Department of Homeland Security
DHS Directives System
Instruction Number: 262-04-001
Revision Number: 00
Issue Date:

DHS WEB (INTERNET AND EXTRANET INFORMATION)

I. Purpose

This Instruction implements the Department of Homeland Security (DHS) Directive 262-04, "DHS Web (Internet and Extranet Information).

II. Scope

A. This Instruction applies throughout DHS.

B. The scope of this Instruction 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.

C. This Instruction applies to DHS employees, contractors, and non-DHS entities that are supporting DHS mission-related activities or accessing DHS internet and extranet services or capabilities via DHS Information Systems, to the extent provided in the contract or other instrument by which such authorized support or access is provided.

III. References

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

B. The Office of Management and Budget (OMB) OMB Circular A-130, "Management of Federal Information Resources"

C. OMB Memorandum 99-05, "Instructions on complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records".

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

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

F. Letter from John Spotila to Roger Baker, clarification of OMB Cookies Policy (September 5, 2000)

G. Requirements for Accepting Externally-Issued Identity Credentials - Memo from Federal CIO to Executive Branch Agency CIOs, 2010

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

I. Directive 140-01, "Information Technology Systems Security"

J. Directive 2260.1, "Review of External Publications"

K. Management Directive (MD) 0480.1, "Ethics/Standards of Conduct and Federal Ethics Laws"

L. MD 4010.2, "Section 508 Program Management Office and Electronic and Information Technology Accessibility"

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

N. Directive 141-01, "Records and Information Management"

IV. Other Resources

A. Content managers across DHS are encouraged to regularly review and incorporate best practices, policies, and procedures for Web publishing available on the DHS Connect Office of Public Affairs (OPA) website under Web Communications.

B. Those resources include the following:

1. Branding Guidelines

2. Content Pre-Cleared for Publishing on DHS.gov

3. Grammar and Web Style

4. Guidelines for Content Providers

5. Linking to Dot-gov and Outside Websites

6. Organization Chart Style

7. Protecting Information from Accidental Exposure

8. Roles of Content Providers

9. Tools for Creating Better Web Content

C. Other guidelines for federal websites include:

1. OMB, "Digital Government: Building a 21st Century Platform to Better Serve the American People"

V. Definitions

For purposes of Directive 264-04 and this Instruction, the following definitions apply.

A. ***Component:*** Any organization that reports directly to the Office of the Secretary (e.g., the Secretary, the Deputy Secretary, the Chief of Staff, the Counselors, and their respective staff) when approved as such by the Secretary.

B. ***Extranet***: Any private network that uses the Internet protocol and the public telecommunication networks to securely connect to the intranet and associated systems. An example of a DHS extranet is hsin.dhs.gov.

C. ***Internet***: The publicly accessible Web content. Within DHS, the top-level Internet URL is www.dhs.gov.

D. ***Intranet***: Private network of Web content accessible only to specific individuals with authorized access. Various non-DHS personnel may at times have access to the DHS intranet.

E. ***Official Presence:*** Any publicly accessible website or social media account that is identified as an official DHS website or account, either by use of the DHS seal and Component names or by declaration in the site to give the public confidence in the authority of the site.

F. ***Operational Component:*** Component with specific centralized program responsible for directly achieving one or more of the Department's mission activities; generally has authority over its Finance, Human Resources, Information Technology, Procurement, and Security programs.

G. ***Personal Use***: Activity conducted for purposes other than accomplishing official or otherwise authorized activity. Executive Branch employees are specifically prohibited from using government office equipment to maintain or support a personal private business. Examples of this prohibition include employees using a government computer and Internet connection to run a travel business or investment service. The ban on using government office equipment to support a personal private business also includes employees using government office equipment to assist relatives, friends, or other persons in such activities. Employees may, however, make limited use under this policy of government office equipment to check their Thrift Savings Plan or other personal investments, or to seek employment, or communicate with a volunteer charity organization.

H. ***Personally Identifiable Information (PII):*** Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to an individual. "Individual" includes but is not limited to, U.S. citizens, legal permanent residents, visitors to the U.S, and Department employees and contractors.

I. ***Social Media:*** Websites and online applications used for social networking.

J. ***Special Use Application***: DHS business software such as mobile applications that use 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 Instruction.

K. ***Support Component***: Component that generally provides specific assistance to other DHS Components and/or external organizations; generally utilizes shared services through Management.

L. ***Top Level Domain***: A top-level domain is one of the domains at the highest level in the hierarchy of DHS Component websites, e.g. dhs.gov, fema.gov, uscis.gov, cbp.gov.

M. ***The Web***: Global computer network that offers text, graphics, sound, and animation resources through the hypertext transfer protocol. Includes the Internet, intranet and extranet.

N. ***Uniform Resource Locator***: An Internet address (for example, http://www.dhs.gov/about-dhs), usually consisting of the access protocol (http), the domain name (www.dhs.gov), and optionally the path to a file or resource residing on that server (about-dhs).

O. ***Web Associated Systems***: refer to those systems that compose the DHS Web and are not directly attributable to specific programs, such as webservers, gateways, security software and appliances, and other ancillary components.

P. ***Web Content***: Information of any kind published to the Web (includes text, graphics, symbols, retrievable data, and presentation concepts).

Q. ***Web Content Management System***: Information technology providing website authoring, collaboration, and administration tools designed to allow users to create and manage website content. Provides the foundation for collaboration, offering users the ability to manage Web content, documents, and output for multiple author editing and participation. Most systems use a content repository or a database to store page content, metadata, and other information assets that might be needed by the system.

R. ***Web Content Publisher***: An individual, division or office responsible for reviewing and publishing content on the Web.

S. ***Web Liaison***: Also known as the Web Content Approver. Individual designated to manage Web content. Within DHS the duties of the Web Liaison include ensuring compliance with accessibility standards for persons with disabilities. This individual is the Component's primary point of contact for Web issues.

T. ***Web Page***: Single document or resource of information connected to the Web and accessible via a web browser.

U. ***Website***: Collection of hypertext markup language (HTML) web pages and subordinate documents typically accessible from the same uniform resource locator (URL) via the Web and normally residing on the same server, forming a coherent, usually interlinked whole.

VI. Responsibilities

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

1. Operates and maintains the official public website for DHS (www.dhs.gov).

2. Establishes documented processes for reviewing information proposed for dissemination to prevent access to non-public information.

3. Designates a member to serve on the Web Content Management Executive Steering Committee, as the Office of Public Affairs (OPA) Web representative (usually the Director of Web Communications) and can designate a stand-in co-chair.

4. Provides and publishes content describing DHS's mission, statutory authority, organizational structure, and Strategic Plan as required by the E-Government Act of 2002, as amended.

5. Develops and makes available education, guidance, and training for the responsible and effective use and management of the Department's external official Web presence.

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

1. Develops and coordinates DHS policies governing the use, risk management, and oversight of DHS websites, providing overall policy implementation and procedural guidance for the Web and associated systems purposes, except where limited incidental personal use is authorized in accordance with MD 4600.1 and other government-wide policies on personal use of government property and office equipment.

2. Integrates guidance regarding the responsible and effective use of DHS websites.

3. Ensures that DHS websites and DHS information are accessible to disabled employees and disabled members of the public, and that access is comparable to that available to non-disabled individuals in compliance with Section 508 of the Rehabilitation Act of 1973.

4. Coordinates corrective action for DHS websites not operated in compliance with this Instruction.

5. In coordination with DHS OPA, assesses the need to isolate, disconnect, terminate, or otherwise shut down DHS websites, web pages and web portals that access Web-based capabilities within Component jurisdiction. Non-compliant websites, web pages and web portals are disabled if they are not brought into compliance with applicable policies within 90 calendar days of identification or notification of noncompliance, and if there is no plan of action or milestones for correction in place. This process can be initiated by OPA or OCIO depending on the specific issue.

6. Provides a consolidated list of education and training resources for the use of DHS websites.

7. Develops and maintains the Information System Security Plans for Web-associated systems.

8. Establishes and enforces technical standards for Web-associated systems.

9. Serves as Executive Co-Chair of the Web Content Management Executive Steering Committee.

10. Hosts and operates a registration system for the Web addresses of public DHS websites that is capable of producing individual DHS Component inventories.

11. Educates and trains DHS employees in the responsible and effective use of DHS websites.

C. ***The DHS Chief Records Officer:***

1. Serves as the authority on records retention and disposition matters relating to Web information for public and internal communication purposes.

2. In addition to the policies prescribed in the Federal Records Act of 1950, as amended, several other government-wide and DHS policies and guidance documents exist regarding records retention and disposition relative to the Web, social media, and related resources that should be referenced when making determinations on Web data preservation or deletion. Contact the Chief Records Officer via DHSrecordsmanagement@hq.dhs.gov.

D. ***The DHS Component Heads***:

1. Designate a content manager to run their public websites.

2. Ensure that website initiatives within their respective areas of responsibility adhere to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.

E. ***DHS Employees***:

1. Comply with Directive 262-04 and other Management Directives (including MD 4600, "Personal Use of Government Office Equipment")

prescribing use and management of Web information and associated systems while at work on-site or off-site.

2. Report discrepancies or policy inconsistencies reflected in Web content to appropriate managers.

F. ***The Web Liaisons/Web Content Approvers***:

1. Establish a formal process for publishing information to the Web that complies with the requirements of Directive 262-04 and applicable authorities.

2. Develop and maintain content for the Web applicable to their specific areas of responsibility as they deem necessary.

3. Respond to certification and reporting requirements for the Web.

4. Review and approve Web content within their areas of responsibility.

5. Manage Web publishing requests sent to OPA from the Components they represent.

6. Ensure that Web content within their areas of responsibility adhere to federal laws, regulations, policies, and guidance including those regarding accessibility, privacy, and security.

G. ***The DHS Office of the Chief Information Security Officer (OCISO)*** within the DHS Office of the CIO:

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

2. Ensures that DHS Web information and associated systems adhere to laws, regulations, policies, and guidance regarding security.

3. Reviews and approves the Information System Security Plans for Web-associated systems.

H. ***The Web Content Providers***:

1. Develop Web content for publication.

2. Adhere to laws, regulations, policies, and guidance, including those regarding accessibility, privacy, and security.

I. ***The Web Content Management Executive Steering Committee*** (ESC) pursuant to Directive 262-04:

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

2. Brokers and remediates intradepartmental concerns and conflicts related to use and management of the Department's Web presence.

3. Has the authority to charter working groups composed of selected members of DHS Components as necessary.

4. Is composed of a mixture of DHS Chief Executive leadership and DHS Component leadership.

5. Is co-chaired by the DHS Assistant Secretary for Public Affairs and the DHS Chief Information Officer or their designees.

6. Is composed of Operational Components' public-affairs and information technology senior leadership.

a. **ESC Chairpersons:**
DHS OPA, Assistant Secretary or designee
DHS OCIO, Chief Information Officer or designee

b. **ESC Members:**
Under Secretary for Management designee (Voting Member)
Senior OPA and CIO leadership from Operational DHS Components (Voting Members, one each per Component)
Executive Director, Enterprise System Development Office (ESDO) (Non-Voting)
Chief Records Officer (Non-Voting)
OPA Director of Web Communications (Non-Voting)

VII. Content & Procedures

A. ***General***:

1. The Department has a single, official Internet home page at www.dhs.gov.

2. All Component public websites include a U.S. flag logo and "Official website of 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.

B. *Use of Web Resources*:

1. DHS websites and pages are established only for official, mission-related purposes except as provided for in Section VII. J below.

2. DHS webservers require the prior written approval of the DHS CIO to host or store websites or other material.

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

C. *Security*:

1. All Web information and information systems comply with Directive 140-01, "Information Technology Systems Security and 4300A Documents."

D. *Privacy*:

1. Post or link clear privacy policies on all public DHS websites at major entry points and at those points or pages where PII is collected from the public. Use the specific label "Privacy Policy" and link to: http://www.dhs.gov/privacy-policy.

2. Collection, gathering, use, dissemination, and protection of PII are in compliance with DHS' stated Privacy Policy (http://www.dhs.gov/privacy-policy) and all applicable laws, regulations, and DHS policies. The DHS Chief Privacy Officer approves exceptions. No webpages are used to gather information from the public or monitor public use of the DHS Web without the express authority of the DHS Chief Privacy Officer.

3. Prior to the collection, gathering, use, or dissemination of PII from members of the public, Web Content Managers complete a Privacy Threshold Analysis (PTA) and submit it to the DHS Chief Privacy Officer for review and approval. A Privacy Impact Assessment or System of Record Notice may be required.

4. All Web information and associated systems comply with the Privacy Act of 1974, as amended, and other applicable laws, regulations, and privacy policies.

5. DHS personnel (e.g. employees, contractors) do not have a right to, 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.

6. Privacy Act Statements (PAS) - When an individual is requested to furnish PII and the information is to be included in a system of records (i.e., a system in which information about the individual is retrieved by name or other unique identifier), a PAS is posted or provided through a well-marked hyperlink on the page where the information is being requested.

a. Web Content Managers ensure that a Privacy Act System of Records Notice has been published in the Federal Register prior to the collection or maintenance of PII from the website. Please contact privacy@hq.dhs.gov with questions.

b. If a PAS would be required for a paper-based solicitation, it is required for online solicitation, regardless of whether the site is a public or private DHS website.

7. Privacy Impact Assessments (PIAs) - A PIA is submitted and approved before activating DHS Web pages or forms that collect, disseminate, process, or consist of PII from or about members of the public or contractors employed at DHS. For additional information, please see Directive 047-01, "Privacy Policy and Compliance."

a. PIAs are posted on the DHS Privacy Office public website.

b. In accordance with OMB Memorandum M-10-23, an adapted PIA is required whenever a DHS Component's use of a third-party website or application makes PII available to the DHS Component.

8. Any loss, theft, unauthorized disclosure, or unauthorized access of PII, suspected or confirmed, is reported upon detection or discovery and in accordance with DHS Privacy Incident Handling Guidance, information security policies, and component policies.

E. ***Paperwork Reduction Act (PRA).*** All Web forms comply with MD 142-01, "Information Collection Program."

F. ***Freedom of Information Act (FOIA).*** All DHS public websites include information on how to request information under FOIA and link to information made available specifically under FOIA.

G. ***Records Management.***

DHS, like all Federal agencies, follows the policy, regulations and guidelines for the Web and associated resources established by OMB and other cognizant regulatory authorities. One such authority, the National Archives and Records Administration, regulates and approves specific guidance regarding Web, social media, and related program records.

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

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

I. ***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 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 4010.2, "Section 508 Program Management Office and Electronic and Information Technology Accessibility" are referenced when making accessibility determinations.

J. ***Content on Public Facing Websites***.

1. A fundamental tenet of the E-Government Act of 2002 is that government agencies establish a formal process for determining what information to publish to the Web. Heads of DHS Components are assigned this responsibility in DHS Delegation 2003, "Delegation of Public Affairs Authority to Components" and Delegation 2002, "Delegation of Public Affairs Authority to the Office of Public Affairs." The process includes review and approval measures to ensure compliance with all laws, regulations, policies, and guidance including those regarding accessibility, privacy, and security. Pursuant to DHS Delegation Number

2001, OPA has final review authority over all publicly released information that is placed on publicly accessible websites.

2. Only Official descriptions of DHS missions and entities are used on DHS websites.

3. DHS websites are mission oriented. Links between the content and DHS's strategic goals and objectives is apparent.

4. A clear Web publishing process is established by each website owner.

5. All DHS websites and pages comply with Directive 141-01, "Records Management."

6. Managers of websites or pages that provide the ability to contact DHS with the expectation of a response ensure that a mechanism is in place to provide an accurate response within a reasonable timeframe.

7. Links to pages outside of DHS control are authorized in support of valid business missions or objectives. Links do not endorse a particular non-governmental product or service, or provide preferential treatment. No payment of any kind is accepted to provide a link on any DHS webpage to another webpage or to provide specific content on a DHS webpage.

8. The following categories of information are prohibited on DHS websites except as noted by *:

a. Classified information.

b. For Official Use Only (FOUO) information.*

c. Inflammatory comments.

d. Information protected under the Privacy Act, as amended.*

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. 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 are not released, and such individuals are not 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 agendas, correspondence, and memos not appropriate for general distribution.*

l. Pre-decisional information, reader files, internal letters, and memoranda are not released unless approved by the appropriate authority.

m. Procurement-sensitive or proprietary information.*

n. Personal opinion or private agendas.

* May be posted on Extranet if sufficient access controls are in place, such as user identification/password access, or approved encryption technologies. The owner of the Extranet site is responsible for ensuring the security of the site.

K. ***Domains and Sub-domains.***

Consolidation of the Department's public websites to lower the number of top-level domains is a high priority for DHS. To establish a new domain or sub-domain, a waiver request is required.

1. All government-owned or operated websites use a dot-gov first level domain (per OMB), and are approved by the DHS Office of Public Affairs and requested through the Office of the Chief Information Officer (OCIO). The U.S. Coast Guard has authority to use the dot-mil first level domain and is required to comply with Department of Defense (DoD) Web policies.

2. Sub-domains on DHS.gov are also approved by the DHS Office of Public Affairs and requested through the OCIO.

3. Sub-domains on Operational Component top-level domains are approved by that component's Office of Public Affairs and relayed to DHS OPA.

4. There is currently an OMB restriction preventing the establishment of new dot-com, dot-gov and dot-mil domains. To obtain a waiver, submit a completed Web Proposal Template to DHS OPA. The template can be downloaded from DHS Connect or requested by e-mailing webpublishing@dhs.gov.

L. ***Search.***

Duplicative search functions on and across DHS websites are avoided absent a compelling operational need or documented business case. Component websites include the preferred DHS search tool.

M. ***Advertising and Endorsement.***

1. For the purpose of advertising, public DHS websites are U.S. Government (USG) publications. The credibility of DHS information should not be adversely affected by association with non-USG sponsorships, advertisements, or endorsements.

2. Advertisements by or for any private individual, firm, or corporation are not inserted or allowed on public DHS websites. DHS endorsement is not implied in any manner for any specific non-USG service, facility, event, or product.

3. Stand-alone non-USG graphics, logos, or aggrandizing statements such as "Powered by ...," "Serviced by ...," and "Designed by ..." are not inserted or allowed on public DHS websites or the DHS-controlled content area of a website prepared or produced with either appropriated or non-appropriated funds. Proprietary rights notices (including copyright and trademark notices) are not aggrandizing statements. Factual acknowledgement of partners, software, technology, and services used on a public DHS website may be included in descriptive information about the service or the organization, such as an "About Us" page; however, such acknowledgement is carefully considered in the security risk assessment and risk mitigation measures for the service, and not used in any manner that supports the appearance of endorsement.

4. Users are not required or encouraged to choose any specific brand of browser software or other client applications to access public DHS websites. DHS websites are designed in accordance with accepted standards of the World Wide Web Consortium to ensure browser compatibility.

N. *Links.*

1. In rare instances, DHS websites 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.

2. Only links to information or services related to the performance of the DHS Component's function or mission and the purpose of the DHS website are established.

3. Links to U.S. Government (USG) websites are not disclaimed. Disclaimers are displayed or linked to public DHS websites that have non-USG links, or through an intermediate "Exit Notice" page generated by the server whenever a request is made for any non-USG link.

4. Links or references to DHS extranet websites are not normally placed on public DHS websites; however, under certain circumstances it may be appropriate to establish a link to a log-on page, provided that details about the contents are not revealed.

O. *Web Measurement and Customization Technologies (WMCT).*

1. In accordance with OMB Memorandum M-10-22, DHS Components may use WMCT (e.g., cookies) for the purpose of improving DHS services online through conducting measurement and analysis of usage, or through customization of the user's experience.

2. Regardless of circumstances, the DHS Components do not use such technologies:

a. To track individual-level user activity on the Web outside of the DHS Web service from which the technology originates.

b. To share the data obtained through such technologies, without the user's explicit consent, with other federal agencies, DHS Components, or other organizations. Explicit consent includes a notice of the purpose and ramifications of the technology being used, as well as an opt-in function to allow the users to signify they have read and understand the information and agree to the technology's use. For example, this could be achieved with a pop-up box and "agree" button that link to privacy policies and Terms of Use statements.

c. To cross-reference, without the user's explicit consent, any data gathered from WMCT against PII to determine individual-level online activity.

d. To collect PII without the user's explicit consent in any fashion.

P. ***Web Metrics.***

1. Site Performance Analytics

a. In accordance with the Federal Digital Strategy, DHS top-level domains use the Web metrics tool supplied by the General Services Administration (GSA) for Department and Government-wide public facing website performance measurement.

b. DHS top-level domains implement the DHS designated website search tool and include a Search box in the top banners on their websites.

2. Search

a. Component websites report the top 10 website search (internal) terms and the top ten search engine (external) queries in a publicly accessible location preferably on a "/metrics" page, e.g. www.dhs.gov/metrics.

3. Satisfaction

a. In accordance with the President's Transparency and Open Government Memorandum (January 21, 2009) and the OMB Director's Open Government Directive Memorandum (December 8, 2009), DHS top-level websites include a customer satisfaction survey composed of four multiple choice questions designed to generate and record feedback from the public about the user experience.

b. For information about the survey tools approved for use on DHS public websites, contact webpublishing@hq.dhs.gov.

c. The customer satisfaction questions for top-level DHS sites are as follows:

i. How would you rate your overall experience today? (Range from 1 poor – 10 excellent)

ii. Were you able to complete the purpose of your visit? (Yes/No)
If no, skip to sub question - What prevented you from completing the purpose of your visit? Please be as specific as possible. (For this question, you have a choice of offering respondents an open text box OR providing the response options below.)

Responses

- Could not find what I was looking for
- Site search function did not work
- Information was confusing
- File did not download
- Video or webinar did not function properly
- Other, please specify

iii. If respondent selects, "Could not find what I was looking for," skip to this question:

- What information were you looking for? Please be as specific as possible. [Open text box]

iv. Would you still return to this website if you could get this information or service from another source? (Yes/No)

v. Will you recommend this website to a friend or colleague? (Yes/No)

d. Customer survey questions do not solicit PII.

4. Reporting

a. Component website performance data on analytics, search, and satisfaction for all top-level domains is reported on DHS.gov by placing DHS Google Analytics data, external and internal search information, and satisfaction survey results in a publicly accessible location, e.g. www.dhs.gov/metrics. Website owners also send reports to DHS OPA at webpublishing@hq.dhs.gov.

Q. ***Contact Information.***

1. Contact information is linked from all major entry points on the DHS Components' principal public websites. Consolidating this information on a single "Contact Us" page is recommended. Contact information contains:

a. Organization's postal address.

b. Street addresses for any regional or local offices that have a function requiring interaction with the public.

c. Office telephone number(s), including numbers for any regional or local offices or toll-free numbers and telephone device for the deaf (TDD) numbers, if available. If TDD lines are not available, use appropriate relay such as the Federal Relay Service as needed.

d. Means to communicate by electronic mail (e.g., e-mail addresses, group mailbox).

e. The policy, procedures, and time for responding to e-mail inquiries.

f. Contact information to report data problems.

g. How to request information and link to information made available specifically under FOIA. (DHS FOIA guidance is posted on the DHS public website.)

h. Contact information for or link to the DHS office that promotes small business participation in DHS contracts.

i. Contact information to report both technical and information problems regarding the website specifically, including accessibility problems.

R. ***Mandatory Links.***

1. A link specifically labeled "No FEAR Act Data" is placed on home pages of DHS public websites and the principal public websites of DHS Components. This specific label links to summary statistical data about equal employment opportunity complaints filed with DHS or with the DHS Components, as applicable and written notification of whistleblower rights and protections pursuant to "The No FEAR Act."

2. USA.gov - Link to the United States Government's Official Web Portal, USA.gov, on home pages of DHS public websites and the principal public websites of DHS Components.

3. WhiteHouse.gov - Link to the Official White House website on home pages of DHS public websites and the principal public websites of DHS Components.

4. DHS public websites and the principal public websites of DHS Components provide links to their respective privacy policies.

S. *Strategic and Annual Performance Plans.* Link to the DHS Component's strategic plan and annual performance plans from major entry points to the DHS public website and the principal public websites of DHS Components.

T. *Official Presence on External Websites and Social Media.* Longstanding guidance on personal communication ethics and the handling and dissemination of DHS information continues to apply when using Web-based capabilities for official-use accounts. Policies and laws related to the protection, control, and release of DHS information, such as operations security, information security, records retention and disposition, and PII apply.

1. Contact Information and Identification

a. Use mission-related contact information, such as official duty telephone numbers or postal and e-mail addresses, to establish official-use accounts when such information is required.

b. Depending on the requirements of the specific Web-based provider, official-use account pages for individuals and pages representing DHS organizations are established in the category "Government," and registered to organization names that begin with "U.S. Department of Homeland Security/[insert name of organization or name of Component]." This requirement does not apply to creation of a specific account name, handle, or nickname.

c. When using a Web-based service for official use, the transparency banner described in *Figure 2* is posted, as possible, to ensure clear distinction between the collaborative forum or discussion board of the provider and the official information available on the DHS Component's website.

2. Communication

a. Sensitive and classified information, and unclassified information that aggregates to reveal sensitive or classified information, is not disclosed.

b. Official-use accounts are not used to conduct communication not related to assigned duties, functions, or activities.

c. Web-based services are used as supplemental communication or distribution channels for DHS information. Do not establish or represent official-use accounts or pages as primary sources of DHS information.

d. A clear description of the purpose for using the Web-based service and that DHS is the content provider is posted, as necessary.

e. Links to official DHS content hosted on DHS-owned, -operated, or -controlled sites is posted, where applicable and possible, when official use of a Web-based service references materials originating from an official DHS website.

f. Links posted are to the Component's official public website.

g. Specific steps to protect individual privacy whenever third-party websites and applications are used to engage with the public are implemented in compliance with OMB Memo M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications."

3. Disclaimers

a. "For official information from or about the U.S. Department of Homeland Security/[insert name of organization or name of Component], please visit [insert homepage or other official information source] at [insert address]." is placed in a prominent location on each authorized page as workable.

b. If the Web-based provider is disinclined or unable to block the display of commercial advertisements, the following message is placed in a prominent location on each authorized page as workable: "The appearance of commercial advertising and hyperlinks inserted by the host of this service does not constitute endorsement by the U.S. Department of Homeland Security/[insert name of organization or name of Component]."

4. Transparency Banner. As workable, the standard transparency banner in *Figure 3* is displayed on external official uses of Web-based services.

5. Web Address Shortening. Some Web-based services (e.g., Twitter, Facebook) encourage shortened address links to fit text and character limitations. Go.USA.gov is available to create short .gov address links for official government addresses in the .gov, .fed, .us, and .mil domains. For official government addresses in other domains, commercial address shorteners may be used.

U. **Official Use**. In addition to approving the establishment of an external official presence, DHS Component Heads may approve the establishment of Web-based accounts by authorized users for public communication related to other assigned duties, such as recruiting, or any other purpose determined necessary in the interest of the federal government.

The following provisions apply to official use:

1. DHS Component, Operational Component, and Support Component heads and official-use account users account fully for exercising sound judgment within the authority and scope of official activities

2. Liaison is conducted with OPA to ensure organizational awareness of their authorized, mission-related public communication. To view the policy for the use of specific DHS-approved social media, visit the Web Communications Social Media page on DHS Connect or contact webpublishing@hq.dhs.gov.

3. Written requests (letters or e-mails) are submitted to Web-based providers to block the display of any commercial advertisements, solicitations, or links on social media and webpages administered with official-use accounts if the Web provider would otherwise normally display such materials. Use the disclaimer in *Figure 1* if the DHS TOS with the Web provider allows for commercial advertisements.

4. Establishing an official presence on, or use of, a website or social media application may require acceptance of a TOS agreement. The "standard" TOS used by the provider may contain legally objectionable terms and conditions which are amended or otherwise addressed for DHS use.

5. DHS employees and DHS contractors who establish an external official presence on a Web-based service verify whether a TOS for that service has been signed and approved by the Office of General Counsel. Such TOS apply to DHS-wide use and operation of external official presence and other official uses. In this case, there is no need for additional TOS at the Component level.

6. Official-use accounts are not used to communicate information unrelated to assigned duties, functions, or activities.

7. Web-based services are used as supplemental communication or distribution channels for DHS information. Official-use accounts or pages do not represent the primary sources of DHS information.

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

VIII. Questions

Any questions or concerns regarding this Directive should be addressed to the Office of the DHS CIO or DHS OPA.

Tay J Bradsher
Tanya J. Bradsher
Assistant Secretary for Public Affairs

15 April 2015
Date

Figure 1. External Links Disclaimer

"The appearance of hyperlinks does not constitute endorsement by the [insert sponsoring organization] of non-U.S. Government sites or the information, products, or services contained therein. Although the [insert sponsoring organization] may or may not use these sites as additional distribution channels for Department of Homeland Security information, it does not exercise editorial control over all of the information that you may find at these locations. Such links are provided consistent with the stated purpose of this website."

Figure 2. Transparency Banner

"Welcome to the [name of DHS Component]'s [name of website] page/presence. If you are looking for the official source of information about the [name of DHS Component], please visit [address of official website or other official information].

The [name of DHS Component] is pleased to participate in this open forum in order to increase government transparency, promote public participation, and encourage collaboration.

Please note that [name of DHS Component] does not endorse the comments or opinions provided by visitors to this site. The protection, control, and legal aspects of any information that you provided to establish your account or information that you may choose to share here is governed by the terms of service or use between you and the [name website].

Visit the [name of DHS Component] contact page at [address of official website or other official information] for information on how to send official correspondence."