Department of Homeland Security
DHS Directives System
MD Number: 139-01
Revision Number: 00
Issue Date: 07/31/2007

DOMAIN NAMES

I. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the approval and acquisition of Domain Names Services (DNS) for web sites owned or operated by, or on behalf of, DHS and its organizational elements.

II. Scope

This directive applies to all DHS organizational elements.

III. Authorities

A. This directive is governed by Public Laws, regulations, and other directives, such as:

1. Department Of Homeland Security Management Directives: MD 4400.1 – "DHS WEB (INTERNET, INTRANET, AND EXTRANET INFORMATION) AND INFORMATION SYSTEMS."

2. Request for Comments (RFC) 2146 titled "U.S. Government Internet Domain Names."

a. In May 1997, the General Services Administration (GSA) issued RFC 2146, which described the registration policies for the top-level domain ".GOV". The purpose of RFC 2146 was to establish a single identifiable Internet name for each U.S. Federal government agency.

b. RFC 2146 restricts Domain Name registration to coincide with the approved structure of the U.S. Government, as listed in the document "Codes for the Identification of Federal and Federally Assisted Organizations," Federal Information Processing Standards (FIPS) 95-1 (or its successor). RFC 2146 provides for waivers to this restriction to be granted based upon the advice of the agency Chief Information Officer.

3. For more information on the .GOV naming convention visit: <http://www.dotgov.gov/dnc.aspx>.

B. References:

1. RFC 1480 - The U.S. Domain: <http://www.dotgov.gov/help_rfc1480.aspx>.

2. RFC 2146 - U.S. Government Internet Domain Names: <http://www.dotgov.gov/help_rfc2146.aspx>.

3. Final Rule - 41 Code of Federal Regulations (CFR) Part 101-35: <http://www.dotgov.gov/help_fr16jn99-11.aspx>.

4. Final Rule - 41 CFR Part 102-173: <http://www.dotgov.gov/final_rule_102.aspx>.

5. 8 United States Codes (USC) 1363a: <http://www.access.gpo.gov/uscode/uscmain.html>.

6. 19 USC 2081: <http://www.access.gpo.gov/uscode/uscmain.html>.

IV. Definitions

A. ***Domain Name***: A domain name is a human-friendly name (such as "WWW.DHS.GOV") that is resolved (i.e., translates domain names into Internet Protocol addresses) by a network of Domain Name Service (DNS) servers to a specific Internet Protocol (IP) address, which is in turn, associated with a single host (referring to a single server or server cluster). Familiar top-level domains include .COM, .EDU, .MIL, .GOV, .ORG, and .US. While "DHS.GOV" is an example of a second-level domain, "WWW.DHS.GOV" and "DHSONLINE.DHS.GOV" are examples of third-level domains. In each case, the domain name is associated with a single IP address and web server. A web address or Uniform Resource Locator (URL) often contains additional directory and filename information following the domain name, such as <www.dhs.gov/directory/filename.htm>.

B. ***Domain Name Service (DNS)***: An Internet service that translates domain names into IP addresses.

C. ***DHS Organizational Element***: The term "DHS Organizational Element" is defined in MD 0010.1, Management Directives System and DHS Announcements.

D. ***DHS Owned Domain Name***: Domain names registered by DHS, or any of its organizational elements, are considered "owned" by DHS.

E. ***DHS Sponsored Domain Name***: Domain names hosted, maintained, and/or subsidized by DHS, or any of its organizational elements, are considered "sponsored" or "operated on behalf of" DHS.

F. ***Internet Protocol (IP) Address***: An identifier for a computer or device on a Transmission Control Protocol/Internet Protocol (TCP/IP) network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The IP address uniquely identifies each device on the network. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example: 10.119.123.200 could be an IP address.

G. ***Uniform Resource Locator (URL)***: The global address of documents and other resources on the Internet. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located. For example, the URL below specifies a web page that should be obtained using the Hyper Text Transfer Protocol (HTTP) protocol: <http://www.dhs.gov/directory/filename.htm>.

H. ***Web Site***: A web site is a collection of files (web pages and documents) on a particular subject that includes a beginning file called a “home page”.

V. Responsibilities

A. ***The DHS Chief Information Officer (CIO)***: Shall be responsible for all aspects of this directive. Specifically, the DHS CIO is responsible for:

1. Approving all third-level DHS.GOV domain names (e.g., “CBP.DHS.GOV”).

2. Approving all second-level non-DHS.GOV domain names owned or sponsored by DHS (e.g., “READY.GOV”).

3. Approving Domain Administrators for third-level DHS.GOV domain names.

4. Approving Domain Administrators for second-level non-DHS.GOV domain names.

B. ***The DHS Domain Name Registrar***: Shall be approved by the DHS CIO and designated as the administrative contact for all new domain names owned or sponsored by the Department. The DHS Domain Name Registrar is responsible for:

1. Tracking all domain name requests within the Department.

2. Presenting domain name requests to the DHS CIO for approval where appropriate.

3. Providing guidance to domain name requestors and Domain Administrators regarding established naming conventions, recommendations, and templates.

C. ***Domain Administrators***: Shall be identified for third-level DHS.GOV domains (e.g., “CBP.DHS.GOV”) and second-level non-DHS.GOV domains (e.g., “READY.GOV”). With the domain name request, the requestor will recommend a Domain Administrator, subject to the DHS CIO's approval. Domain Administrators are responsible for:

1. Approving sub-domain names for those domains for which they are the Administrator.

2. Registering approved sub-domain names with the DHS Domain Name Registrar.

3. Ensuring domain names are maintained either via a technical staff and/or out-sourced DNS hosting service.

4. Ensuring that the DHS Domain Name Registrar is informed when domain names are decommissioned.

D. ***The requesting DHS organizational element***: Is responsible for preparing a request to the appropriate Domain Administrator or DHS CIO (via the DHS Domain Name Registrar) for review and approval of all new domain names. The DHS organizational element’s Chief Information Officer, or other appropriate executive/manager, should sign or approve the request.

VI. Policy & Procedures

A. ***Policy***:

1. The registration of all domain names owned or sponsored by DHS shall be in accordance with Request for Comments (RFC) 2146 - "U.S. Government Internet Domain Names", and compliant with standard Internet naming conventions for U.S. Federal agencies using the .GOV top-level domain. RFC 2146 can be found at <http://www.dotgov.gov/help_rfc2146.aspx>.

2. The standard second-level domain for all DHS public Internet, intranet and extranet domain names shall be DHS.GOV (i.e., all domain names will end with "DHS.GOV"). Exceptions to this policy may be requested through the DHS Domain Name Registrar and are subject to approval by the DHS CIO. For second-level DHS public Internet domain names, the Public Affairs Office will review and concur with the domain names for consistent name branding.

3. Alternate second-level domain names (such as “READY.GOV”) may be requested through the DHS Domain Name Registrar and are subject to approval by the DHS CIO. This includes all potential second-level domain names owned or sponsored by DHS regardless of the top-level domain. (i.e., .GOV, .MIL, .COM, .US, etc.) All DHS-sponsored web sites must be registered as .GOV domain sites unless approved otherwise by the DHS CIO or his/her designee.

4. Third-level DHS.GOV domain names (such as “VENDORS.DHS.GOV”) may be requested through the DHS Domain Name Registrar and are subject to approval by the DHS CIO. The requesting DHS organizational element must submit, with the domain name request, the recommendation of an individual who will act as the Domain Administrator. If the third-level domain name and recommended individual are approved, the Domain Administrator will be granted the delegated authority to review and approve or reject requests for fourth-level domain names.

5. Requests for fourth-level domain names based on a third-level DHS.GOV domain may be reviewed and approved or rejected by the appropriate third-level Domain Administrator. Approved domain names must then be registered with the DHS Domain Name Registrar.

6. Requests for third- or fourth-level domain names not based on DHS.GOV may be reviewed and approved or rejected by the appropriate second-level Domain Administrator. Approved domain names must then be registered with the DHS Domain Name Registrar.

7. Existing DHS domain names which provide well established name recognition for general public and other government agencies are grandfathered from this directive unless new DHS policies state otherwise.

8. United States Codes 19 USC 2081 and 8 USC 1363a, allow Immigrations and Customs Enforcement (ICE) investigative agents to conduct certain investigative operations in an undercover capacity exempt from specific federal regulations and laws. As a result of this statutory exemption, ICE investigative agents in DHS organizational elements are allowed to establish undercover Internet domain names for investigative purposes without seeking DHS approval, provided the ICE General Counsel has oversight of these undercover operations.

B. ***Procedures***:

These procedures are applicable for Internet, intranet and extranet domain names:

1. Second-level domains

2. Second-level domain requestors (e.g., “DHS.GOV”) shall submit a written or electronic request to the DHS Domain Name Registrar. This request should be signed or approved by the requestor’s Chief Information Officer or Program Director.

a. The DHS Domain Name Registrar will ensure the request adheres to DNS policy and standards. The DHS Domain Name Registrar also verifies through the NIC.GOV domain name registration that the requested domain name is available.

b. If the request is denied by the DHS Domain Name Registrar, the requestor is sent a response explaining why the request is not approved and is given instructions on how to register again.

c. If the request is approved, a letter is generated and submitted to the DHS CIO for review and approval. If the DHS CIO has denied the request, the requestor is sent a response explaining why the request was denied. If the request is approved, the DHS DNS Registrar reserves the domain name with NIC.GOV.

d. The DHS Domain Name Registrar forwards the request to the DHS CIO’s DNS team to be added to the DNS database. Notification is provided to the requestor when the action is complete.

3. Third-level domains

a. Third-level domain requestors (e.g., “CBP.DHS.GOV”) shall submit a written or electronic request to the DHS Domain Name Registrar. This request should be signed or approved by the organization’s Chief Information Officer or Program Director.

b. The DHS Domain Name Registrar will ensure the request adheres to DHS DNS policy and standards. The DHS Domain Name Registrar also verifies that the requested domain name does not already exist in the current database.

c. If the request is denied, the requestor is sent a response explaining why the request is not approved and is given instructions on how to register again. If the request is approved, a letter is generated and submitted to the DHS CIO for approval.

d. If the DHS CIO has denied the request, the requestor is sent a response explaining why the request was denied. If the request is approved, the DHS DNS Registrar reserves the domain name.

e. The DHS Domain Name Registrar forwards the request to the DHS CIO’s DNS team to be added to the DNS database. Notification is provided to the requestor when the action is complete.

4. Fourth/Fifth-level domains

a. Fourth/Fifth level domain requestors (e.g., “OCNAC.CBP.DHS.GOV”) shall submit a written or electronic request to the owner of the applicable third-level domain. This request should be signed or approved by the organization’s Chief Information Officer or Program Director.

b. Once the request is approved by the third-level domain owner, the request is forwarded to the DHS Domain Name Registrar to ensure the request adheres to DNS policy and standards.

c. If the request is denied, the requestor is sent a response explaining why the request is not approved and is given instructions on how to register again. If the request is approved, the DHS Domain Name Registrar forwards the request to the DHS CIO’s DNS team for action.

d. Notification is provided to the requestor when the action is complete.

C. ***Internet .GOV Domain Names Fee***.

1. On July 1, 2004, the General Services Administration's (GSA) Federal Technology Service (FTS) began charging for Internet .GOV domain names. This fee applies to new registration and existing Internet .GOV second level domain names. GSA also requires departments and agencies to renew their domain names one year from the date of registration. The fee structure is required to recover a portion of the operating expenses for the Internet .GOV Domain Registry. Failure to pay required fees for renewing or registering domain names will result in releasing that domain name to the available pool.

2. For each second-level DHS domain name that is registered with NIC.GOV, the administrative Point of Contact (POC) and billing POC should keep their contact information up to date for billing purposes.

D. ***Questions or Concerns Regarding the Process***: Any questions or concerns regarding this directive should be addressed to the DHS CIO or DHS Domain Name Registrar.