**DEPARTMENT OF VETERANS AFFAIRS**
**Washington, DC 20420**

**VA HANDBOOK 6513**
**Transmittal Sheet**
**October 12, 2017**

# SECURE EXTERNAL CONNECTIONS

1. **REASON FOR ISSUE:** To establish policy, operational requirements, and procedures to implement the Department of Veterans Affairs (VA) Directive 6513, *Secure External Connections*.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:** This Handbook provides the specific procedures and operational requirements to implement VA Directive 6513. This Handbook establishes VA policy for managing and securing VA external connections (e.g., Site-to-Site [S2S], and Business Partner Extranet [BPE], firewall, and other connections) on and to a VA Trusted Internet Connection (TIC) Gateway. This policy complies with Federal laws, Office of Management and Budget (OMB) mandates, the National Institute of Standards and Technology (NIST) standards and recommendations, Department of Homeland Security Trusted Internet Connections Reference Architecture v2.0, and VA Directive 6500, *Managing Information Security Risk: VA Information Security Program* and VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*.

3. **RESPONSIBLE OFFICE:** The Office of the Assistant Secretary for Information and Technology (005), IT Operations and Services, (005OP), Enterprise Systems Engineering (005OP2) is responsible for the content of this Handbook.

4. **RELATED DIRECTIVE:** VA Directive 6513, Secure External Connections.

5. **RESCISSIONS:** NONE.

**CERTIFIED BY:**

/s/
Dat P. Tran
Acting Assistant Secretary for
Office of Enterprise Integration

**BY DIRECTION OF THE SECRETARY VETERANS AFFAIRS:**

/s/
ROB C. THOMAS, II
Acting Assistant Secretary for
Information & Technology and Chief
Information Officer

**Distribution:** Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

## SECURE EXTERNAL CONNECTIONS

## CONTENTS

PARAGRAPH PAGE

## SECURE EXTERNAL CONNECTIONS

## CONTENTS, cont.

PARAGRAPH PAGE

FIGURES PAGE

APPENDICES PAGE

## SECURE EXTERNAL CONNECTIONS

### 1. PURPOSE

a. The purpose of this handbook is to establish VA policy, procedures, requirements, roles, and responsibilities concerning securing external connections to and from the VA network infrastructures and IT resources. VA Handbook 6513 sets the criteria to assist management in governing and making integration decisions for the security of VA's external connections.

b. This handbook describes the processes for external connections requiring connection to VA Enterprise Infrastructure or IT resources. These processes assist in ensuring external connections are appropriately planned; secure configurations are identified and implemented properly; disconnections are implemented and validated; and external connections are approved via the Enterprise Security Change Control Board (ESCCB) process. The ESCCB process requires validating all external connections on an established basis and monitoring the connections continuously to ensure that only authorized configurations are permitted to approved baselines.

c. ESCCB Standard Operating Procedures (SOP) and User's Guide provide further guidance regarding the request for change (RFC) process for external connections.

### 2. SCOPE

a. The policies, procedures, and controls outlined in this Handbook apply to:

(1) All information technology (IT) systems that connect to the VA Enterprise Network from outside of the protected VA Enterprise Network where the purpose of the connection is to share electronic information;

(2) All VA components and IT resources, including contracted IT systems and services;

(3) All VA or contractor-operated services and information resources located and operated at contract facilities, at other government agencies that support VA mission requirements, or any other third party utilizing VA information and requiring an interconnection in order to perform a VA authorized activity;

(4) All external connections to or from VA Enterprise Networks or IT resources; and

(5) All non-compliant or rogue connections identified during the external connection reoccurring validation process.

b. The Office of Information and Technology (OI&T) will develop and disseminate security controls, and implement or institute additional requirements to maintain the Information Assurance program. This shall include those policies identified and referenced within this handbook and include other governing directives, handbooks, memoranda, notices, and best practices.

c. VA, as a whole, must adhere to the security requirements as set forth in this Handbook.

d. VA National Rules of Behavior (ROB), Non-Organizational Users ROB, and OI&T Security and Privacy Awareness Training outline the responsibilities and expected behavior of all individuals (end users) with authorized access to VA's information and information systems, including sensitive information and communications resources.

## 3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs** is responsible for designating the Department's Chief Information Officer (CIO) as the senior agency official responsible for the Department's IT program.

b. **Assistant Secretary for Information and Technology**, as the VA CIO, is responsible for:

(1) Establishing policies and procedures to ensure effective and secure control over all external connections to VA infrastructure, information systems, and data repositories;

(2) Implementing a risk management approach to IT operations that applies risk categorization to VA information and information systems and ensures a balance between risk to information systems and information with business requirements/continuity of operations;

(3) Monitoring, reviewing, and evaluating compliance with this Handbook; and

(4) As the overall VA system owner, delegating the daily operational and maintenance system owners' responsibilities to VA officials as appropriate.

c. **Deputy Assistant Secretary for Information Security** was created under the IT single authority by the VA CIO. The Deputy Assistant Secretary (DAS) for Information Security has authority over the VA enterprise cyber security budget and is responsible for ensuring external connections are properly identified, inventoried, and securely managed.

d. **Deputy Executive Director, Enterprise System Engineering** has responsibility and authority over the ESCCB and is responsible for:

(1) Ensuring that overarching policies and standards that govern the management of changes to configuration items and/or IT assets are approved according to policies; and

(2) Providing direction for change management functions and escalating RFC to the VA ESCCB while avoiding competing priorities and ensuring change authorization occurs at the lowest level possible.

e. **VA Information System Owners** (OI&T Regional Directors or their designee), as delegated by the VA CIO, are responsible for the overall procurement, development, integration, modification, implementation, operation and maintenance of security over VA information and information systems, including:

(1) Reporting, documenting, and properly securing all external connections to VA information systems under their area of responsibility;

(2) Requesting approval for the establishment of all external connections to VA information systems through the submission of the necessary external connection documentation to the ESCCB; and

(3) Creating and maintaining Interconnection Security Agreements (ISA) and Memorandums of Understanding (MOU), as required, to establish the binding agreements and implementation of technical security controls between the external connecting parties. ISAs and MOUs protect the confidentiality, availability, integrity, and data ownership of VA information processed, stored, or transmitted between interconnecting parties as approved by the ESCCB.

f. **Director, Office of Cyber Security** is responsible for:

(1) Developing VA information security policies and procedures consistent with Federal laws and VA policies; and

(2) Reviewing VA information security policies and procedures related to information security that other departmental organizations manage and oversee.

(3) Maintaining the readiness of OI&T organizations to respond to expected cyber attacks seeking to compromise external connections and veteran data.

g. **Director of Privacy and Records Management** is a voting member of the ESCCB and is responsible for ensuring requests for external connections that involve personally identifiable information (PII) and Protected Health Information (PHI) of VA employees, Veterans, service members and their families is managed in accordance with Federal privacy laws, regulations, and VA policies.

h. **Executive Director, Field Operations** is responsible for implementing the policies outlined in this Handbook.

i. **Director, Field Security Service** is responsible for providing organizations with guidance, templates, and security practices necessary for documenting known external connections.

**j. VA National Change Control Board (NCCB) is responsible for:**

(1) Ensuring that a structured process is used to review, approve, or reject proposed national-level changes to the production environment and that changes are in the interests of program and project management.

(2) All operations changes and operates at the IT Operations and Services (ITOPS) level in OI&T.

(3) Providing leadership and oversight for the National Change Management Process to support change control boards (CCBs) in managing and reviewing national and escalated change requests.

k. **VA Enterprise Security Configuration Control Board (ESCCB)** is responsible for:

(1) Reviewing all changes proposed to external connections that involve VA network resources to ensure the changes are viable from technical, security and privacy standpoints;

(2) Validating all proposed external connection changes do not adversely impact the operation of the existing system or subsystem;

(3) Certifying the external connection complies with Federal and VA policies and procedures;

(4) Processing and reviewing all external connection RFCs in a timely manner;

(5) Maintaining an accurate inventory of all external connection RFCs and their status;

(6) Maintaining an accurate inventory of all external connections;

(7) Coordinating with all key stakeholders to provide written guidance and procedures via this policy, VA User Guides and SOPs; and

(8) Escalating RFCs to higher boards for review and approval per the board’s escalation criteria and VA Directive 6004, Configuration, Change and Release Management Programs.

l. **VA Network and Security Operations Center (NSOC)** is responsible for:

(1) Evaluating external connection RFCs for impact (security or otherwise) at the TIC gateways, Internet Protocol (IP) addresses, and all port security settings;

(2) Providing recommendations, based on the VA NSOC teams’ evaluation of the RFCs, to the ESCCB voting membership through the appropriate venue;

(3) Participating as voting members of the ESCCB;

(4) Implementing the external connection changes once approved by ESCCB;

(5) Monitoring all external connections for compliance with existing federal laws and VA policies; and

(6) Ensuring all external connections, where required, are in compliance with the TIC 2.0.

m. **Director, Product Development** is responsible for:

(1) Ensuring their organizational managers responsible for projects, initiatives, and services include the VA NSOC and ESCCB at the earliest stage of the review and development process;

(2) Ensuring each new product and service receive the appropriate security, technical, and testing evaluations and approvals prior to procurement and/or development; and

(3) Ensuring compliance with VA and Federal policies as they apply to each service or project. Their managers must validate that all requirements for the project/service that require an external connection have been addressed, a RFC has been submitted, and ESCCB or NCCB approval received prior to deployment to VA test, development, or production environments.

n. **Facility Chief Information Officers (FCIO)** must be appointed in writing and are responsible for assisting and coordinating with VA information system owners in:

(1) Reporting all external connections to VA information systems;

(2) Documenting all external connections in OI&T System Security Plans within their areas of responsibility;

(3) Creating, maintaining, and submitting external connection RFCs to the ESCCB for approval; and

(4) Creating, maintaining, and approving ISAs and MOUs, which are required to establish the binding agreements and assurances necessary for implementing the appropriate security controls (management, operational, and technical) between the external connecting parties. ISAs and MOUs are required to protect the confidentiality, availability, and integrity of VA information processed, stored, or transmitted between interconnecting parties as approved by the ESCCB.

o. **Wide Area Network (WAN) and System Administrators** are responsible for assisting and coordinating with the VA information system owners in:

(1) Reporting all external connections to VA information systems;

(2) Documenting all external connections within an approved system or database for those facilities which they have purview and according to VA Device and External Connection Naming Conventions Standard; and

(3) Labeling or ensuring all external connections are labeled in communication closets at VA facilities or leased space and according to the VA Device and External Connection Naming Conventions Standard.

**p.** **Web Governance Board** is responsible for:

(1) Ensuring a consistently high quality product recognizable as coming from VA, with VA "look and feel" branding that comply with all federal mandates and agency requirements;

(2) Reviewing and approving waivers for use of VA branding involving web-related product and services;

(3) Ensuring organizational use of Internet services support VA's mission, goals, and objectives;

(4) Verifying organizational services support legitimate, VA mission-related activities;

(5) Confirming the organizational use of Internet services is consistent with prudent operational, security, and privacy considerations; and

(6) Ensuring Web sites approved to operate on behalf of VA are designed to support the widest range of potential users and computing platforms and that the Web sites comply with Section 508 of the Rehabilitation Act and Section 501 of the Rehabilitation Act of 1973 (29 U.S.C. § 701).

q. **Facility Information Security Officers (FISO) and Information Security Liaisons** are responsible for assisting and coordinating with the VA information system owners in:

(1) Reporting all external connections to VA information systems;

(2) Ensuring all external connections are documented in System Security Plans;

(3) Creating, maintaining, and submitting external connection RFCs to the ESCCB for approval; and

(4) Reviewing and concurring on all MOUs and ISAs for compliance.

r. **Privacy Officers** are responsible for:

(1) Completing a Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) where required;

(2) Determining whether any new RFC involving PII/PHI require either a PTA or PIA;

(3) Determining whether modifications to existing systems require an update to their PIA to reflect modifications;

(4) Determining whether modifications to existing systems require an update to the applicable systems of records (SORN) where the information is found and information system should be referenced, and notifying the appropriate administration's or program office's responsible Privacy Officer or Service (e.g. VHA Privacy Service, VBA Privacy Officer, etc.) to implement necessary changes; and

(5) Reviewing and signing all MOUs and ISAs for compliance.

s. **Under Secretaries, Assistant Secretaries, and Other Key Officials** are responsible for ensuring their respective administrations, staff organizations, and program offices comply with this Handbook. They do so by coordinating and collaborating with OI&T officials within their areas of responsibility regarding external connections.

## 4. POLICY

a. The VA NSOC and ESCCB Support will identify and continuously monitor all external connections to ensure the connections meet or exceed the security requirements specified in NIST Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems* and SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, NIST Federal Information Processing Standards (FIPS) Publications, TIC Reference Architecture v2.0, and VA Directive and Handbook 6500.

b. The ESCCB reviews Requests for Change (RFC) for external connections to ensure the RFCs comply with existing laws, regulations, and VA policies. The Board also evaluates, assesses, and tests the security posture of each RFC and considers the associated business value to VA's mission. The ESCCB consists of standing and non-standing members.

c. ESCCB standing members include representatives from the following VA Program Offices and functional areas (business and technical), who may have voting privileges at the local and technical review levels or the configuration board level:

(1) ESCCB Chairperson;

(2) ITOPS Enterprise Operations/Data Center Operations;

(3) ITOPS Enterprise Infrastructure Support/Web Infrastructure Support (Web Operations);

(4) VA Network and Security Operations Center (NSOC) Gateway Operations/Enterprise Network Defense/Business partner Extranet Architecture/Engineering;

(5) VA Privacy Service;

(6) Office of Public and Intergovernmental Affairs;

(7) Web Governance Board;

(8) Field Security Service;

(9) Enterprise Systems Engineering (ESE) Domain Name Service (DNS);

(10) Office of Cyber Security (OCS);

(11) Local Chief Information Officer; and

(12) Local Information Security Officers.

d. Not only may ESCCB standing members submit votes, but representatives from the Veterans Health Administration (VHA), National Cemetery Administration (NCA), and Veterans Benefits Administration (VBA) may also submit votes as appropriate.

e. ESCCB non-standing members are representatives whose specialized knowledge of a support or functional area, or subject matter expertise is essential for enhancement of the ESCCB decision process.

f. VA NSOC and ESCCB Support will ensure all external connections that are used to share or process sensitive/restricted data operates from a VA TIC Gateway and waivers will not be granted. Any external connection identified as processing or sharing sensitive/restricted data and is not operating through a TIC Gateway will be identified as non-compliant, reported as a security incident to the VA NSOC, and must be configured to meet OMB requirements through an approved transition/modification schedule for that connection.

g. The VA NSOC and ESCCB Support will comply with critical OMB TIC technical capabilities to ensure the continuance, reduction, and consolidation of external connections.

h. ESCCB standing members, technical and functional teams may meet weekly to discuss the status of and resolution to outstanding requests. A requestor may attend the weekly conference calls, as necessary. ESCCB Support will facilitate the discussions, ensure issues and concerns are addressed, and note any action(s) required on the ticket for the RFC. The ESCCB Chair will enter discussions as needed and provide any approval needed on a request using the current ESCCB Electronic Change Management System (ECMS).

## 5. TYPES OF CONNECTIONS

a. An RFC is submitted if it applies to any of the given change types listed and as they are defined in the proceeding sections. Additional change types may become available and will be addressed on a case-by-case basis as emerging technology and requirements dictate their needs.

b. Each RFC must meet specific requirements, contain appropriate documentation, and have a full business-case justification. The justification should be as non-technical as possible ensuring that anyone reading the change request can understand what is being requested.

c. Questions that are required to be answered to support the request are provided on the RFC form and are not all-inclusive. The business case should cover these specifics where possible:

(1) Derivative of what is documented in the MOU where one exists;

(2) Why it is needed and the impact if not fulfilled;

(3) Who is requesting and who is it servicing;

(4) What are the business reasons and the benefits of implementing the change;,

(5) What is the desired outcome; and

(6) Where is it needed or have an impact.

d. **Stand Alone Connection** is a VA-owned device isolated from the VA network that is connected to an ISP or stand-alone router that is also not connected to any VA network. The ESCCB does not approve Stand Alone connections, and stakeholders should work with their FCIO and ISO to get stand-alone connections approved. The ISO must report and document the existence of the stand-alone connection to the External Connection SharePoint site and to ESCCB Support. The following outlines the policy concerning a VA device connected to the external source via Stand Alone connection. The VA device must:

(1) Not connect to the VA network via physical, wireless, virtual LAN (VLAN), or any other connection type;

(2) Ensure appropriate controls, rules, and/or processes are applied and met;

(3) Ensure Air-Gapped MOU is in place;

(4) Have up-to-date anti-virus software (personal firewall software is recommended as well);

(5) Never use or share the same resources/equipment as VA networked components; and

(6) Meet the following local requirements:

(a) The ISO must ensure the external connection technical details are included in the appropriate system security plan (SSP) and other appropriate documentation;

(b) The ISO or SA performs and documents audits on an established reoccurring basis as identified in the SSP; and

(c) The CIO must implement the appropriate technical precautions to ensure the device NEVER touches any VA network.

e. **Air-Gapped Network** is a security measure implemented for computers, computer systems or networks requiring airtight security without the risk of compromise or disaster. It ensures total isolation of a given system - electromagnetically, electronically, and, most importantly physically - from other wired or wireless networks, especially those that are not secure. Air Gap networks only connection to another network is via a human being with multi-media carrying data back and forth between the networks. An air gap is also known as an air wall. An Air-Gapped connection must:

(1) Not connect to any VA network via physical, wireless, virtual, and it is physically isolated from all VA networks;

(2) Not connect to any VA network resources in use or share the same resources/equipment as VA networked components;

(3) Have an Air-Gapped MOU that meets one of the following criteria and is between:

a. VA and a business partner;

b. Facility Directors and Lead OI&T delegates;

c. VA and an external facility host; or

d. VA Facility Director and a facility hosted entity.

(4) Have a full business-case justification for the connection;

(5) Have NO connection to ECSIP; and

(6) Have a direct connection to VA site's resource, for example, a computer used for research.

(7) Does not process or share VA sensitive information. Any air-gapped VA resource processing or sharing VA sensitive information and that has a direct connection to an external entity is considered a non-compliant connection and must be brought within compliance on the TIC gateway.

f. **Local Area Network Extensions** enable a secure VA facility to communicate with the VA Wide Area Network (WAN) by way of an Internet connection. This is accomplished by establishing a VPN connection between the facility and one of the TIC Gateways. Based on the requirement, organizations seeking to implement a LAN extension connection should submit either a RFC to establish a new LAN extension connection or a RFC to modify an existing LAN extension connection. VA devices connected to an external source via a LAN extension require:

(1) No other network connections at the remote end;

(2) VA control, both logical AND physical security of the devices (e.g., VPN device, router, switch, PCs, etc.) supporting and using the connection;

(3) A MOU/ISA, if the boundary was granted the Authority to Operate (ATO) and the Assessment and Authorization (A&A) was performed by a non-VA Authorizing Authority; and

(4) The ESCCB Chair's approval.

g. **Site-to-Site (S2S) Virtual Private Networks (VPN)** enable a VA business partner to securely access specific resources on the VA WAN by establishing a VPN connection between the business partner network and one of the VA TIC Gateways. The traffic that passes over this type of connection will be limited in that only specific VA and business partner systems may communicate with each other.

(1) S2S VPN connections are external connections from the VA to a business partner using an encrypted tunnel over the TIC Gateway. S2S VPNs may be local or national connections. Organizations seeking to implement a national-level S2S must first go through the Veteran-focused Integration Process (VIP) process, which includes the completion of the ITOPS Project Intake form for approval and prior to submission of the RFC. ITOPS has a centralized intake site and processes to triage all national-level assignments, tasks, and projects. The requester can obtain detailed information for the process at the support site ITOPS Project Intake Form via the VA intranet. The requester will select the ITOPS Project Resource Intake Request option on this page, complete the new project request form, and submit the request. The ITOPS intake assists in determining the requirements and resources needed, and whether it can or should be supported as a S2S.

(2) Medical Device/Medical System manufacturers seeking to implement a national-level S2S must first go through VA Biomedical Engineering staff and OI&T's Field Security Service Health Information Security Division (HISD) program office, and not the ITOPS Project and Resource Request Form process, prior to submitting a RFC.

(3) Only devices from a specified area are allowed to participate on a connection. These devices and connections are configured based upon requirements defined by security policies and the agreements set forth in an MOU/ISA. A local ISO is responsible for reviewing and concurring with S2S connections and is authorized to request internal modifications to a S2S connection. VA government employees are allowed to request changes to S2S connections as long as those changes have been vetted prior to ESCCB submission with the system owner, ISO, and FCIO for the connection.

(4) Any device authorized for use on the VA Enterprise could potentially utilize a national S2S connection if the device is included in the Access Control Lists (ACL). All S2S connections terminate at a VA TIC gateway, and any new connections or modifications represent a change within the Gateway. Implementing approved S2S connections or modifying existing connections are standard processes and constitute low risk activities.

(5) S2S VPN supports numerous users, persistent connections, server-to-server connections, access to corporate networks, etc. There are two types of requests under S2S VPN: new S2S connection and modification to existing S2S connection. The following applies to these types of connections:

(a) High availability of hardware and infrastructure is supported through Enterprise Cyber Security Infrastructure Project (ECSIP);

(b) Service Level Agreement (SLA) requirements are supported if they fall within VA WAN SLA specifications;

(c) A S2S VPN connection is NOT designed to support high bandwidth requirements;

(d) All contractors using the connection must complete on a yearly basis OI&T Security and Privacy Awareness Training, as well as acknowledge VA's ROB, and have the necessary security risk designation/background screening either completed or in progress in accordance with existing VA policy; and

(e) Requirements for S2S VPN connections include:

(1) ESCCB and/or NCCB approval;

(2) MOU/ISA;

(3) VPN router at remote location;

(4) S2S worksheet for a new request or updated worksheet reflecting only the changes needed;

(5) ITOPS Project Intake approval if it has national-level impact and prior to submission of ESCCB RFC; and

(6) A full business-case justification for the connection.

h. **Business Partner Gateways (BPG)** are direct connections between a VA site and a business partner network. Any connection with this current architecture that is not TIC 2.0 compliant is required to convert to the TIC compliant architecture solution, such as a BPE, S2S, firewall, etc. NSOC and ESCCB support for these existing legacy connections will be limited to modifications to existing connections until they can be migrated to the TIC, and new BPG connections will not be allowed.

(1) BPGs support high bandwidth requirements and time sensitive applications that cannot be supported across the Internet and/or VA WAN.

(2) BPGs are NOT designed to support any connection where the business case justification of the connection requirements can be met by another connection option.

(3) BPG connections require the following:

(a) A completed A&A and/or a current ATO for both the VA system and the system being accessed;

(b) ESCCB approval;

(c) A MOU/ISA between VA and business partner;

(d) A centrally managed and monitored firewall and/or router (VPN capable if applicable) at the VA facility;

(e) A centrally managed and monitored Intrusion Prevention System (IPS) installed at the VA facility;

(f) On an annual basis: All contractors using the connection must complete OI&T Security and Privacy Awareness Training, as well as sign the VA's ROB;

(g) Have the necessary security clearance either completed or in progress;

(h) Clearance level is dictated by the binding VA contract;

(i) A full business-case justification for the connection;

(j) No connection to ECSIP;

(k) A direct connection to the VA site, which keeps traffic off the VA WAN;

(l) Centrally managed and monitored firewalls, at a minimum;

(m) Strict use of ACLs on firewall restricting access by origination/destination IP address, ports and protocols; and

(n) BPG Worksheet.

i. **Business Partner Extranets (BPE)** are encrypted connections between the VA and an external entity (business partner, vendors, affiliate university, etc.) through one of the VA TIC gateways. BPEs use a leased circuit to connect the two partners directly, which makes the connection capable of supporting higher bandwidth requirements.

(1) BPEs are connections from a remote business partner to a VA Multi-level Protocol Label Switching Cloud, terminating at a TIC gateway, with separate controls in place for each specific connection. There are two distinct types of BPE: internal (sometimes called trusted) and external (sometimes called untrusted). With an internal BPE, the remote network is air-gapped; all connectivity flows through the VA's TIC gateway. The external BPE remote network may have its own connection to the Internet. ACLs are used to limit visibility to only the required VA devices that are similar to S2S VPN.

Organizations seeking to implement a national-level BPE or new BPE project or sub-connection must first go through the Veteran-focused Integration Process (VIP) process, which includes the completion of the ITOPS Project Intake form for approval and prior to submission of the RFC to the ESCCB. The requester can obtain detailed information and register their project via the VA intranet at http://go.va.gov/vipr.

(2) The requester will select the ITOPS Project Resource Intake Request option on this page, complete the new project request form, and submit the request. The ITOPS intake assists in determining the requirements and resources needed, and whether it can or should be supported as a BPE. Once the ITOPS Intake process is completed and the RFC is submitted to the ESCCB, the BPE request may take a minimum of 90 days to implement after it's approved at the ESCCB level and final approved by the NCCB. Requirements for BPE connection or sub-connection include:

(a) ESCCB and/or NCCB approval;

(b) MOU/ISA;

(c) BPE worksheet for a new request or updated worksheet reflecting only the changes needed;

(d) ITOPS Project Intake approval prior to submission of ESCCB RFC;

(e) A full business-case justification for the connection; and

(f) A completed A&A and/or a current ATO for both the VA system and the system being accessed.

(3) There are four types of BPE RFCs: a request for new BPE sub-connection, a request to modify an existing BPE sub-connection, a request to establish or modify a BPE and firewall connection, or a request to establish or modify a BPE and Web server connection.

(a) A RFC for a new BPE sub-connection will establish the initial connection between the VA and a business partner environment. The new sub-connection involves:

1. Modifying an established BPE connection; and

2. Modifying the access control rules associated with a specific program or service that the business partner hosts.

(b) A RFC to modify an existing BPE sub-connection involves either a connectivity update or an update to the connection architecture.

1. Connectivity updates involve modifying the communication requirements between the business partner environment and the VA network. The requesting organization MUST:

a. Document all connectivity changes via a BPE worksheet;

b. Submit a "BPE and Firewall Waiver" RFC to document connectivity from the BPE to the Internet on non-standard ports/protocols; or

c. Submit a "BPE and Web Server" RFC to document connectivity from the Internet to a Web/application server hosted on the business partner environment.

1. Connection architecture updates involve modifying the existing BPE sub-connection architecture (i.e., expanding the available IP address pool, re-IP addressing the remote environment, reallocating the business partners' assigned IP addresses, etc.). Such updates

require the business partner and the VA BPE architecture team to coordinate directly to make changes to the ACL. A BPE worksheet is NOT required for this type of request.

(c) A RFC to establish a BPE and firewall connection involves modifying the communication requirements between the business partner environment and the VA network. The request asks to add access controls that allow business partner devices to connect to the Internet via the TIC gateway. All requested modifications must be reflected on a BPE worksheet.

(d) A RFC to establish a BPE and Web server connection involves adding or modifying inbound traffic flows to a BPE environment for external (Internet) access to a hosted device or service.

j. **Web Server** service delivers (or serves) content, such as Web pages, using Hypertext Transfer Protocol (HTTP), over the VA Intranet or the public Internet. A Web server RFC is a modification or update to host a system or service inside the VA network that provides content and/or application services to end users via the VA Intranet, public Internet, or both. VA Intranet server and Internet/public server are the two options for this change. Organizations may also use this RFC type to request any publically available application server/service, hosted by VA that involves in-bound traffic from the public Internet.

(1) VA Web server includes VA Internet Web/application servers, in-bound traffic on non-web related ports (e.g., sFTP, DICOM, SQL, etc.), and VA Intranet Web/application server. Publicly available resources may support or represent a single site or group within VA and/or support an enterprise function/initiative. However, each will have a Fully Qualified Domain Name (FQDN) in the va.gov address space. Some may be universally viewed as having an impact to the entire VA.

(2) Publicly available resources must be physically located in a Demilitarized Zone (DMZ) within the VA enterprise, but all traffic flows are implemented through the TIC gateways. Intranet servers do not require any changes beyond internal DNS modifications.

(3) Requirements for Web Server connection include:

a. ESCCB approval;

b. Review of the Web Server Request checklist and WASA FAQs;

c. Web Application Security Assessment (WASA) Questionnaire submitted to the VA NSOC Web team at New WASA Questionnaire;

d. WASA final report with all vulnerabilities remediated or an approved POAM accepting risk(s) and vulnerabilities signed by all appropriate approving officials;

e. Privacy Threshold Analysis (PTA) to determine if a Privacy Impact Assessment (PIA) is required;

f. PIA if required;

g. Review of current PIA to determine if a new PIA is required;

h. Full business justification;

i. Meet the requirements of VA Directive 6404, *VA System Inventory (VASI)*, VA Directive and Handbook 6102, both titled *Internet/Intranet Services*, Section 508 Compliance Enforcement for Software and Application and Section 508 Compliance Enforcement for VA Internet and Intranet Websites Memorandums; and

j. Register websites and web applications in the VA Web Registry and all other web requirements must be registered in VASI.

k. **Firewall Waivers** allow communication from VA to a routable destination (typically a public IP address) using ports or protocols that the VA TIC gateway's default firewall configuration blocks.

(1) A firewall waiver must include the VA source IP addresses, destination remote IP addresses, and the required ports and protocols.

(2) The requesting organization must provide both VA and remote IP addresses with this type of request.

(3) Unified Resource Locators (URL) are not acceptable with the exception of firewall requests that require APPIDs to be unblocked.

(4) Firewall waivers denote non-standard OUTBOUND communications from specified devices within VA to one or more publicly available destinations. Regardless of the number of devices involved on either end, changes approved via the ESCCB are implemented at the TIC gateway.

(5) A firewall RFC should be submitted for APPID unblock and will require only a full business justification and will not require an MOU/ISA. In cases where there is a known risk/vulnerability that is to be part of the acceptance, a risk acceptance will be required and approved as a POAM through Risk Vision. All associated URLs must be included in the RFC.

(6) Firewall waivers for Geo-located countries where VA facilities reside and operate and those with North Atlantic Treaty Organization (NATO) countries will be documented through the ESCCB process and according to policies. A country's susceptibility to risks changes daily; therefore, an in-depth review process must be established to address those high-risk areas even if the area is listed as a NATO country. Foreign travel with a VA laptop, or device, and remote access will be part of the in-depth review process. The process will define, document, and validate the mitigation of those risks.

(7) Implementation of approved firewall modifications is a standard process and constitutes a low risk activity. Requirements for firewall waiver include:

a. ESCCB and/or NCCB approval;

b. As applicable an MOU/ISA, BAA, or Data Use Agreement, and for foreign countries proof of State Department clearance will also be required;

c. Firewall supplemental worksheet when there are too many entries for the fields on the form request;

d. Full business justification; and

e. Approved POAMs accepting risk(s) when required or where no MOU/ISA exists for ftp, sFTP, SSH and whitelist requests.

l. **VA Department of Defense Gateway** is a multipurpose encrypted connection between the VA WAN with a Department of Defense (DoD) entity or Defense Health Agency (DHA) network. The DHA network connects DoD health facilities throughout the US and overseas. This gateway allows any DoD healthcare facility to request access to resources on the VA network and to share medical information when active or retired military members transition between the DoD medical facilities and VA medical facilities.

(1) Organizations may request either a new VA DoD connection or a modification to existing VA DoD connection. Requirements for DoD Gateway include:

(2) Submission of New VA DoD Connection when no connection exists between VA and the DoD entity, when the connection is a direct connection between VA and the DoD entity, and either falls within the boundary of the current signed DoD MOU/ISA.

(3) Submission of Modification to Existing VA DoD Connection when a TIC compliant connection is already in place between VA and DoD entity and modifications are required.

(4) Implementation and approval of a VA DoD Connection or modification is a standard process and constitutes a low risk activity. Requirements include:

a. Completing and forwarding of the Enterprise Infrastructure VA DoD Connection Migration Spreadsheet to VA OI&T EIE by requester;

b. VA OI&T EIE verifying forms for accuracy and completion;

c. Requester submitting completed documentation to DoD CRM Team via CRM.Team@tma.osd.mil;

d. Completion of Ports and Protocol worksheet from the DoD CRM Team that provides the national address translation IP addresses;

e. ATO of external entity;

f. MOU/ISA;

g. ESCCB approval; and

h. Full business justification.

(5) A requirement for a connection between VA and other DoD entities may exist but will not fall under DHA and where the national-level MOU/ISA does not apply; when this occurs, refer to the connection requirements for a S2S, unless directed to use the above process.

m. **Domain Name Service (DNS)** involve two types of requests: internal and external. The VA National Service Desk (NSD) supports new and modifications to internal DNS, whereas organizations requesting external DNS entries will submit a Web server RFC because each unique external FQDN is associated with its own network address translation. Any external DNS change signifies a change in the va.gov namespace for which VA is the authoritative source, and could be considered as having an impact on the entire VA. If the DNS involves a BPE a modification to BPE/Web Server change request will be submitted. The following is required for a DNS request:

(1) A full business justification;

(2) Fully Qualified Domain Name (internal and external) registered with the VA Web Registry when it involves web sites and web applications, and entered into VASI for all other requirements; and

(3) ESCCB approval.

n. **Edge Security Zone Service** offers an environment to deploy a service that provides connections to and from both the VA WAN and the Internet that is not provided through any other RFC connection. The Security Zone serves as a DMZ environment where access control entries restrict traffic to and/or from an environment. Organizations may request either a new edge security zone connection or a modification to existing edge security zone connection. The following applies to an edge security zone service request:

(1) The requester submits a request through the NSD to VA NSOC prior to submitting a RFC for new edge security zone service;

(2) The VA NSOC directs the requestor to use this request type after approval from the VA NSOC leadership is granted;

(3) A ITOPS Project Intake Form submission is required for all new edge security zone service;

(4) The requester submits a Firewall RFC documenting the NSOC approval date, the NSD ticket number, the ITOPS Project Intake identification number, and provides all other required documentation; and

(5) A modification to existing edge security zone connection request is only submitted if the service has already been deployed. The requester is not required to contact the VA NSOC or have a ITOPS Project Intake identification number completed prior to submission of a modification, but should reference the initial ESCCB request on the RFC form.

## 6. ESCCB REQUEST FOR CHANGE PROCESS

a. The ESCCB processes a RFC through the ECMS. The RFC is subject to reviews, assessments, and approvals at all defined levels prior to implementation on any VA enterprise information system. The ESCCB change process for a RFC begins when the local ISO or VA government employee or their representative submits a RFC to modify the VA network infrastructure that will allow an external connection. The proceeding paragraphs explain the process and actions that occurs to a RFC once submitted in the ECMS. Figure 1: ESCCB Review and Approval Process Flow, below, depicts the change process.

b. The local level management (business or system owners, FCIO, FISO, and local privacy) vets and accepts the RFC prior to submission of the request into the ECMS. A requester submits the RFC in the ECMS application page at https://esccb.va.gov/cgweb/MainUI/StartPage.aspx. Contractors can create a request but may not be listed as a requester and should contact their VA government counterpart or Contracting Officer Representative confirming the needed changes prior to submission.

c. Once the RFC reflects “Submitted” within the ECMS,  ESCCB Support will validate that the request is complete and ready to move forward to the next level of processing.  The staff will return incomplete requests to the requester via the ECMS.  The ECMS generates and sends email automated notifications to the requester indicating what information is still required to complete the RFC.  The request is considered complete once all required fields are filled on the application form and all supporting documentation for the ticket has been attached to the request.

d. The system offers the ability to assign a priority status to a request.  The priority status assists ESCCB Support and the VA NSOC with prioritizing, processing, and implementing the RFC received.

e. Each RFC is reviewed and approved in sequence by the ISO and CIO at those local levels.  Each level may approve, reject, or return the ticket to the requester for more information.  Once the ticket is approved at each level, the request is automatically forwarded for “Technical Review”.

f. Technical reviewers from the following groups may evaluate the RFC based upon the change type:  VA NSOC’s BPE Architecture and Operations, Enterprise Network Defense, ESE DNS, Gateway Operations, and Remote Access Management.  The technical review process may take 10 business days, barring the need for additional information or corrections, or the need to address associated security risks.  If the RFC requires additional information, the 10-day window stops and the RFC is returned to the requester.  The requester updates and resubmits the ticket via the ECMS.  The ECMS will automatically notify the technical reviewers and ESCCB staff via e-mail of the resubmission.  The 10-day window will restart at this time.  The next level of review and approval is ESCCB Voting.  The voting members perform functional area review and approval based upon the change type requested.  The ESCCB Voting level within the ECMS consists of members from VA Privacy, Web Governance Board, Field Security Service, and OCS.  Upon review of the ticket, they may request more information, approve, reject, or close the ticket.  Once all members at this level have voted to approve, the request is submitted to the ESCCB Chair for a decision.

g. The ESCCB Chair may request more information, reject the request, approve for implementation, or approve to escalate to the NCCB for their review and approval.  Section 7 of this Handbook outlines the NCCB escalation process.  If the RFC does not meet NCCB escalation criteria, the RFC is automatically e-mailed to the NSD after the ESCCB Chair’s approval.  The NSD creates a helpdesk ticket and sends the notification to the appropriate VA NSOC implementation team.  The requester and approving ISO receives an automatic e-mail notification of the ESCCB Chair’s decision and the NSD ticket reference number.

h. If a request meets the NCCB escalation criteria, the requester is invited to attend the next NCCB weekly meeting to provide a brief description to the NCCB and answer any questions concerning their request from the NCCB.  If the requester is unable to attend, a representative can attend and answers any questions from the NCCB.

i. An RFC can be assigned emergency status when it impacts either patient care, has a monetary impact on VA, affects a major IT initiative being implemented by VA, or involves Section 508 compliance. The process for a ticket designated with emergency status begins when the local ISO or VA government employee submits a RFC in the ECMS and selects the emergency status option on the form field. ESCCB Support validates the request to ensure it meets emergency status criteria.

j. ESCCB Support forwards the request to the local ISO and CIO for review and approval once the emergency status is validated. The ISO and CIO approval sends the RFC to technical review. Technical review is completed within 48 hours, barring the need for additional information or the need to address and/or mitigate associated security risks. If more information is required, the 48-hour window stops until the ticket has been updated and resubmitted by the requester, whereas the 48-hour window resumes. Once the technical review level approves, ESCCB Voting, which consists of OCS, Privacy Services, and Network ISO, reviews and approves if no additional information is needed. The request is sent to the ESCCB Chair for a decision after the final level of ESCCB voting approval is received.

k. The ESCCB Chair may request more information, reject the request, approve for implementation, or approve to escalate to the VA NCCB for review and approval. If the ESCCB Chair determines that the RFC does not require escalation to the NCCB, the Chair will approve and the NSD is sent an automated notification of the approval. The NSD creates a separate ticket and forwards the request to the appropriate VA NSOC implementation team. The ECMS also sends an automated notification to the contact ISO and requester.

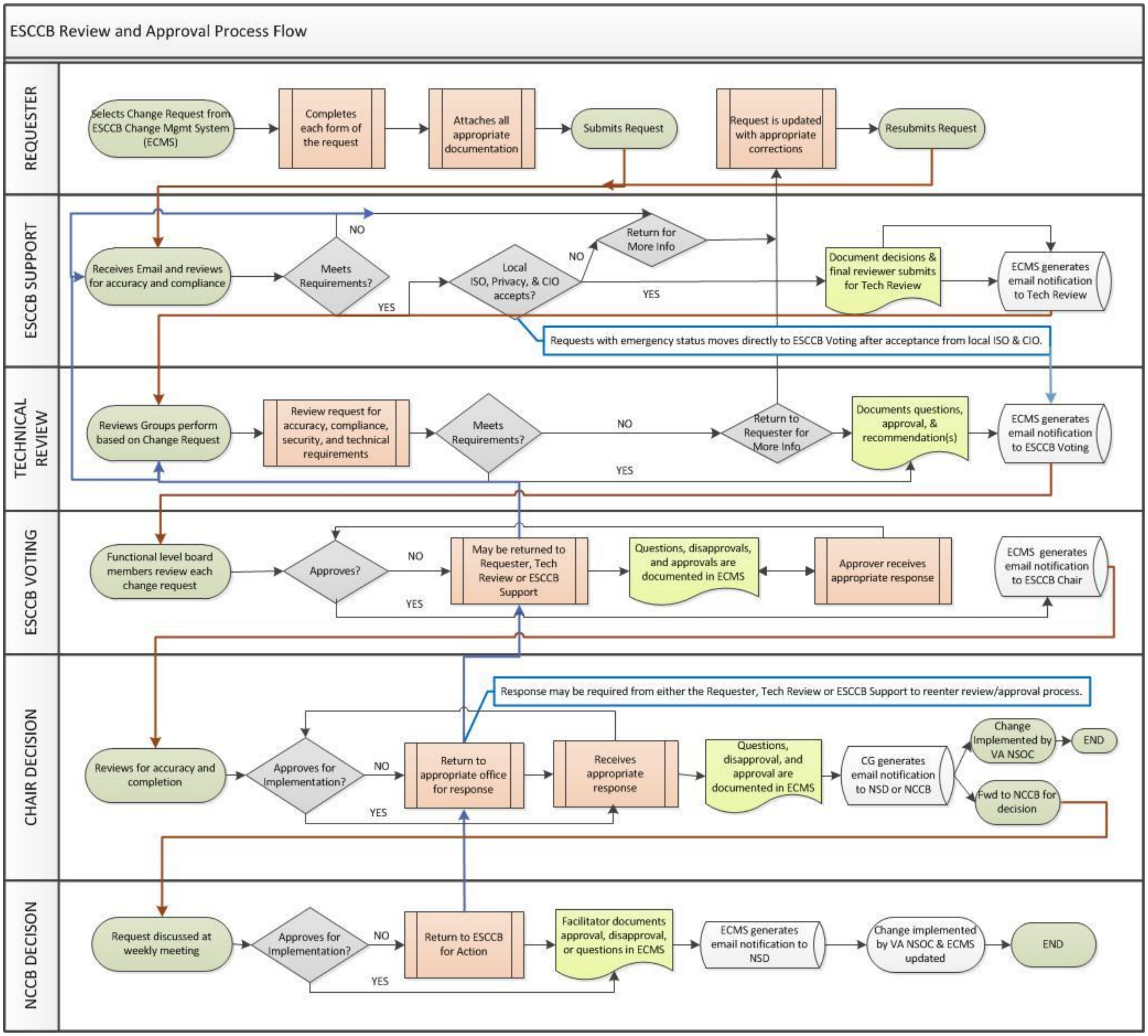
ESCCB Review and Approval Process Flow
REQUESTER
Selects Change Request from ESCCB Change Mgmt System (ECMS)
Completes each form of the request
Attaches all appropriate documentation
Submits Request
Request is updated with appropriate corrections
Resubmits Request
ESCCB SUPPORT
Receives Email and reviews for accuracy and compliance
Meets Requirements?
NO
YES
Local ISO, Privacy, & CIO accepts?
NO
Return for More Info
YES
Document decisions & final reviewer submits for Tech Review
ECMS generates email notification to Tech Review
Requests with emergency status moves directly to ESCCB Voting after acceptance from local ISO & CIO.
TECHNICAL REVIEW
Reviews Groups perform based on Change Request
Review request for accuracy, compliance, security, and technical requirements
Meets Requirements?
NO
Return to Requester for More Info
YES
Documents questions, approval, & recommendation(s)
ECMS generates email notification to ESCCB Voting
ESCCB VOTING
Functional level board members review each change request
Approves?
NO
YES
May be returned to Requester, Tech Review or ESCCB Support
Questions, disapprovals, and approvals are documented in ECMS
Approver receives appropriate response
ECMS generates email notification to ESCCB Chair
CHAIR DECISION
Response may be required from either the Requester, Tech Review or ESCCB Support to reenter review/approval process.
Reviews for accuracy and completion
Approves for Implementation?
NO
YES
Return to appropriate office for response
Receives appropriate response
Questions, disapproval, and approval are documented in ECMS
CG generates email notification to NSD or NCCB
Change Implemented by VA NSOC
END
Fwd to NCCB for decision
NCCB DECISON
Request discussed at weekly meeting
Approves for Implementation?
NO
YES
Return to ESCCB for Action
Facilitator documents approval, disapproval, or questions in ECMS
ECMS generates email notification to NSD
Change implemented by VA NSOC & ECMS updated
END

**Figure 1. ESCCB Review and Approval Process Flow**

**Figure 1, above, illustrates the ESCCB review and approval process. The general sequence flows as follows:**

- Requestor: submits RFC with appropriate documentation to ESCCB Support via ECMS.
- ESCCB Support: reviews for accuracy and appropriate documentation and if it meets the requirements for technical review forwards RFCs to the local ISO and CIO for approval.
- Technical Review: (1) reviews the RFC for accuracy, security and technical compliance; (2) documents questions, recommendations, approval and/or disapproval; (3) approval moves RFC to ESCCB Voting.
- ESCCB Voting Levels: documents approval or disapproval; approval forwards the RFC to ESCCB Chair.
- ESCCB Chair: approves or disapproves the RFC for implementation or forwards for NCCB decision.
- NCCB Decision: approves or disapproves the RFC. Approved RFCs are implemented by the VA NSOC.

## 7. NCCB ESCALATION CRITERIA

The following section describes the NCCB escalation process for each RFC. The RFC form on every change type includes questions that must be addressed on all submissions, eliminating the need to submit a separate document with the RFC when escalated to the NCCB for approval or as informational.

### a. **Firewall Waiver**

Only firewall waivers that involve the entire VA IP address space (10.0.0.0/8) require escalation to the NCCB. These changes may trigger the need to review and update the firewall baseline configuration documentation.

### b. **Site-to-Site VPN**

Only S2S VPN requests related to national-level S2S connections require escalation to the NCCB. The ESCCB will provide informational notification to the appropriate parties concerning approved modifications to national S2S connections according to SOPs.

### c. **VA Web Server**

The VA Web Internet/Public Server request which provides access to publically available resources and VA Intranet Servers request may require escalation to the NCCB. The specific criteria on web server change types, and whether to escalate, is listed below and will be entered in the RFC data collection form fields in the ECMS to assist in determining which requests require escalation.

(1) Internet/Public Server

(a) Server supports or represents a specific VA site or group and does not collect PII or PHI – not escalated;

(b) Server supports or represents a specific VA site or group and does collect PII or PHI – escalated for informational purposes; and

(c) Server supports or represents an enterprise-wide function or service offered by VA – escalated for approval.

(2) VA Intranet Servers:

(a) Server supports or represents a specific VA site or group and does not collect PII or PHI – not escalated;

(b) Server supports or represents a VA function or group across the enterprise and does collect PII or PHI – escalated for informational purposes; and

(c) Server supports or represents a VA function or group across the enterprise and does collect PII or PHI – escalated for approval.

### d. **DNS Requests**

Only DNS requests that involve using the va.gov namespace on servers hosted outside VA (not within our 10. or 152. IP address space) require escalation to the NCCB.

### e. **Business Partner Gateway**

Modifications to existing legacy connections and the BPG architecture imply local impact only; therefore, policy does not recommend escalating BPG requests to the NCCB. However, BPG modification requests with an identified impact of “Entire VA” may be deemed important enough to be escalated for informational purposes.

f. **Business Partner Extranet**

Modifications to internal and external BPE connections requests will be escalated to the NCCB for informational purposes and when it impacts the “Entire VA”. Only new BPE requests are escalated to the NCCB for approval.

g. **VA DoD Gateway**

All approved DoD gateway requests will be escalated to the NCCB for informational purposes. The ESCCB chair will determine which of these requests will need to be escalated to the NCCB for approval.

h. **Edge Zone Security Services**

All ESCCB approved national-level requests that involve the entire VA IP address range will be escalated to the NCCB for final approval.

## 8. S2S AND LAN EXTENSION PROCESS

a. Subsequent to the ESCCB’s approval, the following must occur when implementing the S2S extension connection:

(1) The ECMS will send an automatic notification to the VA National Service Desk (NSD) that the connection was approved. The NSD will open a ticket and notify VA NSOC implementation team.

(2) The VA NSOC will schedule a meeting with the appropriate VA and the external entity technical points of contacts (POCs) to discuss the details of the request.

(3) If all IPs, ports, and documents are accurate in the ESCCB approved ticket, VA NSOC will schedule another meeting to conduct the connection turn up.

(4) During the connection turn up meeting, VA NSOC will verify the connection is “up” and “operational” as defined by the RFC. If an issue is encountered and VA NSOC or the external engineers require additional time, a new meeting may be scheduled to continue working.

(5) If the connection is not implemented within 90 days of the ESCCB approval date, the VA NSOC will close the ticket. The VA full time employee (FTE) remote access lead notifies the ESCCB, VA NSOC ESCCB representative, and the requester that the ticket will be closed.

(6) After 90 days of the date of approval and lack of implementation of the connection, the following process will occur:

(a) VA NSOC Remote Access Team will close the NSD ticket. The VA FTE remote access lead notifies the ESCCB, VA NSOC ESCCB representative, and the requester that the ticket has been closed.

(b) VA NSOC will request that new and verified documentation be resubmitted.

(c) The ESCCB will determine whether a new RFC is required. The requester contacts the ESCCB Staff and submits the modified documentation for reevaluation.

(d) If the ESCCB determines documentation requires a new RFC, the requester and ESCCB will follow the normal ESCCB review and approval process.

(e) When the ESCCB approves the request, the VA NSOC will re-engage the technical POCs for VA and the external entity and the process will start from the beginning.

(f) If a reevaluation by the ESCCB is not required, VA NSOC will require the following:

1. The ESCCB Chair must provide written approval to the VA NSOC.

2. The requester will provide the ESCCB Chair and VA NSOC with a statement confirming that all the documentation approved previously by the ESCCB has been reviewed and is up-to-date.

3. The requester must contact NSD to open a new NSD ticket. The new ticket must include all documentation submitted in the original RFC.

4. When the VA NSOC receives the new ticket, they will re-engage the technical POCs for VA and the external entity and restart the implementation process.

(g) Connections expected to take longer than 90 days requires the requester to annotate the RFC with the expected date of completion. The ticket will remain open until that date. VA NSOC will close tickets for connections not implemented within 30 days of the annotated expected date. The normal process of closing the ticket due to failure in implementing the connection will resume.

b. The following must occur when implementing the LAN extension connection:

(1) The ESCCB will notify the NSD that the connection was approved. The NSD will open a ticket and notify the VA NSOC implementation team.

(2) VA NSOC will schedule a meeting with the appropriate technical POCs from VA and the external entity to discuss the details of the request.

(3) If all IPs, ports, and documents are accurate in the ESCCB approved ticket, the requestor will coordinate with the NSOC regarding shipping and configuring the LAN extension hardware.

(4) LAN extensions are considered plug-and-play and do not require a turn up call for further configurations. However, if the requester is unable to connect the LAN extension, he or she should contact the VA NSOC staff for assistance.

(5) If the connection has not been implemented within 90 days of the ESCCB approval date, the VA NSOC will close the NSD ticket. The VA FTE remote access lead will notify the ESCCB, VA NSOC ESCCB representative, and the requester that the ticket will be closed.

(6) The only exemption to delaying the 90-day implementation timeframe is the requirement for ordering circuits.

(7) The requester will notify VA NSOC when the circuit is expected to be turned up. When providing updates the requestor should include the NSD number with all communication. Status updates will be provided to VA NSOC a minimum of every 30 days.

(8) Failure to provide updates may result in the NSD ticket being closed by VA NSOC. The connection will still need to be implemented within a reasonable amount of time.

(9) After 90 days from the date of ESCCB or NCCB approval and the lack of implementation of the connection, the following process will occur:

(a) VA NSOC Remote Access Team will close the NSD ticket. The VA FTE remote access lead will notify the ESCCB, VA NSOC ESCCB representative, and the requester that the ticket has been closed.

(b) The VA NSOC will require the requester to submit new and verified documentation through the ECMS and attach the documentation to the RFC.

(c) The requestor will contact the ESCCB to determine whether a new RFC will be required.

(d) If the request requires a new RFC, the requester must prepare and submit via the normal ESCCB review and approval process.

(e) If the existing ESCCB approval is still valid, the VA NSOC will require the following:

1. The ESCCB Chair will provide written approval to the VA NSOC and the RFC will be updated with the approval in the ECMS.

2. The requester will provide the VA NSOC a statement confirming that all the documentation approved previously by the ESCCB has been reviewed and is still current. If there are any modifications, then the request will be resubmitted for ESCCB evaluation.

3. The requester must contact the NSD to open a new NSD ticket. The new ticket must include all documentation submitted with the original RFC.

4. When the VA NSOC receives the new NSD ticket, they will re-engage the technical POCs for VA and the external entity and the implementation process will restart.

(f) If the connection is expected to take longer than 90 days, annotate the RFC with the expected date of completion. The ticket will remain open until that date. If the connection is not implemented within 30 days of the expected date noted in the RFC, the VA NSOC will close the ticket. The normal process of closing the ticket due to failure of implementing the connection will resume.

## 9. OTHER SECURITY REQUIREMENTS for EXTERNAL CONNECTIONS

a. To obtain ESCCB or NCCB approval, external connections must incorporate adequate information assurance and security controls to safeguard VA information systems and data, ATOs where applicable, and TRM approval for software being utilized on the VA Enterprise.

b. Connections involving a Cloud Service Provider (CSP) requirements will vary based upon the business needs and technical solution. The VA Cloud Program is managed by the Enterprise Cloud Service Broker (ECSB). The ECSB should be contacted for those Programs looking to operate in the Cloud. The type of connection for a CSP will follow those outlined in Section 5 of this policy and will be determined based upon the business needs.

c. Continuous monitoring will be in place for all external connections through technical and manual mechanisms. Auditing and filtering will be deployed and well documented. Security issues, concerns, or incidents will be immediately reported to the CIO and ISO. Connections involving serious violations will be terminated immediately until all issues have been addressed and resolved. All concerned parties will follow agreed upon procedures outlined in their SSPs and MOUs/ISAs. At a minimum, all connections shall conform to the following specifications:

(1) **Configuration and Installation**

(a) The NSOC will only configure the external connections as outlined in the request and as approved by the ESCCB or NCCB;

(b) Configure the firewall hardware, operating system, and software with all current upgrades, patches, and configuration changes, including mitigating all related known and potential exploits;

(c) Support high availability configurations and load balancing through integrated capabilities or by integration of third party products (i.e., hardware);

(d) Configure the firewall so that it cannot be identifiable as such to other network(s) or, at most, appears to be just another router;

(e) Disguise or hide internal DNS to prevent direct external requests;

(f) Ignore service requests like “echo” or “chargen” that could be used in a denial of service attack;

(g) Prevent network connections from bypassing the firewall;

(h) Install in locations that are physically secure from tampering; and

(i) When a RFC requires modification, modify the RFC prior to approval and/or prior to full implementation. Modifications to an approved request prior to full implementation must be reviewed and accepted by the ESCCB staff and VA NSOC. Approvals of modifications to approved but not fully implemented RFCs are processed and approved as “In Scope Change” and only by the ESCCB Support when updated information has been included in the RFC. An automatic notification is sent to the VA NSOC through the ECMS. Modification to a request already implemented is submitted as a “Modification to Existing” connection unless otherwise agreed upon as an In Scope approval by ESCCB Support and NSOC and on case-by-case basis.

(2) **Access Management**

(a) Follow existing network policies when granting access to or from an external connection. A MOU and/or ISA must be in place for all external connections and shall be signed by all appropriate parties prior to granting access. Any assistance needed or questions concerning the submission and review process for MOU/ISAs should be directed to the local ISO or contact Field Security Service.

(b) Only grant access to external connections to those sites, agencies, or individuals identified in the request. All future requests will follow the ESCCB process, VA security, and IT policies.

(c) Restrict use of a particular application to only those customers authorized to access the application.

(d) Implement a "deny all services except those specifically permitted" design policy.

(e) Implement a strong authentication technique for administrative login to permit secure remote login by the authorized system administrator.

(f) Employ techniques to reduce network/computer threats by reducing or eliminating particular network traffic to or from external connections. This should include blocking ports or IP addresses that can be used to exploit internal networks/computers. This should also include content filtering to permit or deny connections to specific hosts or groups of external hosts.

(g) Incorporate and operate a systematic method of intrusion detection. Data from intrusion detection must be stored such that it can serve as evidence in forensic investigations.

(h) The contracting office will include agreed upon language in all contracts involving external connections. Contractor security guidance will follow guidance in accordance with VA Handbook 6500.6, *Contract Security,* and grant access to VA information or information systems only to those contractor employees and subcontractor employees, requiring such access and whom have read, understand, agree to abide by the rules and acknowledge by signing VA's ROB. They must also acknowledge their understanding on an annual basis.

(i) If a medical device vendor anticipates that the services under the contract will be performed by 10 or more individuals, VA's ROB may be signed by the vendor's designated representative. The contract must reflect that, by signing the ROB on a yearly basis on behalf of the vendor, the designated representative has ensured all such individuals working on a VA contract have reviewed and understand VA's ROB when accessing VA's information and information systems, and these rules will be reviewed and acknowledged on a yearly basis by each of these individuals.

(j) Contracting facilities hosting VA information or systems will be monitored on a continuous basis to assess compliance and for reporting purposes.

(3) **Auditing and Filtering**

(a) Log access to and through every firewall.

(b) Capture login attempts by authorized and unauthorized users.

(c) Employ IP-filtering that can filter on a wide variety of attributes, including source and destination IP addresses, protocol types, port numbers, and inbound and outbound interfaces.

(d) Generate an audit trail of calls passing through each firewall for review of security anomalies at future times.

(4) **Notification of Incidents**

(a) Provide notification of threats, including unsolicited distribution of executable files, and notification of efforts by accepted users to gain access to systems or applications that they do not have permission to enter.

(b) Generate alarms, predicated on the occurrence of a specific event or combination of events, on a timely basis (e.g., within 60 seconds) after the event occurs.

(5) **Security Enhancements**

(a) Accommodate new services and needs to allow for changes in VA security policy.

(b) Contain advanced authentication measures, or the hooks for installing advanced authentication measures, if strong authentication for inbound access is required.

(c) Ensure the ESCCB authorizes the connections prior to use.

(d) Administrations and staff offices will implement procedures necessary to ensure that connections under their purview are approved and validated annually.

(e) Prior to connection approval, Administrations and staff offices will ensure that connections meet current standards issued by NIST, the National Security Agency for DoD connections, TIC 2.0, and other Federal-wide authorities that regulate information security.

(f) Processing approval is granted through the A&A management official responsible for the protected asset.

(g) Organizations, other than those that sponsor the use and administration of the connections, shall review the connections periodically and independently. These reviews will ensure that connections remain in compliance with the minimum-security standards as outlined in security policies and this Handbook, while ensuring that MOU/ISAs, risk assessments, security plans, and contingency plans remain current.

## 10. CONNECTION DECOMMISSION PROCESS

When a connection is no longer needed, the connection will be formally decommissioned. The connection to any device, site, service, etc. will be terminated, all access control rules deleted, and the return of any VA material and equipment will occur and be a documented artifact with the RFC for the decommission. The decommission option is part of the form on each applicable change type within the ECMS. The requester submits an RFC that indicates whether the connection should be decommissioned -- as soon as possible or on/or before a specific date.

## 11. ADMINISTRATIVE UPDATES

a. Administrative changes or documentation updates may be required for existing connections. Administrative updates occur when there are updates to the MOU/ISA, authorized POC, FCIO, system owner, and responsible ISO. The current responsible ISO or authorized POC should submit these updates. The requester can also make administrative updates when submitting a modification to an existing connection.

b. The MOU/ISA updates are submitted whenever a new version of an MOU/ISA for the connection is signed or as the result of a substantial change to the scope of the connection.

c. An administrative update is submitted when the responsible ISO for the connection is changed. The old and new responsible ISO's information (name, phone, and e-mail) is required for this update.

d. Authorized POCs are assigned to specific named connections and are authorized to submit RFC for these connections. A listing of authorized POCs is provided to the VA NSOC. Administrative update should be provided anytime there is a modification to the listing of authorized individuals for these specific connections.

## 12. MOU, ISA, and Business Associate Agreement (BAA) and Data Use Agreement (DUA) Requirements

a. An MOU and ISA are required for all external connections where VA sensitive information and data is stored, processed, and transmitted on or by any system, storage media or in any form or format which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. This applies to any information whose improper use or disclosure could adversely affect the ability of the VA to accomplish its mission, and secure proprietary information, and records about individuals requiring protection under various confidentiality provisions such as 38 U.S.C. § 7332, the Privacy Act and the Health Insurance Portability & Accountability Act's (HIPAA) Privacy and Security Rules. MOU/ISAs will be validated annually and documented in RiskVision GRC tool.

b. These requirements not only involve securing VA data and reducing the risk of data being exposed, but also apply to data disclosed to entities outside of the VA system boundary.

c. If VA's business concerns or priorities take precedence over obtaining a signed MOU/ISA at the time of the external connection request, then an approved POAMs accepting risk(s) signed by the appropriate authorities must be submitted with the RFC with appropriate controls documented and in place to protect the data. The POAM must provide a degree of assurance against risk and address all concerns that may come from the security oversight community.

d. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.

e. BAAs are mandated by HIPAA, defined at 45 CFR 160.103, and amended by the Health Information Technology for Economic and Clinical Health Act. BAAs are meant to document a vendor's acknowledgement that it will protect VA's protected health information and will adhere to HIPAA's Privacy, Security and Breach Notification Rules. However, BAAs do not specifically address the security concerns or requirements of an interconnection. Therefore, it is not recommended that VA use a BAA in lieu of an MOU and/or an ISA involving an external connection. VA Handbook 1605.05*, Business Associate Agreements* provides policy and procedures for the establishment and management of BAAs between VA Health Administration facilities and designated Business Associates.

f. DUAs will be implemented to meet Presidential- Congressional- or Federal – mandated actions. The actions may involve a compilation of entities across multiple business industries that must conduct business with the VA whereby the VA and those entities are obligated to conform and meet a compliance deadline. A DUA will be worked out on a case-by-case by the VA Program Office responsible for completing the action and meeting the mandate. If the impact is at a National level, the DUA should be coordinated and processed through the FSS HISD office.

g. All MOUs, ISAs, DUAs, and BAAs will be reviewed and validated each year by the ISO on the anniversary of the final approver's signature and the review entered in the FSS SharePoint site for its entry. Agreements requiring renewal should begin 6 months prior to expiration. The status of expiring agreements associated with external connections will be noted on any RFC involving that agreement.

This page is intentionally blank for the purpose of printing front and back copies.

## APPENDIX A. REFERENCES

a. Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.,* (P.L. 113-283), December 2014;

b. Department of Veterans Affairs Information Security Enhancement Act of 2006, 38 U.S.C. § 5721 *et seq.* (P.L. 109-461);

c. Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules, 45 C.F.R. Parts 160 and 164;

d. Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*;

e. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;

f. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*;

g. IEEE/EIA 12207, *Industry Implementation of International Standard*;

h. Medical Device Isolation Architecture (MDIA), Health Information Security Division;

i. NIST SP 800-12, *Introduction to Computer Security: The NIST Handbook*;

j. NIST SP 800-30, *Guide for Conducting Risk Assessments*;

k. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;

l. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*

m. NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*;

n. NIST SP 800-53A REV 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;

o. NIST SP 800-60*, Guide for Mapping Types of Information and Information Systems to Security Categories, (2 Volumes). Volume 1: Guide, Volume 2: Appendices*;

p. NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*;

q. NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i RSN/802.11i*;

r. NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*;

s. NIST SP 800-121, *Guide to Bluetooth Security*;

t. NIST SP 800-120, *Recommendation for EAP Methods Used in Wireless Network Access Authentication*;

u. Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*;

v. OMB Circular A-130, *Appendix III, Security of Federal Automated Information Resources*;

w. OMB Circular A-130, *Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources*;

x. OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*;

y. OMB Memorandum M-08-26, *Transition from FTS2001 to Network*;

z. OMB Memorandum M-08-27, *Guidance for Trusted Internet Connection (TIC) Compliance*;

aa. VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*;

bb. VA Handbook 1605.05, *Business Associate Agreements*

cc. VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*;

dd. VA Handbook 6500.6, Contract Security;

ee. VA Directive 6004, *Configuration, Change and Release Management Programs*

ff. VA Office of Information Technology Change Management Process Document

gg. Veteran-Focused Integration Process (VIP) Guide: https://vaww.OI&T.va.gov/veteran-focused-integration-process-vip-guide/

## APPENDIX B. TERMS AND DEFINITIONS

1. **External Connection:** An external connection may consists of hardware and/or software that is intended to permit or prevent traversal of traffic that travels between VA and external entities. The following examples of categories of external connections are provided to clarify the definition, but are not to be considered inclusive of all categories:

a. Connections to the Internet intended to provide a variety of Internet-related services (e.g., e-mail or Web access) to a community of VA users or facilities. This category of connection is often called an Internet gateway, firewall, or border router.

b. Remote access services (RAS) intended to provide a community of VA employees a VPN capability to VA computer assets from home or other remote locations. RAS service points are considered VA-authorized arrangements for satisfying remote access needs and are subjected to formal A&A. Unsecured dial-in modem connections, established independently by an individual employee using remote access products on their office personal computer, are not considered RAS service points and are explicitly prohibited by prior VA policy.

2. **External Entity:** Any computing or network resource that is not part of any VA's computing or network infrastructure. For example, any connection to another government agency, vendor, or university network, or use of such an external network, is a connection to an external entity. A VA employee using a computer at the employee's home, or when traveling, to access the VA network via a VPN connection is an external entity because non-VA data communications infrastructures are employed between the employee's off-site computer and VA's internal network.

3. **Other Terms and Definitions:** For other terms and definitions as defined by the VA, reference VA Handbook 6500, Appendix A – Terms and Definitions.

This page is intentionally blank for the purpose of printing front and back copies.

# APPENDIX C. ACRONYM LIST

| Acronym | Definition |
|---|---|
| A&A | Assessment and Authorization |
| ACL | Access Control List |
| ADAS | Associate Deputy Assistant Secretary |
| ATO | Authority To Operate |
| AV | Anti-virus |
| BAA | Business Associate Agreement |
| BPE | Business Partner Extranets |
| BPG | Business partner Gateway |
| CBOC | Community Based Outpatient Clinic |
| CIO | Chief Information Officer |
| CSP | Cloud Service Provider |
| DAS | Deputy Assistant Secretary |
| DCISO | Deputy Chief Information Security Officer |
| DHA | Defense Health Agency |
| DMZ | Demilitarized Zone |
| DNS | Domain Name Service |
| DoD | Department of Defense |
| DUA | Data Use Agreement |
| ECMS | Electronic Contract Management System |
| ECMS | ESCCB Change Management System |
| ESCCB | Enterprise Security Change Control Board |
| ECSIP | Enterprise Cyber Security Infrastructure Project |
| ERF | ESE Registration Form |
| ESE | Enterprise Systems Engineering |
| ESSS | Enterprise Security Solutions Service |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FISO | Facility Information Security Officer |
| FQDN | Fully Qualified Domain Name |
| FTE | Full Time Employee |
| HIPAA | Health Insurance Portability & Accountability Act |
| HISD | Health Information Security Division |
| HTTP | Hypertext Transfer Protocol |
| IP | Internet Protocol |
| IPRM | Information Protection and Risk Management |
| IPS | Intrusion Prevention System |
| ISA | Interconnection Security Agreement |
| ISP | Internet Service Provider |
| ISO | Information Security Officer |
| IT | Information Technology |
| ITOPS | IT Operations and Services |
| LAN | Local Area Network |

| Acronym | Definition |
|---|---|
| MDIA | Medical Device Isolation Architecture |
| MOU | Memorandum of Understanding |
| NCCB | National Change Control Board |
| NCA | National Cemetery Administration |
| NIST | National Institute of Standards and Technology |
| NSD | National Service Desk |
| NSOC | Network and Security Operations Center |
| OI&T | Office of Information and Technology |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| PHI | Protected Health Information |
| PO | Privacy Officer |
| POC | Point of Contact |
| PTA | Privacy Threshold Analysis |
| OCS | Office of Cyber Security |
| OGC | Office of General Counsel |
| OMB | Office of Management and Budget |
| RAS | Remote Access Services |
| RFC | Request for Change |
| ROB | Rules of Behavior |
| S2S | Site to Site |
| sFTP | Secure Files Transfer Protocol |
| SLA | Service Level Agreement |
| SOP | Standard Operating Procedure |
| SP | Special Publication |
| SSH | Secure Shell |
| SSP | System Security Plan |
| TIC | Trusted Internet Connections |
| TRM | Technical Reference Model |
| URL | Unified Resource Locator |
| VA | Department of Veterans Affairs |
| VASI | VA Systems Inventory |
| VBA | Veterans Benefits Administration |
| VHA | Veterans Health Administration |
| VIP | Veteran-focused Integration Process |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WASA | Web Application Security Assessment |