Department of Homeland Security
DHS Directives System
Directive Number: 262-04
Revision Number: 00
Issue Date: April 13, 2015

DHS WEB (INTERNET AND EXTRANET INFORMATION)

I. Purpose

A. This Directive establishes Department of Homeland Security (DHS) policy regarding the use of DHS Web (Internet and extranet) for public communication purposes.

B. It provides instruction regarding:

1. Establishing, operating, and maintaining DHS Internet, and extranet services on unclassified networks to collect, disseminate, store, and otherwise process unclassified DHS information for public communications purposes.

2. Use of Internet and extranet based capabilities to collect, disseminate, store, and otherwise process unclassified DHS public information.

II. Scope

A. This Directive applies throughout DHS.

B. The scope of this Directive is limited to the use and management of DHS Web systems where the intent is to make information available to the public or to a general audience within DHS. It does not pertain to the behind the firewall sections of Special Use Applications that happen to use the Web as all or part of their communication network, but does cover their publicly accessible and visible face.

C. This Directive applies to DHS employees, contractors and non-DHS entities that are supporting DHS mission-related activities or accessing DHS or Internet and extranet based capabilities via DHS information systems.

D. DHS Management Directive (MD) 4400.1, "DHS Web (Internet, Intranet, and Extranet Information and Information Systems)," and Directive 139-01, "Domain Names" are hereby rescinded.

III. Authorities

A. Title 5, United States Code (U.S.C.), Section 552a, "Records Maintained on Individuals" [The Privacy Act of 1974, as amended]

B. Title 29, U.S.C., Section 794d, "Electronic and Information Technology" [Section 508 of the Rehabilitation Act of 1973]

C. Title 44, U.S.C., Chapter 35, "Coordination of Federal Information Policy" and Chapter 36, "Management and Promotion of Electronic Government Services"

D. Title 44, U.S.C., Chapter 21, "National Archives and Records Administration," Chapter 29, "Records Management by the Archivist of the United States and by the Administrator of General Services," Chapter 31, "Records Management by Federal Agencies," Chapter 33, "Disposal of Records," Chapter 35, "Coordination of Federal Information Policy," and Chapter 36, "Management and Promotion of Electronic Government Services"

E. Executive Order 13571, 'Streamlining Service Delivery and Improving Customer Service"

F. Office of Management and Budget (OMB) Memorandum M-05-04, "Policies for Federal Agency Public Websites"

G. OMB Memorandum M-10-06, "Open Government Directive"

H. OMB Memorandum M-10-22, "Guidance for Online Use of Web Measurement and Customization Technologies"

I. OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications"

J. OMB Memorandum Improving the Accessibility of Government Information

K. DHS Delegation 2001, "Delegation to the Assistant Secretary for Public Affairs"

L. DHS Delegation 2003, "Delegation of Public Affairs Authority to Components"

M. DHS Delegation 04000, Delegation for Information Technology"

N. The following regulations regarding Privacy:

1. Title 18, U.S.C., Chapter 119, "Wire and Electronic Communications Interception and Interception of Oral Communications"

2. Title 15, U.S.C., Chapter 91, "Children's Online Privacy Protection"

3. OMB Memorandum 99-18, "Privacy Policies on Federal Websites"

4. OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Websites"

5. Directive 047-01, "Privacy Policy and Compliance"

6. MD 4600.1, "Personal Use of Government Office Equipment"

7. 4300A, "DHS Sensitive Systems Policy"

IV. Responsibilities

A. The ***DHS Assistant Secretary for Public Affairs***:

1. Authorizes and serves as the oversight authority for all DHS public websites.

2. Provides procedural guidance for establishing and maintaining DHS websites and ensures that style, message, and content on the Internet and extranet conform to the direction and vision set by the Secretary and is responsible for all aspects of this Directive.

3. Enforces the policies outlined in all aspects of Directive 262-04.

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

1. Ensures adherence to Web and information systems policies, laws, regulations, and guidance including those regarding accessibility and security.

2. Ensures that DHS websites, Web pages and Web portals adhere to laws, regulations, policies and guidance regarding IT and network security, as administered by the Office of the Chief Information Security Officer (OCISO).

3. Establishes the records retention and disposition matters relating to Web information for public and internal communication purposes, as administered by the DHS Chief Records Officer.

C. The ***DHS Chief Privacy Officer*** is the authority on privacy matters relating to Web information for public communication purposes. In addition to the policies prescribed in the Privacy Act of 1974, as amended, several other government-wide and DHS policies and guidance documents exist regarding privacy relative to the Web that *should be referenced* when making privacy determinations. Please contact privacy@hq.dhs.gov with questions.

D. The ***DHS Component heads***:

1. Establish a formal process for publishing information to the Web that conforms to the requirements of this Directive and applicable authorities.

2. Respond to certification and reporting requirements for their Internet and extranet systems.

E. The ***Web Content Management Executive Steering Committee***:

1. Is established by this Directive and is co-chaired by the Assistant Secretary for Public Affairs and the DHS Chief Information Officer or their designees.

2. Provides DHS vision and direction for implementation and use of the Web.

3. Is composed of a mixture of DHS Chief Executive leadership and members from DHS organizations that own and operate top-level domain public web sites, nominated by the DHS Component heads.

V. Policy and Requirements

A. ***Policy***:

1. The DHS websites serve as a primary mechanism for the public to learn about and review DHS activities, and for key stakeholders to engage with DHS. DHS encourages the use of DHS websites to allow and encourage the electronic conduct of Department business.

2. Each DHS website communicates to the fullest array Department information, including general information, program actions and activities, mission, statutory authority, organizational structure, strategic plan, regulations, and educational materials.

B. ***Requirements***:

1. All DHS public websites include a U.S. flag logo and "Official website of the Department of Homeland Security" in the website banner above the Component logo and name as seen on www.dhs.gov. Compliance is required by October 1, 2014.

2. DHS websites and pages are established only for official, mission-related purposes except as provided for in the Instruction to this Directive.

3. In accordance with Executive Order 13571, DHS is required to keep pace with and exceed customer expectations by applying technology best practices from the private sector "to deliver services better, faster and at a lower cost."

4. All DHS public websites include a highly visible link to the DHS Office of Inspector General.

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

6. All DHS Web and information systems (to include their sponsoring entities and program managers) comply with the Federal Records Act of 1950 and all other applicable DHS-specific and government-wide records retention policies and disposition schedules.

7. All DHS-owned or operated websites use a dot-gov first level domain (per OMB). Domains are approved by the DHS Office of Public Affairs (OPA) and are requested through the Office of the Chief Information Officer (OCIO). Sub-domains on DHS.gov are also approved by the DHS Office of Public Affairs and requested through the OCIO.

8. U.S. Coast Guard (USCG) operated websites are authorized to use a dot-mil first-level domain. All USCG websites comply with Department of Defense policies and procedures.

9. All DHS top-level domains (e.g. dhs.gov, fema.gov, uscis.gov) use the DHS- preferred search tool (determined by OPA and the OCIO) and provide a search bar on the home page.

10. To maximize readability for external audiences, DHS public websites follow the Associated Press Stylebook with some exceptions as outlined by DHS OPA.

11. Non-US government (USG) advertisements, logos and aggrandizing statements (such as "Powered by...") are not allowed on DHS public websites.

12. In rare instances, DHS Internet and extranet services may include links to websites that are not government-owned or government-sponsored if these websites provide government information and/or services in a way that is not available on an official government website.

13. Web metrics requirements are outlined by the Assistant Secretary of Public Affairs and OMB.

14. All DHS top-level domains include links to No FEAR Act Data (summary statistical data about equal employment opportunity complaints filed with DHS or with DHS Components, as applicable, and written notification of whistleblower rights and protections pursuant to "The No FEAR Act" or The Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002), USA.gov, and WhiteHouse.gov.

15. DHS employees and contractors follow the guidelines for official presence on external websites and social media environments outlined by the Assistant Secretary of Public Affairs and found in the instruction to this Directive.

16. All exceptions to this Directive are submitted by the DHS Component CIO in writing to DHS OPA and the DHS CIO, and handled on a case-by-case basis.

VI. Questions

Address any questions or concerns regarding this Directive to the Office of the Chief Information Officer or the DHS Office of Public Affairs.

Chip Fulghum
Acting Deputy Under Secretary for Management

APR 13 2015
Date