Department of Homeland Security
Management Directive System
MD Number: 4900

INDIVIDUAL USE AND OPERATION OF DHS INFORMATION SYSTEMS/ COMPUTERS

1. Purpose

This directive establishes the Department of Homeland Security (DHS) policy for the use and operation of DHS information systems and computers by individual users.

2. Scope

This directive applies to all individual users of DHS owned or provided information systems, including personal and desktop computers. This document provides the minimum DHS level of information systems/computer security requirements. Components or relying parties (data owners) may impose more stringent security requirements for the protection of their compartmental data and infrastructure.

3. Authorities

This directive is governed by numerous Public Laws, Executive Orders, Presidential Decision Directives, Federal Regulations, DHS Management Directives, and Circulars, such as:

A. Public Law 100-235, Computer Security Act of 1987, January 1988.

B. Public Law 107-296, Homeland Security Act of 2002.

C. E Government Act, Title III, Federal Information Security Management Act (FISMA), December, 2002.

D. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.

E. Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.

F. Privacy Act of 1974, As Amended. 5 United States Code (U.S.C) 552a, Public Law 93-579, Washington, DC July 14, 1987.

G. Executive Order (E.O.) 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001.

H. Presidential Decision Directive (PDD) 63, *Critical Information Protection*, May 1998.

I. 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.

J. Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.

K. DHS Management Directive No. 4300, IT System Security and publications.

L. DHS Management Directive No. 4100, National Wireless Management Office Policy and Operations.

M. DHS Management Directive No. 4500, DHS Email Usage.

N. DHS Management Directive No. 4400, DHS Web and Information Systems Policy.

O. The applicable security authorities and regulations that pertain to Federal Information Processing Systems (FIPS) as defined by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

4. Definitions

A. ***Information Systems:*** Include, but are not limited to, information technology, access to government networks, and transverse of government networks to access public networks such as the Internet.

B. ***Information Technology:*** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information. IT includes, but is not limited to, desktop computers, personal computers, laptops, handheld computers, Personal Digital Assistants (PDAs), related peripheral equipment and software.

C. ***Information Assurance:*** The overall effort taken by an organization to ensure the availability, authentication, confidentiality, integrity, and non-repudiation of its sensitive data and the supporting information systems infrastructure. IA includes the protection of information and information systems against unauthorized access or unauthorized modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users.

D. Additional definitions for this directive are set forth in the National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009 June 5, 1992.

5. Responsibilities

A. ***The Under Secretary for Management***, through the DHS Chief Information Officer, shall be responsible for all aspects of this directive.

B. ***The DHS Chief Information Officer (CIO)*** shall:

1. Provide procedural guidance regarding this policy.

2. Ensure effective, secure operation of all DHS information technology resources, including computers, data storage, and network devices.

3. Make available copies of this policy on the intranet to ensure that all users of DHS information systems are made aware of their responsibilities and liabilities when using such systems.

4. Ensure that all DHS Information Systems are operated in accordance with applicable regulations and directives.

C. ***DHS supervisors*** shall:

1. Provide employees, contractors and other personnel within their area of responsibility with a copy of this policy and ensure proper understanding of the policy.

2. Ensure that all personnel using information systems sign the User Agreement shown in Attachment A of this document.

3. Take appropriate disciplinary and other actions when notified of non-compliance with the policy.

6. Policy and Procedures

A. ***Policy.*** It is the policy of DHS that the individual computer user (user of information systems) is the primary responsibility for protection of DHS information. Organizational information assurance efforts are monitored as part of the overall DHS IT Security Program.

B. ***Procedures and Mandatory Requirements***.

All DHS individual users of DHS information systems are responsible for complying with the requirements listed below. Exceptions may be granted in the case of law enforcement entities using systems exclusively for forensic analysis of electronic crimes. Such exceptions must be submitted in writing to the DHS CIO.

1. ***Identification and Authentication***. All users must be properly identified and verified prior to being granted access to government computers and network services. At a minimum, a domain unique user name and properly formatted password will be employed. The password must be a minimum of eight characters in length and must contain both alpha and numeric characters. Default passwords should be immediately changed when assigned. Users must never reveal their passwords to anyone. Passwords should not be constructed from obvious personal data, i.e. social security number, telephone numbers, relative's names, pet's name, etc.

Strong identification and authentication (I&A) technology should be considered to replace user ID/password schemes. Strong I&A techniques include one time passwords (OTP) (tokens), digital certificates, and smart cards.

2. ***Training***. All users will complete a government approved security training course prior to being given access to government information systems. This training course must address the security aspects unique to the particular system as well as the functionality of desktop hardware and standard suite of software applications.

3. ***User Agreements***. All users must read, sign and provide to their IT Support organization, a user agreement prior to being granted access to DHS systems. The document will delineate the user's specific responsibilities and duties of individual users. An example of this type of agreement is provided in Appendix A and is posted on the DHS Intranet.

4. ***Logon Banner.*** Prior to granting access to DHS information systems, each user must read and acknowledge a logon banner that describes the conditions under which usage is granted (official business) and a statement that use of the system constitutes consent for monitoring of the system. This screen will provide an overt and auditable way for the user to either accept or reject the conditions of system use. A copy of a Logon Banner is provided in Appendix B.

5. ***Software Licensing and Liabilities***. Users must not duplicate or remove copyrighted software (except for backup purpose and according to manufacturer's guidance) from government equipment without the expressed written permission of the System Administrator or Information Systems Security Officer (ISSO). The individual will be personally liable for any software copyright violations committed on government systems under their control.

6. ***Non-government Software***. Users must not install software (commercial, shareware, or freeware) of any type on government information systems without the expressed permission of the System Administrator or ISSO. All software must be approved by the appropriate DHS configuration management process before installation on DHS information systems.

7. ***Acknowledgement to Monitor***. The use of government furnished equipment and information systems constitutes the consent to monitoring and auditing of the use of the equipment/systems at all times. Monitoring includes the tracking of transactions within DHS networks and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media. Users must understand that there is no expectation of privacy when using or storing data on government information systems.

8. ***Classified Processing***. Users must not process classified information on any DHS system not specifically approved and marked for the appropriate level of classified processing. Any discovery of inadvertent or unapproved classified processing on non-classified systems will be reported to the ISSO so the effected system can be isolated and sanitized. Under no circumstances will classified information be processed or stored on non-government computers or storage media except as provided by the National Security Industrial Security program. The use of privately owned (personal) computers to process or store classified information is specifically prohibited.

9. ***Physical Security***. Users will not remove DHS computer systems or software from Government facilities without expressed permission of the ISSO or equipment custodian. Portable equipment such as laptop computers or Personal Digital Assistants (PDAs) will be accounted for with a property pass prior to removal from Government facilities. DHS Organizational Elements may request a waiver to the 'property pass' requirement if implementation causes an undue burden and can be substantiated. Users are responsible for providing adequate physical security protection of portable equipment when outside Government facilities and keeping these items under their exclusive control.

10. ***Protection of Data***. Users will protect storage magnetic media in accordance with the highest level of data sensitivity contained. Whenever possible, stored data will be encrypted on removable media and in portable devices when not in Government facilities.

11. ***Reporting Requirements***. Users will promptly report to the Organizational Element/ Directorate ISSO any suspicious activity, malicious code, or perceived compromise effecting DHS computer systems or networks. Any loss, theft, or damage to computer systems must be promptly documented and reported to the ISSO and equipment custodian.

12. ***Electronic mail (E-mail)***. The government e-mail system is provided for the conduct of official DHS business. However, limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of network services. Users are prohibited from sending e-mail or enclosures that are obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable. As technology becomes available, users will digitally sign and encrypt all official e-mail containing sensitive data. Under no circumstances will Government e-mail systems be used to foster commercial interests or individual profit. Users must comply with the DHS MD No. 4500, Email Usage policy and DHS MD No. 4600, Personal Use of Government Office Equipment policy.

13. ***Use of Internet***. Accessing Internet resources is for official use only, including research. However, limited personal use is authorized as long as this use does not interfere with official duties or cause degradation of network services. Access of inappropriate sites is prohibited. These locations include sites that are obscene, hateful, harmful, malicious, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable. As technology becomes available, these offensive Web sites will be inaccessible. However, access to unauthorized sites (i.e. child pornography/hacker sites) for investigative purposes by criminal investigators and criminal research specialists may be allowed for investigative purposes only. Access to these sites for such investigative purposes must be done with a stand-alone system explicitly stood up for investigative purposes. Users must report to IT Security staff sites inadvertently accessed that should be blocked. Under no circumstances will access to the Internet be used to foster commercial interests or individual profit. Users must comply with the DHS MD No. 4400, Web and Information Systems policy and DHS MD No. 4600, Personal Use of Government Office Equipment policy.

14. ***Remote Access***. In order to improve employee productivity while away from government facilities, and in keeping with Federal telecommuting guidance, a secure remote access capability will be implemented within DHS. Users are required to protect dial-in telephone numbers and Internet access addresses as well as passwords. As technology becomes available within DHS, strong Identification & Authentication and encryption controls will be introduced into the remote access capability.

Government owned equipment is strongly recommended when remotely accessing DHS network resources. However, if personal equipment is used, the user must employ virus protection methods that are FIPS Certified and all other connections to untrusted networks (i.e. the Internet) must be terminated prior to remotely accessing the DHS networks.

15. ***Access Privileges***. Each user is granted specific access privileges based on security clearance and need to know. Under no circumstances will

users attempt to access accounts or data stores that are not expressly authorized to them. This includes, but is not limited to, gaining administrative privileges on local or network devices.

Users are responsible for contacting the ISSO and system administrator when their job position no longer requires access to specific devices or data stores.

16. ***User Accounts***. User accounts are assigned to specific individuals. Users are prohibited from allowing others to use their account and from accessing other users' accounts. Users are individually accountable for all actions under their credentials.

17. ***Security Screen Savers***. Unless specifically authorized in writing by the System Administrator, users will log off government systems when leaving the area unattended for extended periods (overnight). Password protected screen savers or active account locking mechanisms requiring re-typing the password are required, based on a given time of system inactivity. This length of time (usually about 15 minutes) will be established via local security policy.

C. ***Questions or Concerns Regarding the Process:*** Any questions or concerns regarding this directive should be addressed to the Office of the DHS CIO.