Department of Veterans Affairs
Washington, DC 20420

VA DIRECTIVE 6212
Transmittal Sheet
September **21, 2000**

SECURITY OF EXTERNAL ELECTRONIC CONNECTIONS

1. REASON FOR ISSUE: This directive describes the minimum security requirements for Department of Veterans Affairs (VA) external electronic connections.

2. **SUMMARY OF CONTENTS**

a. External electronic connections, hereinafter referred to as "connections" shall incorporate adequate controls to safeguard VA information systems and data. Controls described in this directive are VA standards for securing connections based on existing threats and current technological countermeasures.

b. Connections shall be accredited prior to use. Compliance with these controls is required before connections are certified and accredited for use. Connections shall be periodically and independently reviewed by an organization other than that which sponsors the use and administration of the connection.

3. RESPONSIBLE OFFICE: The Technology Integration Service (045A2), Office of the Assistant Secretary for Information and Technology, is responsible for the material contained in this directive.

4. RELATED HANDBOOK: None.

5. RESCISSION: None.

CERTIFIED BY:

Robert P. Bubniak

Acting Principal Deputy Assistant Secretary for Information and Technology

BY DIRECTION OF THE ACTING SECRETARY OF VETERANS AFFAIRS:

Robert P. Bubniak

Acting Principal Deputy Assistant Secretary for Information and Technology

Distribution: RPC: 6002
FD

SECURITY OF EXTERNAL ELECTRONIC CONNECTIONS

1. PURPOSE AND SCOPE

a. VA has deployed many connections between VA computer systems and external entities. These connections consist of hardware and software that are expected to permit or prevent traversal of traffic that travels between VA and external entities. A secure connection consists of hardware, software, and associated physical, procedural, technical, and personnel security controls.

b. The purpose of this directive is to describe the minimum security requirements for VA's connections. Controls outlined in this directive are VA standards for secure connections, based on existing threats and current technological countermeasures.

c. This directive applies to all VA organizations that install, operate, manage, and control connections.

2. POLICY

a. Connections shall incorporate adequate controls to safeguard VA information systems and data. At a minimum, all connections shall conform to the following specifications.

(1) Configuration and Installation.

(a) Activate the minimum set of operating system services to support firewall operation. Activate no other operating system services.

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

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

(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 Domain Name Systems (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) Be installed in locations that are physically secure from tampering.

(2) Access Management

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

(b) Implement a “deny all services except those specifically permitted” design policy.

(c) Implement a strong authentication technique for administrative log-in to permit secure remote log-in by the authorized system administrator.

(d) Support integration of external authentication mechanisms, such as the Lightweight Directory Access Protocol (LDAP), and Remote Authentication Dial-In User Service (RADIUS).

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

(f) 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.

(3) Auditing and Filtering

(a) Log access to and through the firewall.

(b) Capture log-in attempts by authorized and unauthorized users.

(c) Employ a flexible, user-friendly IP-filtering language that is easy to program and can filter on a wide variety of attributes, including source and destination IP addresses, protocol types, port numbers, and inbound and outbound interfaces.

(d) Concentrate, filter, and log dial-in access.

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

(f) Support third-party products for log analysis and data reduction.

(4) Notification

(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) Future 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.

b. Connections must be accredited prior to use.

(1) Administrations and staff offices will implement procedures necessary to ensure that connections under their purview are accredited.

(2) Prior to accreditation, Administrations and staff offices will ensure that connections are certified to current standards issued by the National Institute of Standards and Technology, the National Security Agency, and other Federal-wide authorities that regulate information security.

(3) Accreditation requires authorization for processing by the management official responsible for the protected asset. Typically, this official is the facility director.

c. Connections shall be periodically and independently reviewed by an organization other than that which sponsors the use and administration of the connection. These reviews will be conducted when there is significant change to the protected asset. These reviews will ensure that connections remain in compliance with the minimum security standards outlined in this directive, and will ensure that risk assessments, security plans, and contingency plans remain current.

3. RESPONSIBILITIES

a. **Secretary of Veterans Affairs.** The Secretary has designated the Department's Chief Information Officer as the senior agency official responsible for the Department's information technology programs.

b. **Chief Information Officer.** The Department's Chief Information Officer (CIO) is responsible for the effective and secure control of VA's connections. The CIO, having established this directive for the security of connections, will monitor, review, and evaluate compliance with this directive.

c. Administration Heads, Assistant Secretaries, and Other Key Officials. These officials will ensure compliance with this directive within their respective Administrations and staff offices. These officials will establish necessary procedures to certify, accredit, and review connections that are installed, operated, managed, and controlled within their respective Administrations and staff offices.

4. **REFERENCE:** VA Directive 6210, Automated Information Systems Security.

5. DEFINITIONS

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

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

(2) Remote access services (RAS) intended to provide a community of VA employees dial-in 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 certification and accreditation. Unsecure 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.

b. **External Entity.** Any computing or network resource that is not entirely part of the VA's computing or network resources. For example, any connection to a government or university network apart from VA, 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 dial-up 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.