are only connected to MPE local area networks (LANs).

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, system integration testing, customer acceptance testing, production, and internal networks in cases where connectivity requests do not comply with pre-established connectivity standards.

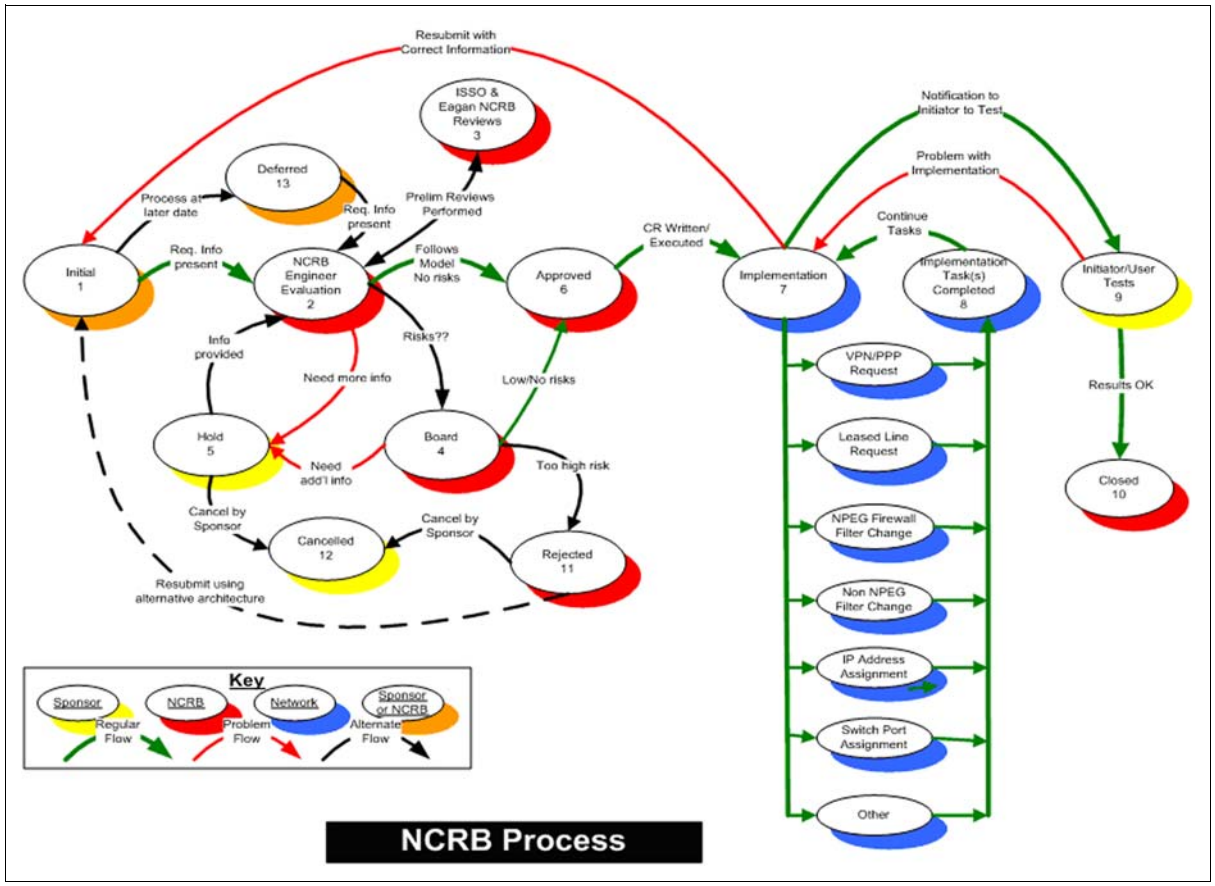
The NCRB evaluates and either approves or denies any changes to Postal Service firewall configurations. No changes are made to firewall configurations by Telecommunications Services personnel or their designees without the evaluation of and the approval by either the NCRB chairperson or his/her designee or the NCRB (as applicable).

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

1-5.2 Network Connectivity Review Board Process Overview

An overview of the NCRB process is presented in Exhibit 1-5.2 followed by a brief description of the steps in the NCRB process.

Exhibit 1-5.2
NCRB Process



Step 1, Determination of Need for Connectivity Request and Submission of the Request — The requester and executive sponsor determine the need for connectivity to Postal Service network infrastructure. The requester and executive sponsor submit an online request with a Technical Architectural Drawing and the appropriate documentation (see 3-1.2, Documentation Requirements for the Connectivity Request Package). A reference number is assigned to the request upon submission of the request. Use the reference number in all communication about this request.

Step 2, Preliminary Request Evaluation — The request form is reviewed to ensure that all information has been included on the request form. An e-mail is sent requesting any missing information. The request is deferred until the missing information is received and the request is updated.

The NCRB staff and the assigned Information Systems Security Officer (ISSO) perform the preliminary request evaluation.

Step 3, NCRB Engineer 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 determination is made if the request follows pre-approved standards or if the request requires an NCRB review. If the request requires NCRB review, an e-mail is sent to the NCRB stakeholders and the requester is notified to attend the NCRB teleconference.

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

Step 6, Scheduling Pre-Implementation Review — The implementation engineers review the implementation requirements of the request and schedule the change.

Step 7, Implementation — The request is implemented based on the approved request and is completed by the appropriate group(s).

Step 8, Confirmation — A confirmation e-mail is sent to the requester as notification 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).

1-6 NCRB Connectivity Tool Kit

The NCRB Connectivity Took Kit (CTK) is an online connectivity request form located on the NCRB page. Go to *blue.usps.gov* and do as follows:

a. Under “Inside USPS”, click on “Chief Information Officer.”

b. Click on “Information Technology.”

c. On the “Welcome to Corporate Technology” page, click on “Corporate Information Security.”

d. Click on “Network Connectivity Review Board.”

e. Under “How to Request the Service,” click on the links to the CTK Online NCRB Request form and instructions.

1-7 Granting an Exception to the Policies

Any exception to the policies in this handbook must be based on risk acceptance and approved by the chief information officer and executive vice president. If the exception impacts sensitive-enhanced or sensitive information, the chief privacy officer must also approve.

2 Roles and Responsibilities

2-1 General

The development of policies and procedures governing the protection of the Postal Service network falls under the purview of executive vice president and chief information officer. This chapter describes the roles and responsibilities associated with network connectivity.

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 chairperson.

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 ensure 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 and load balancers.

d. Managing remote access, Virtual Private Network (VPN), and dial-in connectivity.

e. Designing and managing the Postal Service network infrastructure.

f. Implementing the NCRB-approved requests and notifying the program manager and submitter upon implementation of the request.

g. Ensuring security controls are monitored or reviewed periodically to ensure their effectiveness and reliability.

h. Providing assistance for the design of proposed and future connectivity needs.

i. Removing connectivity and services no longer required or in use.

2-4 NCRB Change Control Board

The NCRB Change Control Board 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 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. Deciding on approval or rejection based on NCRB analysis findings.

h. Forwarding the approved connectivity request package to the implementation organizations.

i. Providing technical guidance throughout the network connectivity process.

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, and connections via the Internet to Postal Service nonproduction, production, and internal networks.

b. Developing standard connectivity and documentation criteria to expedite approval of connectivity requests without additional board action.

c. Determining criteria for standard connectivity that will allow for pre-approved requests.

d. Analyzing business cases and supporting documents for connectivity requests.

e. Evaluating connectivity requests and approving or rejecting them based on 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. Assisting the requester in identifying alternative solutions for denied requests that are acceptable to the requester and the Postal Service.

h. Evaluating firewall change requests and either approving or rejecting them.

i. Requesting additional information, security reviews, or audits about proposed or approved connections.

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 Business Partner (BP) network.

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 all activities associated with the requested connectivity, including 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 4-2, Business Case and Connectivity Description).

d. Ensuring completion of a connectivity risk assessment (if required).

e. Requesting and supporting a BP site security review by the Postal Inspection Service or a designated 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 requested) connectivity description, architectural diagrams, business case, Facilities and Postal Inspection Service approvals, configuration and enforcement strategy, 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 prior to 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 stated 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. Ensuring prompt notification and escalation of any information security incident according to the Postal Service incident-reporting process.

r. Notifying the NCRB when the BP partner trading agreement ends or connectivity is no longer required.

s. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service intranet.

2-8 Portfolio Managers

Portfolio managers are responsible for the following:

a. Supporting the executive sponsor in 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, and appropriate NCRB request forms.

b. Ensuring IT security controls are implemented to meet the information security requirements stated in Handbook AS-805.

c. Ensuring that the NCRB has approved any substantive configuration or procedural change before it is implemented.

d. Informing the NCRB of any changes affecting BP connectivity.

e. Notifying the NCRB when the BP partner trading agreement ends or connectivity is no longer required.

f. On a semiannual basis, reviewing and validating business partner connectivity to the Postal Service Intranet.

g. Ensuring prompt notification and escalation of any information security incident according to the Postal Service incident reporting process.

2-9 Business Partners

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

a. Before connectivity approval:

(1) Describing accurately the requirements for the proposed connection.

(2) Providing an architectural diagram of the connecting LAN/WAN (wide area network) showing all current and anticipated network connections.

(3) Providing configuration and enforcement strategy for the isolation of the connecting LAN.

(4) Cooperating in a connectivity risk assessment.

(5) Allowing a site security review by the Postal Service Inspection Service and/or CISO and/or providing an acceptable site risk assessment.

(6) Providing information required for development of the business case to the executive sponsor.

(7) Providing information to the executive sponsor as requested.

(8) 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 Postal Service read access to all connecting LAN firewalls or similar compensating controls.

(5) Allowing security reviews by the CISO staff.

(6) Allowing the Postal Service Inspection Service and/or the CISO to conduct site security review.

(7) Allowing audits by the Office of the Inspector General.

(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 record-keeping procedures for all information security incidents.

(10) Reporting any security incident immediately to the Postal Service Computer Incident Response Team (CIRT) and the executive sponsor and maintaining a point of contact with the CIRT.

(11) Establishing change control, system maintenance, and auditing procedures that comply with Postal Service policy.

(12) Notifying the executive sponsor when connectivity is no longer required.

2-10 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 record-keeping 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.

2-11 Information Systems Security Officers

ISSOs are responsible for the following:

a. Coordinating the completion of the Business Impact Assessment to determine sensitivity and criticality of the information resource.

b. Providing advice and consulting support to executive sponsors about the security requirements and controls necessary to protect the information resource, based on the resource's sensitivity and criticality designation.

c. Evaluating potential threats and vulnerabilities to the information resource and appropriate choice of countermeasures.

d. Recommending security requirements and controls.

e. Providing guidance on the Certification and Accreditation (C&A) process.

f. Conducting site security reviews with the Inspection Service.

g. Updating the NCRB Request Information on the Enterprise Information Repository Security View page.

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 Service 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 network into a remote site of a business partner.

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 nonproduction, production, or internal Postal Service networks via the Internet.

j. Non-ACE-supported infrastructure, including personally owned devices, physical access control devices (e.g., key card devices and biometric devices); environmental systems (e.g., redundant power feed controllers, heating, ventilation, 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 in Exhibit 3-1.2 should be obtained through the executive sponsor and included in the request package.

Exhibit 3-1.2
Documentation Requirements for Connectivity Requests

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
Business Case and Connectivity Description	X	X	X
Architecture Diagram	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

Requesting an extension of the Postal Service internal network into a remote BP 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. A 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. A configuration and enforcement strategy for the isolation of the connecting LAN must be provided.

g. The manager, CISO or his/her designee must have:

(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 minimum password criteria as designated in Handbook AS-805. System administrators will use two-factor authentication.

j. All remote site systems administrators must have an appropriate Postal Service security clearance.

3-1.4 Business Partner Database Connectivity

The NCRB performs the following tasks related to BP leased line connectivity involving approved database access:

a. Track access by BPs to databases throughout the lifecycle of connectivity. (See 2-7 and 2-8 for responsibilities on termination notification.)

b. Notify Database Systems and Services on approval of BP leased line connectivity to database.

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. Assigning a case number when the request is submitted through the NCRB CTK Online Request form.

b. Ensuring that the connectivity request package contains the necessary documentation in the format required by the NCRB.

c. Ensuring that all stakeholders are notified of the requested connectivity and sent a copy of the request.

3-4 Network Connectivity Review Board Engineer Evaluation

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

a. Evaluating the request and determining whether it meets the published standards for Fast Track connectivity.

b. Contracting the requester or technical contact for any additional or missing information.

c. Forwarding the package as follows:

If. . .	Then. . .
The request meets the standards and has no risk,	The chairperson, NCRB, or his/her designee approves the request and 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 full board for evaluation.

3-5 Evaluation of Nonstandard Connectivity Requests by Network Connectivity Review Board

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. Works with the requester to identify alternative solutions acceptable to the requester and the Postal Service.

c. Approves or denies the connectivity request.

d. If no approval, refers request to the NCRB CCB.

e. Documents the decision associated with each request.

3-6 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 review and scheduling the implementation.

3-7 Implementation

The implementation engineers review the implementation requirements of the request and schedule the implementation.

The chairperson, NCRB, or his/her designee is available to provide technical guidance throughout the network connectivity process. The request is implemented based on the approved request and is completed by the appropriate implementation group. A confirmation e-mail of the establishment of connectivity is sent to all the contacts listed on the request.

The requester should test the connectivity when notified that the implementation has been completed. If there are any problems, the implementation group should be contacted to resolve any problems.

3-8 Escalation Procedures

If a request is not approved, the executive sponsor can escalate it to the NCRB CCB.

3-9 Monitoring

All extranet connections are monitored to ensure the connection is not a threat to the Postal Service network infrastructure. See Handbook AS-805, 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 Business Case and Connectivity Description

A high-level description of the requested connectivity, including the applications, is required. The connectivity description must include the following:

a. Postal Service information resources that need to be accessed and for what purpose.

b. Whether sensitive-enhanced or sensitive data will be transmitted or stored.

c. Whether the access is temporary. Specify the period of time for which the connection should be available. Include 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. Physical locations from which the user will be accessing Postal Service information resources.

h. Data communications requirements, including devices and services needed.

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, and configurations.
e. Switches (VLAN information).
f. Intrusion detection system (include vendor, release levels, 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.
i. 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.
j. Where data is stored. The data should be identified based on data type, the defined sensitivity and criticality levels of that data, and whether it is encrypted.
k. If user authentication is required for the use of this application, explain how that is accomplished and where the authentication database resides.

4-4 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.

4-5 Configuration and Enforcement Strategy

The configuration and enforcement strategy should indicate how the BP will ensure 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 is maintained.

4-6 Site Security Review

All business partner sites connecting to a Postal Service information infrastructure are subject to a site security review preformed by the manager CISO and the Chief Inspector, or their designees. A site security review must be conducted if a facility is hosting sensitive-enhanced, sensitive, or critical information resources and the facility has not undergone a site security review in the last 3 years. A site security review may be conducted at any time as long as connectivity exists between the business partner and the Postal Service.

4-7 NCRB Request Forms

A CTK Online NCRB Request form must be completed for all NCRB connectivity requests. This form is used to request all new or changed connectivity including corporate VPN, wireless, enclave, business partners, DMZ, switchports, and load balancing.

Submit all requests through the CTK Online NCRB Request form, located at: *http://ncrbrequest.usps.gov/NCRB*.

This page intentionally left blank

5 Contact Information

For information about the Postal Service network connectivity, send an e-mail to NCRB@.usps.gov.

For assistance in completing the CTK Online NCRB Request form, contact the NCRB at 919-501-9718 or 919-501-9616.

This page intentionally left blank