Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6513
Transmittal Sheet
July 16, 2010

SECURE EXTERNAL CONNECTIONS

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

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Directive establishes VA policy, roles and responsibilities regarding the secure establishment of external connections to the VA network infrastructure. This document also establishes VA policy for the conversion of current external connections to the One-VA Internet Gateway, as appropriate, both inbound and outbound, to ensure compliance with Federal laws, Office of Management and Budget (OMB) mandates, National Institute of Standards and Technology (NIST) recommendations and VA Directive and Handbook 6500, *Information Security Program.*

3. RESPONSIBLE OFFICE(S): The Office of the Assistant Secretary for Information and Technology (005), Office of Information Protection and Risk Management (005R), is responsible for the content of this Directive.

4. RELATED HANDBOOK: Handbook is under development.

5. RESCISSIONS: None.

CERTIFIED BY:

/s/
Roger W. Baker
Assistant Secretary for
Information and Technology

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Roger W. Baker
Assistant Secretary for
Information and Technology

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 regards to securing external connections to the VA network infrastructure. This document also establishes VA policy for the conversion of current external connections, as appropriate, to the One-VA Internet Gateways to ensure compliance with Federal laws, Office of Management and Budget (OMB) mandates, National Institute of Standards and Technology (NIST) recommendations and VA Directive and Handbook 6500, *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 identify and continuously monitor all external connections ensuring that these connections meet or exceed the security requirement in NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems and in support of VA Directive and Handbook 6500, *Information Security Program*.

b. The VA Enterprise Security Change Control Board (ESCCB) voting membership will be composed of the VA Office of Information and Technology (OI&T) operational, security, privacy services, and Veterans Health Administration/National Cemetery Administration/Veterans Benefits Administration (VHA/NCA/VBA) representatives, as appropriate. The Board will review external connection change requests (CRs) for compliance with existing laws, regulations, and VA policies and evaluate those CRs via an assessment of the security posture and business value of the external connection to VA's mission.

c. VA will transition all external connections to the One-VA Internet Gateway when and where possible. If any external connection cannot be transitioned because of bandwidth limitations, time sensitive transmissions, or other reasons, justification must be submitted to the ESCCB.

d. VA will comply with critical OMB Trusted Internet Connection (TIC) technical capabilities to ensure the continuance, reduction, and consolidation of 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 this Directive; 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 (DAS) for Information Protection and Risk Management (IPRM) under the IT Single Authority, the VA CIO has created the DAS for IPRM. The DAS for IPRM has authority over the VA enterprise cyber security budget and is responsible for ensuring external connections are properly identified, inventoried and securely managed. The DAS for IPRM also serves as the VA Chief Information Security Officer (CISO).

d. Associate Deputy Assistant Secretary (ADAS) for Cyber Security is responsible for:

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

(2) Reviewing VA information security policies and procedures related to information security that are under the management and oversight of other Department organizations; and

(3) Ensuring that all Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA) clearly define the security controls implemented to protect the confidentiality, availability, and integrity of VA information processed, stored, or transmitted between interconnecting parties.

e. Associate Deputy Assistant Secretary (ADAS) of Privacy and Records Management is responsible for being a voting member of the ESCCB to ensure all external connections are in accordance with Federal privacy laws and VA policies.

f. Deputy Assistant Secretary (DAS) for Field Operations is responsible for implementing the policies outlined in this Directive and as provided in a forthcoming handbook.

g Director, Field Security Operations is responsible for ensuring organizational elements are provided the resources and tools for the implementation and management of security practices regarding external connections.

h. VA ESCCB is responsible for:

(1) Ensuring all proposed external connection changes to VA network resources are reviewed to ensure security and privacy viability within 10 business days after complete and proper documentation has been submitted;

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

(3) Ensuring external connection compliance with enterprise VA policies and procedures and the rules outlined in VA National Rules of Behavior;

(4) Ensuring the timely processing and review of all external connection CRs;

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

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

i. VA Network and Security Operations Center (VA-NSOC) is responsible for:

(1) Evaluating external connection CRs for impact on network and gateway bandwidth and IP address/port security settings and making recommendations to the ESCCB voting membership;

(2) Participating as a voting member of the ESCCB;

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

(4) Monitoring of all external connections for compliance with existing federal laws and VA policies.

j. Under Secretaries, Assistant Secretaries, and Other Key Officials are responsible for ensuring compliance with this directive within their respective

Administrations, Staff Organizations, and Program Offices by coordinating and collaborating with OI&T officials within their area of responsibility regarding external connections.

k. 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, daily operations, maintenance, and implantation 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 ISAs and MOUs as required, to establish the binding agreements and implementation of technical security controls between the external connecting parties to protect the confidentiality, availability, and integrity of VA information processed, stored, or transmitted between interconnecting parties as approved by the ESCCB.

.

l. Facility CIOs and System Administrators are responsible for:

(1) Assisting and coordinating with the VA information system owners in reporting all external connections to VA information systems;

(2) Assisting and coordinating with VA information system owners in creating, maintaining and submitting of external connection CRs for approval to the ESCCB. ISAs and MOUs are required to establish the binding agreements and assurance necessary for the implementation of the appropriate security controls (management, operational, and technical) between the external connecting parties to protect the confidentiality, availability, and integrity of VA information processed, stored, or transmitted between interconnecting parties as approved by the ESCCB.

m. Facility Information Security Officers (ISOs), Information Security Liaisons and Privacy Officers (POs) are responsible for:

(1) Assisting and coordinating with the VA information system owners in reporting all external connections to VA information systems;

(2) Assisting and coordinating with VA information system owners in creating, maintaining and submitting external connection CRs for approval to the ESCCB. ISAs and MOUs are required to establish the binding agreements and assurance necessary for the implementation of the appropriate security controls (management, operational, and technical) between the external connecting parties to protect the confidentiality,

availability, and integrity of VA information processed, stored, or transmitted between interconnecting parties as approved by the ESCCB.

4. REFERENCES:

a. Federal Information Security Management Act (FISMA) (P.L. 107-347, Title III), December 2002;

b. 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. Office of Management and Budget (OMB) Circular A-130, Appendix Ill, *Security of Federal Automated Information Resources;*

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

g. OMB Memorandum M-08-26, *Transition from FTS200I to Networx*;

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

i. VA Directive and Handbook 6500, *Information Security Program.*

5. ACRONYMS and ABBREVIATIONS:

a. ClO - Chief Information Officer

b. CISO - Chief Information Security Officer (CISO)

c. CR - Change Request

d. DAS - Deputy Assistant Secretary

e. ADAS - Associate Deputy Assistant Secretary

f. DCISO - Deputy, Chief Information Security Officer

c. ESCCB - Enterprise Security Change Control Board

d. FISMA - Federal Information Security Management Act

e. IPRM - Information Protection and Risk Management

g. ISA - Interconnection Security Agreement, same as (SIA)

h. IT - Information Technology

i. LOB - Line of Business

j. MOU - Memorandum of Understanding

k. NIST - National Institute of Standards and Technology

l. OI&T - Office of Information & Technology

m. OMB - Office of Management and Budget

n. TIC - Trusted Internet Connections

o. VA - Department of Veterans Affairs

p. VA - NSOC - Department of Veterans Affairs, Network Security Operations Center