

Issue Date: 03/01/2003

DHS WEB (INTERNET INTRANET, AND EXTRANET INFORMATION) AND INFORMATION SYSTEMS

I. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding DHS web (Internet, Intranet, and Extranet) and Information Systems.

II. Scope

- A. This directive applies to all DHS organizational elements.
- B. The scope of this directive is limited to the use and management of DHS Web information and associated systems where the intent is to make information available to the public or to a general audience within DHS. It does not pertain to Special Use Applications that happen to use the Web as all or part of their communication network.

III. Authorities

This directive is governed by numerous Public Laws and Authorities, such as:

- A. Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) of 2002.
- B. Public Law 104-106.
- C. 5 U.S.C. 552a.
- D. Section 508 of the Rehabilitation Act of 1973 and implementing policy and guidance.
- E. The following regulations and documents regarding the Privacy Act:
 - 1. Electronic Communications Privacy Act of 1986.

2. Computer Matching and Privacy Protection Act of 1988.
3. Paperwork Reduction Act of 1995.
4. Children's Online Privacy Protection Act of 1998.
5. OMB Circular No. A-130, Management of Federal Information Resources
6. OMB Memorandum 99-05, Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records".
7. OMB Memorandum 99-18, Privacy Policies on Federal Web Sites.
8. OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Websites.
9. Letter from John Spotila to Roger Baker, clarification of OMB Cookies Policy (September 5, 2000).

IV. Definitions

For purposes of this directive, the following definitions apply.

- A. **Content**: Information of any kind published to the Web (includes text, graphics, symbols, retrievable data, and presentation concepts).
- B. **Designated DHS Official**: The Commandant of the Coast Guard, the Inspector General, the General Counsel, the Director of the Secret Service, the Director, Bureau of Citizenship and Immigration Services, the Privacy Officer and the Civil Rights Officer.
- C. **DHS Organization Heads**: Secretary, Deputy Secretary, all Undersecretaries, Chief Officers and Designated DHS Officials
- D. **Extranet**: Any private network that uses the Internet protocol and the public telecommunication networks to securely connect to DHS Intranet and associated systems.
- E. **Internet**: The publicly accessible Web presence of DHS. The top-level (home) page URL is www.dhs.gov.
- F. **Intranet**: The DHS Web presence only accessible via authorized access to DHS networks. Note that various non-DHS personnel may at times have access to the DHS Intranet.

G. **Personal Use**: Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

H. **Special Use Application**: DHS business software that uses the Web as all or part of its communications network. Generally has a limited audience and restricted access via user identification/password. The fact that a particular application may have a vast audience (for example, a Human Resources application accessible by all employees) does not exempt it from this category. Special Use Applications are not subject to this directive.

I. **The Web**: Refers to the Internet, Intranet, and Extranet collectively.

J. **Web Content Manager**: Any individual designated to manage web content for an organizational element of DHS. The duties of the Web Content Manager include ensuring compliance with accessibility standards for persons with disabilities. This individual is the organization's primary point of contact for web issues.

K. **Web Content Provider**: Any individual who authors content for publication to DHS Web sites.

L. **Web Page**: Any single document posted to the Web.

M. **Web Site**: A group or system of web pages generally related by their content or ownership.

V. Responsibilities

A. **DHS Web management** is divided into three distinct disciplines - management of Web information, management of associated systems, and management of security. Accordingly, the responsibilities and authorities for each discipline are assigned to an appropriate official. Within the discipline of information management, different officials and entities have disparate responsibilities.

B. **The Web Executive Oversight Board (WEOB)** is established by this directive and shall be comprised of members from a broad cross-section of DHS organizations, such members to be nominated by the DHS Organization Head. The Board will:

1. Provide DHS vision and direction for implementation and use of the Web.

2. Be chaired by the DHS Chief Information Officer or a senior executive official designated by the DHS CIO. The WEOB Chair shall designate an individual to perform administrative duties related to WEOB activities.
3. Broker and remediate intradepartmental concerns and conflicts related to use and management of the Web.
4. Have the authority to charter working groups comprised of selected members of DHS organizational elements as necessary.

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

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

1. Provide overall policy implementation and procedural guidance for the Web and associated systems.
2. Ensure adherence to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.
3. Develop and maintain the Information System Security Plans for Web associated systems. (Web associated systems refer to those systems that comprise the DHS web and are not directly attributable to specific programs, such as web servers, gateways, security software and appliances and other ancillary components.)
4. Establish and enforce technical standards.
5. Authorize all DHS Web sites.
6. Provide technical procedural guidance for establishing and maintaining DHS Web sites.
7. Serve as Executive Sponsor of the Web Executive Oversight Board.
8. Establish a single Internet repository for all DHS policy deemed releasable to the Internet.

E. **The DHS Chief Information Systems Security Office (CISSO)** within the DHS Office of the CIO shall:

1. Provide policy implementation and procedural guidance regarding information and information system security for the Web.

2. Ensure that DHS Web information and associated systems adhere to laws, regulations, policies, and guidance regarding security.
3. Review and approve the Information System Security Plans (ISSP) for Web-associated systems.

F. **The DHS Assistant Secretary for Public Affairs** shall:

1. Ensure that style, message, and content on the Internet conform to the direction and vision set by the Secretary.
2. Designate a member to the Web Executive Oversight Board.
3. Provide and publish content describing DHS's mission, statutory authority, organizational structure, and Strategic Plan as required by the E-Government Act of 2002, as amended.

G. **DHS Headquarters Organization Heads** shall:

1. Ensure that Web site initiatives within their respective areas of responsibility adhere to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.
2. Establish a formal process for publishing information to the Web that accommodates the requirements of this directive and applicable authorities.
3. Develop and maintain content for the Web applicable to their specific areas of responsibility, as they deem necessary.
4. Respond to certification and reporting requirements for their Web information and associated systems.
5. Designate a Web Content Manager.
6. Designate a member to the Web Executive Oversight Board. Such member will represent all agency components within the organization.

H. **Web Content Managers** shall:

1. Review and approve Web content within their area of responsibility.
2. Manage Web content incidents.

3. Ensure that Web content within their area of responsibility adheres to laws, regulations, policies, and guidance including those regarding accessibility, privacy, and security.

I. **Web Content Providers** shall:

1. Develop Web content for publication.
2. Adhere to laws, regulations, policies, and guidance, including those regarding accessibility, privacy, and security.

J. **DHS employees** shall:

1. Comply with this and other directives (including MD 4600) prescribing use and management of Web information and associated systems.
2. Report discrepancies or policy inconsistencies reflected in Web content to appropriate managers.

K. **DHS employees** shall not:

1. Access pornographic material.
2. Access streaming media for entertainment purposes.

VI. Policy & Procedures

A. **General.**

1. The Department shall have a single Internet home page.
2. The Department shall have a single Internet repository for all DHS policy deemed releasable to the Internet. DHS policy shall not be repeated (duplicated) on other DHS Web sites or pages. Links to this repository or to specific documents are preferred and approved.

B. **Use of Internet Resources.**

1. DHS Web sites and pages shall be established only for official, mission-related or mission supporting purposes except as provided for below.
2. Limited incidental personal use is authorized in accordance with MD 4600 and with Government-wide policies on personal use of Government property and office equipment.

3. DHS Web servers shall not be used to host or store web sites or pages not authorized by the DHS CIO.

4. All activities sponsoring Web pages shall give due consideration and make every effort to minimize the use of bandwidth by their Web implementations.

C. **Security/Terms of Use.**

1. The DHS CISSO is the authority on security matters relating to Web information and associated systems. The CISSO promulgates the Interim Information System Security (ISS) Directive (and its subsequent amendments) which establishes DHS policy on information and information system security. The ISS Directive establishes a framework for managing the security of information and information systems. For the purposes of the ISS Directive, the Web is a General Support system. Information regarding the security level of the Internet, Intranet, and Extranet systems and content is currently being developed and will be contained in the DHS Web Information System Security Plan.

2. A standard Security Statement shall be applied DHS-wide and shall be readily accessible from all top level, or entry point DHS Web pages, or as deemed necessary by the CISSO.

3. All Web information and information systems shall comply with DHS MD # 4300 and subsequent amendments.

D. **Privacy.**

1. The DHS Chief Privacy Officer is the authority on privacy matters relating to Web information and information systems. In addition to the policies prescribed in the Privacy Act of 1974, several other Government-wide policies and guidance documents exist regarding privacy relative to the Web that should be referenced when making privacy determinations. They are listed in Section III of this Directive.

2. All Web information and associated systems shall comply with Privacy Act of 1974 and other applicable laws, regulations, and privacy policies.

3. A standard privacy statement shall be applied Department-wide and shall be readily accessible from all top level, or entry point DHS Web pages.

4. Information gathering, use, dissemination, and protection shall be in compliance with DHS's stated Privacy Policy. The Chief Privacy Officer must approve exceptions.

5. No Web page shall be used to gather information from the public or monitor public use of the DHS Internet without the express authority of the DHS CIO.

6. DHS personnel (employees, contractors, etc.) do not have a right, nor should they have an expectation, of privacy while using the Web when accessed via Government computers or networks. All such Web activities are subject to monitoring at all times.

E. **Accessibility.**

1. The DHS CIO is the authority on accessibility matters relating to Web information and associated systems for DHS.

2. All Web information and associated systems shall comply with Section 508 of the Rehabilitation Act of 1973 and all other applicable DHS specific and government-wide accessibility policies.

3. The policies and authorities prescribed in Section 508 of the Rehabilitation Act of 1973 and in MD 4010 should be referenced when making accessibility determinations.

F. **Content.**

1. A fundamental tenet of the E-Government Act of 2002 is that Government agencies must establish a formal process for determining what information to publish to the Web. Heads of DHS organizational elements are assigned this responsibility. The process shall also include review and approval measures to ensure compliance with all laws, regulations, policies, and guidance including those regarding accessibility, privacy, and security.

2. Only Official descriptions of DHS missions and entities shall be used on DHS Internet Web sites.

3. DHS Web sites shall have a mission orientation. A linkage between the content and DHS's strategic goals and objectives should be apparent.

4. Information shall only be published to the Web by persons or entities that can rightfully be considered to be the controlling authority of the information.

5. All DHS Web sites and pages shall comply with DHS and Government-wide policy regarding records management.
6. Managers of sites or pages that provide the ability to contact DHS with the expectation of a response shall ensure that a mechanism is in place to provide an accurate response within a reasonable timeframe - generally within three working days.
7. Links to pages outside of DHS Web sites are authorized in support of valid business objectives. Links may not endorse a particular non-Governmental product or service or provide preferential treatment. No payment of any kind shall be accepted to provide a link on any DHS Web page to another Web page or to provide specific content on a DHS Web page.
8. The following categories of information are prohibited on DHS Web sites except as noted by *:
 - a. Classified information.
 - b. For Official Use Only (FOUO) information. *
 - c. Inflammatory comments.
 - d. Information protected under the Privacy Act. *
 - e. Advertisements or endorsements of commercial products or services.
 - f. Copyrighted or trademarked material without explicit permission from the author or not subject to fair use. "Fair use" is a legal concept that permits the use of copyrighted material within certain limitations, such as quoting a short excerpt of a publication. Only legal counsel should make fair use determinations.
 - g. Personal statements regarding political candidates, politics or other political statements.
 - h. Pornographic material.
 - i. Information regarding DHS personnel or their families. Names and duty addresses of personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories will not be released nor will such individuals be identified in photographs or articles. *

- j. Information that would interfere with an official investigation or law enforcement activity, or judicial proceeding, including information that could subject law enforcement personnel to potential harm. *
- k. Internal program agenda, correspondence, and memos not appropriate for general distribution. *
- l. Pre-decisional information, reader files, internal letters, and memoranda shall not be released unless approved by the appropriate authority.
- m. Procurement-sensitive or proprietary information. *
- n. Personal opinion or private agenda.
- o. Duplication of DHS directives or other Government documents.
- p. Links from DHS Internet sites to DHS Intranet sites.
- q. Operations security (OPSEC) and Information Security (INFOSEC) material.*

* May be posted on Intranet and Extranet if sufficient access controls are in place, such as user identification/password access, or approved encryption technologies.

G. **Exceptions to this Directive:** All exceptions to this Directive must be submitted by the DHS Organizational Element CIO in writing to the DHS CIO and will be handled on a case-by-case basis.

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