Department of Defense
INSTRUCTION

SUBJECT: Internet Domain Name Use and Approval

References: See Enclosure 1

1. PURPOSE. This Instruction:

    a. Establishes .MIL as the Top Level Domain (TLD) required to be used by the Department of Defense.

    b. Provides procedures for the approval, registration, and use of Internet domain names in the Department of Defense.

    c. Implements policy and assigns responsibilities to comply with domain name requirements in Reference (a).

2. APPLICABILITY AND SCOPE

    a. This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

    b. This Instruction does not apply to domain names used for communications internal to a DoD Component (e.g., private Local Area Networks), nor domain names used for non-operational purposes (e.g., research, developmental, and testing networks).

3. DEFINITIONS. These terms and their definitions are for the purpose of this Instruction only.

    a. access-controlled. Available to authorized users through effective restrictive measures. Domain and/or Internet Protocol (IP) address restriction is not an effective method of access control. Such restrictions are easily defeated. The current version of the Security Technical

Information Guide, "Access Control in Support of Information Systems," published by the Defense Information Systems Agency (DISA) at http://iase.disa.mil/stigs/stig, provides guidance.

b. <u>forward address name service</u>. Provides the ability to translate a domain name address to its assigned machine-readable IP address.

c. <u>name servers</u>. The machines and software services that translate between human-readable domain names and machine-readable IP addresses.

d. <u>publicly accessible</u>. Access is not limited. Includes Web sites and other information technologies that have very limited access controls such as domain and/or IP address restrictions.

e. <u>reverse address name service</u>. Provides the ability to translate a machine-readable IP address to its assigned domain name. Referred to as "in-addr.arpa" in the case of Internet Protocol Version 4 (IPv4), and "ip6.arpa" in the case of IPv6.

f. <u>WHOIS</u>. The name of Internet and operating system services that provide registration information by domain names, IP addresses, and/or personal identification codes. The term is not an acronym.

4. <u>POLICY</u>. It is DoD policy to:

a. Conduct DoD publicly-accessible and access-controlled, Internet-based communications (e.g., electronic mail and Web operations) under the Internet domain established for the Department of Defense, the .MIL TLD. Enclosure 2 describes the delegation of this TLD to the Department and the purpose of other major TLDs. Enclosure 3 lists exceptions and situations that may warrant special approval for the use of other TLDs.

b. Use the .MIL domain to provide names only for IP addresses allocated or assigned to the Department of Defense by the American Registry for Internet Numbers.

c. Use .MIL and other acquired domains only on networks that meet DoD information assurance certification and accreditation requirements of DoD Instruction 8510.01 (Reference (b)) and are approved to operate by the responsible Designated Approval Authority, as defined in DoD Directive 8500.1 (Reference (c)).

d. Not use .MIL domain names that redirect to non-.MIL domain named hosts (e.g., name.mil will not redirect to name.com).

5. <u>RESPONSIBILITIES</u>. See Enclosure 4.

6. <u>PROCEDURES</u>. See Enclosure 5.

7. <u>INFORMATION REQUIREMENTS</u>

    a. The information requirements in this Instruction are exempt from licensing in accordance with paragraph C4.4.2. of DoD 8910.1-M (Reference (d)).

    b. Application templates, registration templates, and guidance are maintained on the DoD Network Information Center/SIPRNet Support Center (NIC/SSC) Web Site at http://www.nic.mil.

8. <u>RELEASABILITY</u>. UNLIMITED. This Instruction is approved for public release. Copies may be obtained through the Internet from the DoD Issuances Web Site at http://www.dtic.mil/whs/directives.

9. <u>EFFECTIVE DATE</u>. This Instruction is effective immediately.

John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures
1. References
2. Internet Domain Name Structure and Delegation
3. Specific Rules for DoD Internet Domain Name Use and Approval
4. Responsibilities
5. Procedures
6. DoD Component .GOV Domain Approval Justification Template
7. DoD Component CIO .GOV Domain Request Letter Template

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a)   Office of Management and Budget (OMB) Memorandum 05-04, "Policies for Federal Agency Public Websites," December 17, 2004[1]

(b)   DoD Instruction 8510.01, "DoD Information Assurance Certification and Approval Process (DIACAP)," November 28, 2007

(c)   DoD Directive 8500.01E, "Information Assurance," October 24, 2002

(d)   DoD Manual 8910-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998

(e)   International Organization for Standardization Standard Number 3166-1, "Country Name Codes," 2006 or current edition[2]

(f)   Request for Comments 1480, "The US Domain," June 2003[3]

(g)   DoD Instruction 1015.10, "Programs for Military Morale, Welfare, and Recreation (MWR)," November 03, 1995

(h)   Parts 102 through 173 of title 41, Code of Federal Regulations

(i)   DoD Directive 5144.01, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005

(j)   National Institute of Standards and Technology Special Publication 800-87, "Codes for the Identification of Federal and Federally Assisted Organizations," March 2007

---

[1] Listed with Memorandums in the OMB section of the White House Web site (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-04.pdf).

[2] http://www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm

[3] http://www.isi.edu/in-notes/rfc1480.txt

ENCLOSURE 2

INTERNET DOMAIN NAME STRUCTURE AND DELEGATION

1. In the Domain Name System (DNS) naming of computers, there is a hierarchy of names. There is a set of "top-level domain names" (TLDs). These are the generic TLDs and the two letter country codes from International Organization for Standardization (ISO) Standard Number 3166 (Reference (e)). The Internet Assigned Numbers Authority (IANA) provides a list of the generic TLDs that presently includes twenty domains and descriptions.

2. A hierarchy of names usually exists under each TLD. For example, .MIL is a TLD, .OSD.MIL is a Second Level Domain (SLD) and TRICARE.OSD.MIL is a Third Level Domain (not usually referred to with an acronym).

3. Each of the generic TLDs was created for a general category of organizations. The country code domains (e.g., FR, NL, KR, US) are each organized by an administrator for that country.

4. All generic TLDs are international in nature, with the exception of two (.MIL and .GOV) that are restricted to use by entities in the United States. Descriptions follow:

    a. .COM - This domain is for commercial entities - companies.

    b. .EDU - Registrations are now limited to four-year colleges and universities. Register schools and two-year colleges in the .US country domain. (See paragraph 4.h.)

    c. .NET - This domain is for the computers of network providers - Network Information Center and Network Operation Center computers, the administrative computers, and the network node computers. The customers of the network provider should have domain names of their own (not in the .NET TLD).

    d. .ORG - This is the miscellaneous TLD for organizations that do not fit anywhere else. Some non-government and non-profit organizations fit here.

    e. .INT - This domain is for organizations established by international treaties or international databases.

    f. .GOV – Agencies of the U.S. Federal government have exclusive use of this domain. State and local agencies use the .US country domain. (See paragraph 4.h.) DoD Components do not generally qualify for use of this domain.

    g. .MIL – The U.S. Department of Defense has exclusive use of this domain.

    h. .US – The country domain, .US, provides for the registration of all kinds of entities in the United States on the basis of political geography, that is, a hierarchy of <entity-name>.<locality>.<state-code>.US (for example, "NATIONALGUARD.MEMPHIS.TN.US").

Branches of the .US domain are used within each state for schools (K12), community colleges (.CC), technical schools (.TEC), state government agencies (.STATE), councils of governments (.COG), libraries (.LIB), museums (.MUS), and several other generic types of entities. Detailed information on the organization of the .US country domain is available in Request For Comments 1480 (Reference (f)).

    i. Other international domains include .AERO, .ASIA, .BIZ, .CAT, .COOP, .INFO, .JOBS, .MOBI, .MUSEUM, .NAME, .PRO, .TEL and .TRAVEL.

ENCLOSURE 3

SPECIFIC RULES FOR DoD INTERNET DOMAIN NAME USE AND APPROVAL

1. Use of the non-.MIL and non-.GOV domains should be consistent with the exceptions in paragraphs 1.a. through 1.i. and approved by the DoD Component Chief Information Officers (CIOs). Regardless of the Internet domain name and/or hosts used, DoD information assurance policies and requirements for handling DoD information apply.

    a. Subcomponents, such as Reserve Officer Training Corps units that do not fund or operate Internet systems, may use the domains of their hosting organizations or of the organizations that support their Internet communications.

    b. The DoD Education Activity and accredited military institutions that award college or university degrees may use the .EDU domain.

    c. Publicly accessible recruiting Web sites may use the .COM domain.

    d. Morale, Welfare, and Recreation and Armed Services Exchanges may operate non-.MIL domains in accordance with DoD Instruction 1015.10 (Reference (g)) and paragraph 4 of this enclosure.

    e. Within applicable laws, other domains may be used in the temporary, direct support of national security and emergencies.

    f. Other domains may be used for research and development purposes that are temporary and non-operational in nature.

    g. A DoD Component may acquire a non-.MIL SLD or non-.GOV SLD to protect a DoD Component trademark or to prevent the domain name from being used in a manner that would be confusing to the public or with conflicting purposes, provided the domain name is held in reserve or used to redirect visitors to a corresponding .MIL domain. In cases involving trademarks, the DoD Component will also require legal review prior to such acquisition.

    h. A DoD Component may be represented through a non-.MIL SLD or non-.GOV SLD when participating in a public-private partnership information system where most of the content is non-government, but where the government shares data and shares in the funding.

    i. A DoD Component may be represented through a non-.MIL SLD or non-.GOV SLD when using specialized business services or processes on contracted commercial systems not connected to the NIPRNet or SIPRNet and not reliant on access control mechanisms used in the .MIL domain (e.g., Army/Navy Knowledge Online credentials and Common Access Card credentials). Generic services such as Web site hosting and electronic mail services do not constitute specialized business services.

2. The DoD Components do not generally qualify for use of the .GOV domain. The General Services Administration (GSA) dotGov Registrar requires DoD CIO approval to process applications for .GOV domain names according to parts 102 through 173 of title 41, Code of Federal Regulations (Reference (h)). Applications for DoD CIO approval must clearly describe special needs or requirements that are not satisfied in the .MIL domain. The DoD Component CIOs must endorse applications prior to DoD CIO approval. Examples of special needs or requirements for use of the .GOV domain that may be approved include:

    a. Inability of Global Information Grid (GIG) assets to support the operations in the .MIL domain, as documented by a waiver granted through DoD CIO governance processes.

    b. Exceptional public expectation to find Secretary of Defense (cabinet-level) information at a .GOV address (e.g., defense.gov, dod.gov, and pentagon.gov).

    c. An international program for which the Department of Defense is the lead agency representing the United States.

    d. A government-wide program for which the Department of Defense is chartered as the executive agent or host and funded to represent multiple Federal, State, and local governments and/or non-government entities.

3. Web sites and other Internet media in domains specifically funded by, registered to, or exclusively used by the Department of Defense, and visible to or distributed to the public shall not be used to advertise or market private individuals, commercial firms, corporations, or not-for-profit firms. Such media must not imply in any manner that the Department of Defense endorses or favors any specific commercial or not-for-profit product, commodity, or service.

4. The DoD Component CIOs must track all SLDs acquired/used by the DoD Components. Tracking additional subdomains is encouraged, but optional.

ENCLOSURE 4

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO shall:

a. Issue policies and procedures for use of all Internet domains in the Department of Defense consistent with DoD Directive 5144.01 (Reference (i)).

b. Decide approval of DoD Component requests to use the .GOV domain.

c. Adjudicate DoD Component appeals to requests for .MIL SLDs that are disapproved by the DISA.

2. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Require the use of .MIL TLD as the primary TLD in their functional areas and their respective Components. Enclosure 3 lists exceptions and situations that may warrant special approval for the use of other TLDs.

b. Ensure DoD Component CIOs:

(1) Track all SLDs used by the DoD Components.

(2) Manage and administer the subdomains assigned to them by DISA or approved for the DoD Components' use.

(3) Annually verify administrative and technical contact information is correct in the registrations maintained at the DoD Network Information Center/SIPRNet Support Center (DoD NIC/SSC) and at the General Services Administration's Government Domain Registration and Services Web site (hereafter referred to as the "dotGov Web site") at http://www.dotgov.gov.

3. DIRECTOR, DISA. The Director, DISA, shall:

a. Manage and administer the .MIL, .SGOV.GOV, and associated subdomains on the NIPRNet and SIPRNet and maintain the associated registration databases.

b. Operate the Department of Defense Domain Name Service (.MIL) for DoD networks.

c. Serve as the registrar for .MIL and maintain the .MIL registration database.

d. Manage domain name registration and IP address allocation on an enterprise basis to promote interoperability and security.

ENCLOSURE 5

PROCEDURES

1. APPLICATION FOR AND REGISTRATION OF DOMAINS

    a. All applications for and registration of domains must be coordinated with and approved by the respective DoD Component CIOs. The DoD CIO and DISA will only accept applications from or endorsed by designees in the offices of DoD Component CIOs. New SLDs will only be issued to DoD Component CIOs or their designees.

    b. The DoD subcomponents must apply for subdomains of existing SLDs via the DoD Component CIO to which the SLD is assigned. Assignments and contacts for the .MIL and .GOV SLDs can be found via the WHOIS services on the Web sites of the DoD NIC/SSC and the dotGov Web site, respectively.

2. APPLICATION FOR .MIL SLDS

    a. Subcomponents under major DoD Components cannot be registered as a SLD under the .MIL domain, and must register through their respective DoD Component domain administrators.

    b. The SLDs under .MIL will be descriptive of the organizations they will serve. A domain name length of 12 characters or less is preferred, and must be unique (first come is first served if duplicates occur). Only the characters A through Z, a through z, numerals 0 through 9, and hyphen "-" may be used in domain names.

    c. Each SLD under .MIL will be supported by at least two name servers. The following applies to name servers supporting domains in the .MIL domain:

        (1) The networks on which the name servers are located must have both forward and reverse address name services.

        (2) The name servers must be registered at the DoD NIC/SSC.

        (3) The administrators of name servers must comply with all policies and directives that pertain to:

            (a) The registration and administration of nodes in the .MIL domain.

            (b) The administration of nodes for the service or agency that the subdomain supports.

(4) The administrative contact and the technical contact must have email addresses that are in the .MIL domain (must end with .MIL). The host servers for these addresses must be registered with the DoD NIC/SSC. The administrative and technical contact information must be updated and verified annually.

d. The DoD Component CIOs or their designees must use the Domain Template in the NIPRNet Registration section of the DoD NIC/SSC Web site to request the creation of a .MIL SLD.

e. The DoD NIC/SSC will process the request on receipt of an error-free application consisting of the completed Domain Template, supporting justification, and the organizational charter. Incomplete submissions will not be processed. The DoD NIC/SSC will assess initial submissions and provide guidance within 72 hours. The approval decision will routinely be made within 2 weeks of complete and accurate submission of required information and documentation. Priority actions will be handled on an expedited basis.

f. The DoD NIC/SSC will notify the administrative and technical contacts of its decision via e-mail.

3. <u>APPLICATION FOR .GOV SLDS</u>

a. Applications must comply with the registration guidance and procedures published at the dotGov Web site.

b. The DoD Component CIO and the DoD CIO must approve the acquisition and use of a .GOV SLD before it is registered at the dotGov Web site. Applications must include identification of funds and a credit card holder to function as the billing contact for the registration and maintenance fees established by the General Services Administration.

c. The DoD Component CIOs must also:

(1) Complete the DoD Component .GOV Domain Approval Justification and the DoD Component CIO .GOV Domain Request Letter. (See templates, Enclosures 6 and 7.) Transmittal of copies as attachments to digitally-signed email to domain-application@osd.mil is preferred.

(2) Initiate the registration process at the dotGov Web site on receipt of DoD CIO approval. The .GOV SLD will be held until final approval and activation by the dotGov Registrar.

(3) The DoD CIO will review the DoD Component Internet Domain Approval Justification and the DoD Component CIO .GOV Domain Request Letter. On approval, the DoD CIO will send the required cabinet-level CIO endorsement to the dotGov Registrar.

d. The dotGov Registrar will notify all registered contacts of the approval decision.

e. The DoD Component billing contact must then log in to the dotGov Web site and pay the registration fee with a credit card before the new .GOV SLD will be activated.

4. APPLICATION FOR .SMIL.MIL AND/OR .SGOV.GOV SUBDOMAINS

a. U.S. Government and DoD Component CIOs must use the SIPRNet Domain Template in the SIPRNet Registration section of the DoD NIC/SSC Web site to request the creation of third-level domains under either .SMIL.MIL or .SGOV.GOV.

b. The DoD NIC/SSC will process the request on receipt of an error-free application consisting of the SIPRNet Domain Template, supporting justification and the organizational charter. The DoD NIC/SSC will assess initial submissions and provide guidance within 72 hours. The approval decision will routinely be completed within two weeks of complete and accurate submission of required information and documentation. Priority actions will be hastened.

c. The .SGOV.GOV domain is to be used by non-DoD agencies of the U.S. Government (USG) that require access to the SIPRNet. Only those USG Federal-level agencies that would qualify for an SLD under the .GOV domain, as listed in National Institute of Standards and Technology (NIST) Special Publication 800-87 (Reference (j)), may register as a third level domain under the .SGOV.GOV domain. Those qualifications are defined as follows:

(1) Top-level entities (e.g., those with codes ending in 00 such as "1200 Department of Agriculture"), and independent agencies and organizations (e.g., National Science Foundation) are eligible for registration directly under .GOV.

(2) Autonomous law enforcement components of top-level entities (e.g., Federal Bureau of Investigation, Secret Service, Coast Guard) are eligible for registration.

(3) Cross-agency collaborative organizations (e.g., Federal Networking Council, Information Infrastructure Task Force) are eligible for registration under .GOV on presentation of the chartering document and are the only organizations not listed in NIST Special Publication 800-87 (Reference (j)) eligible for registration under .GOV.

(4) Subsidiary, non-autonomous components of top-level or other entities are not eligible for separate registration. International organizations listed in NIST Special Publication 800-87 (Reference (j)) are not eligible for registration under .GOV.

(5) Organizations listed as "Federally Aided Organizations" are not eligible for registration under .GOV and should register under .ORG or other appropriate TLD.

(6) A domain name should be derived from the official name for the organization (e.g., USDA.SGOV.GOV or Agriculture.SGOV.GOV). The registration shall be listed in the

registration database under the official name for the organization or under the name in the organization's chartering document.

d. Only one registration and delegation shall be made per agency. The domain name length is preferred to be 12 characters or less and must be unique (first come is first served if duplicates occur).

e. Only registered customers of the .SGOV.GOV domain will receive the services provided by DoD NIC/SSC personnel for .SGOV.GOV domains.

f. All name servers supporting a third level or lower level domain under .SGOV.GOV or .SMIL.MIL must be registered at the DoD NIC/SSC. Each domain is required to have at least two name servers. Name servers should be members of separate networks, i.e., not on the same local area network (LAN) nor connected to the same router.

g. All hosts in the .SGOV.GOV domain or in any of its subdomains must be registered at the DoD NIC/SSC.

h. Reverse address name service for networks will be provided through registration at the DoD NIC/SSC (DoD NIC/SSC maintains the .ARPA, IN-ADDR.ARPA, and IP6.ARPA domains for the SIPRNet).

5. TRACKING

a. The .MIL, .SMIL.MIL, .GOV and .SGOV.GOV domains are automatically registered as part of the application process. No additional procedures are necessary.

b. The DoD Component CIOs must establish a system for tracking use of all other domains acquired and used by the DoD Components.

ENCLOSURE 6

DoD COMPONENT .GOV DOMAIN APPROVAL JUSTIFICATION TEMPLATE

1. Domain Requested: _____

2. Projected length of use: _____

3. Provide narrative verification of compliance with 41 Code of Federal Regulations Part 102-173, "Federal Management Regulation; Internet GOV Domain" and the GSA .GOV Program Guidelines.

4. Describe the specific mission requirement that the domain will support. Provide supporting law, policy, or DoD issuance reference(s) if applicable.

5. Describe specific inadequacies of the .MIL domain in meeting the mission requirement and provide copies of any waivers granted through DoD CIO governance processes.

6. Provide evidence of the DoD Authority to Operate (ATO) or Interim ATO to verify that the IT system supported by the domain is certified and approved as required by the DoD Instruction 8510.01, "DoD Information Assurance Certification and Approval Process (DIACAP)," November 28, 2007.

7. If the domain will be used in a manner that allows public viewing of information, identify the office/person (including contact information) that will be conducting the public affairs and Operations Security reviews as required by DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996.

8. Contact information for questions about this justification:
    [*Name, E-mail Address, Telephone*]

ENCLOSURE 7

DoD COMPONENT CIO .GOV DOMAIN REQUEST LETTER TEMPLATE

Department of Defense Chief Information Officer
CIO Management Services
6000 Defense Pentagon
Washington, DC 20301-6000

Attn: Internet Domain Name Manager

As the [*DoD Component name*] Chief Information Officer, I formally request that authority over the [*desired second level name*].gov second-level domain name be delegated to the [*DoD Component name*]. The [*DoD Component name*] will ensure payment via credit card of the annual $125.00 domain name fee and will also ensure that use of the requested domain name conforms to the DoD Internet regulations and guidelines.

This domain name is consistent with the Department's Internet policies. It will be used for [*name of program and purpose*].

[*Mr./Ms. first name, last name*] is the administrative contact for [*xxxxxx.gov*] and can be reached at [*telephone number*] or via email at [*email address*]. [*Mr./Ms. first name, last name*] is the billing contact and can be reached at [*phone number*] or via email at [*email address*]. Thank you for your assistance in this matter.

Sincerely,

[*DoD Component name*] Chief Information Officer

Attachments: