Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6513
Transmittal Sheet
October 12, 2017

SECURE EXTERNAL CONNECTIONS

1. REASON FOR ISSUE: This Directive establishes the Department of Veterans Affairs (VA) policy and responsibilities regarding secure external connections to any VA network infrastructure.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive establishes overarching guidelines and authorizations for managing and securing all of VA's external 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(S): The Office of the Assistant Secretary for Information and Technology (005), Service Delivery Engineering (005OP), Enterprise Systems Engineering (005OP2) is responsible for the content of this Directive.

4. RELATED HANDBOOK: VA Handbook 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 OF VETERANS AFFAIRS:

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

Distribution: Electronic Only

SECURE EXTERNAL CONNECTIONS

1. PURPOSE

a. The purpose of this Directive is to establish Department of Veterans Affairs (VA) policy and to define roles and responsibilities in regard to securing all external connections to the VA network infrastructure. This document also establishes VA policy for the conversion of current and future, inbound and outbound external connections to the VA Trusted Internet Connection (TIC) and One-VA Gateways to ensure compliance with Federal laws, Office of Management and Budget (OMB) mandates, National Institute of Standards and Technology (NIST) guidance and recommendations, 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*.

b. This Directive applies to all VA organizations and information technology (IT) resources, including contracted IT systems and service connections to medical systems and research systems.

2. POLICY

a. VA will have in place a mechanism to identify and continuously monitor all external connections ensuring that these connections meet or exceed the security requirements OMB mandates, guidelines identified in NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, and in support of VA Directive and Handbook 6500.

b. The VA Enterprise Security Change Control Board (ESCCB) will review an external connection request for change (RFC) for compliance with existing laws, regulations, and VA policies; and evaluate those RFCs via an assessment of the security posture and business value of the external connection to VA's mission. The Board voting membership will be comprised of the VA Office of Information and Technology (OIT) operational, security, privacy services, and Veterans Health Administration/National Cemetery Administration/Veterans Benefits Administration representatives, as appropriate.

c. All external connections to VA systems on the internal One-VA Wide Area Network are required to connect through the VA TIC Gateways.

d. All of VA and its external partners will comply with OMB TIC Reference Architecture 2.0 requirements to ensure the continuance and required security of external connections.

e. No modifications will be made to external connections without proper review, assessment, and approval of all appropriate VA organizations as outlined in this Directive and VA Handbook 6513, *Secure External Connections*.

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 Handbook 6513; and

(4) As the overall VA system owner, delegating the daily operational and maintenance system owner 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** (OIT 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 assist in protecting the confidentiality, availability, and integrity 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.

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 Veterans or their beneficiaries is managed in accordance with Federal privacy laws 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 the interests of program and project management.

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

(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 within 10 business days 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 the VA information system owners in:

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

(2) Documenting all external connections in OIT 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 and Local Area Network (WAN/LAN) 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 Network Device Naming and Tracking Standards; and

(3) Labeling or ensuring all external connections are labeled in communication closets at VA facilities or leased space, and according to the VA Network Device Naming and Tracking Standards.

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 Sections 508 and 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 OIT 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) where required;

(2) Determining whether any new RFC involving PII/PHI require a either Privacy Impact Assessment (PIA) or Privacy Threshold Analysis;

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

(4) 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 Handbook 6513. They do so by coordinating and collaborating with OIT officials within their areas of responsibility regarding external connections.

4. REFERENCES

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

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

c. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

d. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

e. FISMA 11-01 Announcing Trusted Internet Connections (TIC) Reference Architecture v2.0

f. NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology* Systems

g. OMB Circular A-130, Appendix Ill, Security of Federal Automated Information Resources

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

i. OMB Memorandum M-08-26, Transition from FTS200I to Networx

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

k. Trusted Internet Connections (TIC) Reference Architecture Document Version 2.0

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

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

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

5. ACRONYMS and ABBREVIATIONS

Acronym	Definition
CIO	Chief Information Officer
DAS	Deputy Assistant Secretary
ESCCB	Enterprise Security Change Control Board
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
ITOPS	IT Operations and Services
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NSOC	Network Security Operations Center
OIT	Office of Information & Technology
OMB	Office of Management and Budget
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RFC	Request for Change
TIC	Trusted Internet Connections
VA	Department of Veterans Affairs