

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Security Manual
Chapter:	Security Testing
Current Effective Date:	6/15/05
Revision History:	
Original Effective Date:	

Purpose

To establish the security testing requirements for the Department of Health and Human Services (DHHS) Information Technology Services (ITS) and Physical Infrastructure.

Policy

Security testing shall be performed on a periodic basis to ensure that information resources are adequately protected. The security testing policy applies to all systems/applications, the network and the physical infrastructure to evaluate the effectiveness of the security measures and controls implemented.

Roles and Responsibilities

The DHHS Privacy and Security Office (PSO) shall develop standards, enterprise-wide procedures, and guidelines for security testing.

The Division of Information Resources Management (DIRM) working with the DHHS PSO shall ensure that security testing is performed on all DHHS systems/applications, the network, and the DHHS Physical Infrastructure.

The DHHS Divisions/Offices shall be notified of any vulnerabilities found during testing and shall review and implement controls to minimize the risk associated with these vulnerabilities.

Implementation

IS Security testing is performed to protect information from unauthorized modification, loss of use, disclosure, or other threats arising from human or systems-generated activities, malicious or otherwise. Network security testing is performed primarily to identify potential vulnerabilities and remediate them before they affect ITS operations. Physical security testing primarily focuses on the adequacy of internal/perimeter access controls.

Policy implementation shall be based upon the use of management-approved security standards and best practices. The following paragraphs specify the IS Security Testing requirements.

1. *Developing a Security Test Strategy.* The DHHS PSO shall develop a comprehensive test strategy that tests the security of all physical, network and ITS components.
2. *General Security Test and Evaluation (ST&E) Process.* The DHHS PSO shall develop a process that identifies the security test requirements, develops security test plans and procedures, identifies the proper tools for testing, enables testing, evaluates the results, and makes recommendations for improvement.
3. *Scheduling Security Tests.* Security testing shall be integrated into the workflow as a normal part of the duties of security administrators to evaluate system security mechanisms and validate that systems are operating properly. The DHHS Divisions/Offices or their designated affiliate(s) responsible for the administration of the ITS network, LAN and systems, shall work with the DHHS PSO and/or DIRM to prioritize operational system testing activities according to system criticality, testing costs, and the benefits that testing will provide. Security testing of all sensitive and critical information systems shall be performed at least once per year. Likewise, physical security testing and network security testing shall be performed at least once per year.
4. *Types of Security Tests.* The DHHS Divisions/Offices or their designated affiliate(s) responsible for the administration of their ITS network, LAN and systems, shall work with the DHHS PSO and/or DIRM to perform adequate testing to ensure adequate security is being provided in the operating environment. Typically, a combination of several types of security testing techniques is needed to provide a comprehensive assessment of the operational environment. Tests that shall be included in overall security testing strategy for each DHHS Division/Offices shall include:
 - A. Network Mapping – Network mapping involves using a port scanner to identify all active hosts connected to an organization’s network, network services operating on those hosts (e.g., file transfer protocol and hypertext transfer protocol), and the specific application running the identified service. The result of the scan is a comprehensive list of all active hosts and services operating in the address space scanned by the port scanning tool.
 - B. Vulnerability Scanning – Vulnerability scanners identify not just the hosts and open ports but any associated vulnerabilities automatically instead of relying on human interpretation of the results. Most vulnerability scanners probe for a finite number of problems and attempt to provide information on mitigating discovered vulnerabilities. Vulnerability scanners can be either network scanners or host scanners.

- C. Penetration Testing – Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.
 - D. Password Cracking – Password cracking programs can be used to identify weak password usage.
 - E. File Integrity Checkers – A file integrity checker computes and stores a checksum for every file to be protected and establishes a database of the checksums. It provides a tool for system administrators to recognize when changes were made to files, particularly unauthorized changes.
 - F. Anti-Virus and Malicious Code Detection – Anti-Virus software programs shall be installed to protect both the network and systems in the operating environment.
 - G. Modem Security – Software programs (war dialing) that detect the use of unauthorized modems that might be used to bypass existing security measures.
 - H. Physical Access Testing – Physical access testing (both perimeter and internal) shall be performed on a periodic basis (recommend every three (3) months). Likewise, physical access testing of the ITS production and network environment shall be performed at similar intervals.
5. *Log Reviews.* Various system logs (e.g., firewall logs, IDS logs, server logs) can be used to identify deviations from security policy. In conjunction with security testing, log review and analysis will provide a more comprehensive evaluation of the operational environment. The DHHS Divisions/Offices or their designated affiliate(s) responsible for the administration of their ITS network, LAN and systems shall work with the DHHS PSO and/or DIRM to perform this evaluation.
6. *Recommending Security Enhancements.* Following Security Testing and Evaluation (ST&E), all DHHS Divisions/Offices shall consider the recommendations made for improving security and set priorities to keep the risk within an acceptable range.

Enforcement

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS Security Officer (DHHS.Security@ncmail.net). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#)

Exceptions

Any exceptions to this policy will require written authorization. Exceptions granted will be issued a policy waiver for a defined period of time. Requests for exceptions to this policy should be addressed to the Director of the Division of Information Resource Management (DIRM). The waiver request will be processed in accordance with the DHHS [ITS Waiver and Appeals Policy](#).