U.S. Customs and Border Protection

Attachment U

Network Security Practices

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	July 27. 2009	Initial CBP 1400-05D release is based solely on existing 1400-05C, Version 2.1 appendices which were found to be unrelated to existing DHS 4300A, Version 6.1.1 attachments. The policy content of this attachment is exactly the same as the 1400-05C, Version 2.1 appendix. It is now presented in the attachment format.
2.0	December 21, 2010	No Changes

CONTENTS

Hardening of routers and switches is based on NSA hardening guidelines. As CBP-specific hardened configurations are developed, they will be compiled into network engineering operational documentation.

1.0 INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDSs) detect inappropriate, incorrect, or malicious activity and are deployed on hosts and networks. CBP employs both host-based and network IDSs. These devices work closely with firewalls to identify break-in attempts and defeat intruders.

1. As with other network devices physical access to IDS devices must be restricted to authorized users only.
2. For software-based IDSs, administrators must ensure compliance with licensing.
3. IDS devices must be monitored on a daily basis and data reviewed by assigned SAs and security personnel for suspicious activity.
4. IDS source code must be stored in off-line storage.

2.0 COMSEC

Communications Security (COMSEC) is discussed in the *CBP National Security Systems Handbook* for classified systems and networks

3.0 GENERAL COMMUNICATIONS DEVICE STANDARDS

For all communications devices, network operations staff must:

1. Maintain validated lists of all Media Access Control (MAC) addresses, Access Control Lists (ACLs), and IP addresses.
2. Assign static IP addresses to network devices.
3. Restrict physical access to communications devices.
4. Enforce password protection for devices.
5. Configure strong passwords for network devices in accordance with CBP policy (eliminate all default passwords).
6. Ensure password text file is encrypted on device.

4.0 GENERAL DEVICE MAINTENANCE

All processes and procedures for general device management must be documented in operations manuals, kept current, and made available to authorized users only. Changes must adhere to change management processes in accordance with the CBP Change Control Board (CCB). Device management includes documentation of the following procedures:

1. Upgrades and patches – testing, configuration control, rollout strategy.
2. Procedures for planned maintenance-windows procedures.
3. Emergency maintenance procedures.
4. Use of remote access for device management.
5. Ports, services and interfaces – protection–enabled, unused-disabled.
6. Warning Banners.
7. Network Topology Drawings – currency and accuracy.
8. Account lockout.
9. Unattended time-out.
10. Log file configuration and protection.

5.0 ACCESS CONTROL LISTS

All processes and procedures for access control must be documented in operations manuals, kept current, and made available to authorized users only. Such documentation includes the following procedures:

1. Traffic filtering.
2. IP address spoof protection/exploits protection.
3. Configuration loading and maintenance.
4. Router change management.
5. Syslog.

6.0 NETWORK AND NETWORK DEVICES

Router configurations and site-specific instructions are contained in local Site Operations Manuals. However, the following practices apply to all CBP networks and network devices. (Other detailed security configuration guidance for network devices is available in NSA publications.)

6.1 Routers and Router Tables

Processes and procedures for routers and router tables must be documented, in operations manuals, kept current, and made available to authorized users only. NSA hardening guidelines will be used to standardize configurations for routers and switches. Documentation of the following must be included:

1. Access Control List (ACL) configurations –updates of allowed IP addresses table.
2. Verify ACL lists with authorized IP user base.
3. Key management plan – to include key exchange, time expiration, and key compromise procedures.
4. User account access level requirements – assigned lowest privilege level to perform duties.
5. Review site policy to verify authorized user list is filed with security office.
6. No user accounts permitted without passwords.
7. No group accounts permitted.
8. Remote access via username command to create accounts.
9. All access points (e.g., console, auxiliary, teletype) have password-enabled access.
10. Use of Type 5 encryption (MD5 hash algorithm) for passwords vs. proprietary – *enable secret* vs. *enable password* functionality.
11. Use service password-encryption option to hide password display on the screen.

6.2 Router and Switch Configurations

CBP routers and switches must be configured to the CBP standard.

6.3 Network Management

Network Management documentation must include the following topics.

1. Eliminate default community names such as PUBLIC

2. Use different community names for access types (e.g., read-only, read, and write)

3. Use secure tunneling technology, such as IPSEC, to secure traffic between net management center workstations and managed devices

4. Set up security alarms for defined violations and categorized by severity of alarm

5. Maintain audit trail logs of logons, transactions, and other defined activities

6.4 Virtual Private Networks (VPN)

All VPN connections must be fully documented to include the following technical information:

1. Tunnel termination location

2. External security enclaves/domains – management agreements, ISAs, etc.

3. IDS/no IDS for VPN

6.5 Domain Name System (DNS)

As CBP migrates to new technologies such as Active Directory, the following components and procedures for the DNS must be documented, kept current and made available to authorized users only:

1. De-Militarized Zone (DMZ) configuration

2. Eliminate **blind zone transfers** (unknown DNS servers) by restricting zone transfers to and from only certain authorized and authenticated IP addresses.

3. Remote updates or changes to the DNS server will be accomplished with only the most approved version of SSH or equivalent encrypted connection. The preferred method for making DNS updates is directly through the local DNS server's console.

4. Deploy only the latest, approved version of BIND.

5. Enable DNS query logging for logging critical DNS messages.

6. Ensure that latest patches and versions are implemented in accordance with applicable CSIRC vulnerability notices.

7. Provide reverse look-up capability for any zone for which the DNS server is authoritative.

6.6 Firewalls

All firewall processes and procedures must be fully documented to include the following technical information:

1. Physical access to firewalls shall be restricted to authorized personnel only.

2. Strong identification and authentication shall be implemented for administration of the firewalls.

3. Remote maintenance paths to the firewalls shall be encrypted.

4. Quarterly testing of the firewalls shall be completed to ensure the firewall configuration is correct and unauthorized modifications have not occurred.

5. Firewalls shall be configured and maintained in accordance with CBP-defined procedures.

6. Unauthorized services and their associated ports shall be disabled, as specified by CBP hardening guidelines and approved device configurations.

7. All firewalls must be located in a physically secure area.

8. Firewalls and gateways must be configured to prohibit any Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) service that is not explicitly permitted by the CISO.

9. All firewall systems must enable an audit capability to monitor operations and to support investigations of real or perceived violations of local security policy.

10. All firewall systems will provide an intrusion detection capability, either as an integral part of the firewall or through an add-on of a third-party product. The program will provide for a scalable response to attacks and must be capable of remote notification. An alert will be sent from the firewall to the CSIRC.

11. Application gateways will be used as a firewall component to protect applications where the client or server resides on an external network. This provision may be waived for non-standard applications where a proxy application is not available or if the application provides user-to-user encryption.

12. Screening routers, if used as a firewall component, must have the capability to filter based upon TCP and UDP ports as well as the IP addresses and incoming network interfaces. It is not recommended that a screening router be the sole segment of a firewall system; rather, it will form a portion of the security features.

13. Only required services will be permitted to pass through a firewall. Permitted services will be documented to include (where applicable):

    a. Service allowed including TCP or UDP port number

    b. Description of the service

    c. Business case necessitating the service

d. Technical description of internal security controls associated with the service

14. Inbound filtering will be performed to exclude or reject all data packets that have an internal host source local address.

15. Inbound services are prohibited unless a valid business case is presented for approval by the CISO, which includes technical documentation of the security controls to be used for such services. Inbound services will provide strong authentication using one-time or session passwords, challenge and response protocols, digital signatures, CBP-approved encryption protocols or other security measures approved for use in the CBP network environment.

16. All servers made available to the public or to the World-Wide-Web (WWW), will be located outside of the firewall perimeter or in the De-Militarized Zone (DMZ).

17. User accounts must not be installed on externally addressable systems.