Department of Defense
INSTRUCTION

NUMBER 8410.01
December 4, 2015

DoD CIO

SUBJECT: Internet Domain Name and Internet Protocol Address Space Use and Approval

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Instruction (DoDI) 8410.01 (Reference (a)) in accordance with the authority in DoD Directive 5144.02 (Reference (b)).

b. Establishes *.mil* as the top-level domain (TLD) required to be used by the DoD and policies for its use.

c. Provides procedures for the approval, registration, and use of Internet domains and names in the DoD.

d. Implements policy and assigns responsibilities to comply with TLD requirements in Office of Management and Budget (OMB) Memorandum 05-04 (Reference (c)).

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint 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 DoD (referred to collectively in this instruction as the "DoD Components").

b. Does **not** apply to TLDs used for communications internal to a DoD Component (e.g., private local area networks) or to TLDs used for non-operational purposes (e.g., research, developmental, and testing networks).

3. POLICY. It is DoD policy to:

a. Conduct DoD public and private Internet-based communications (e.g., electronic mail and Web operations) under the TLD established for the DoD—the *.mil* TLD—in accordance with Reference (c). Enclosure 2 describes the delegation of this TLD to the DoD 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 DoD by the American Registry for Internet Numbers.

c. Use *.mil* and other acquired domains only on networks that are approved to operate by the responsible authorizing official, in accordance with DoDIs 8510.01 and 8500.01 (References (d) and (e)).

d. Not use *.mil* or *.gov* domain names that redirect to non-*.mil* or non-*.gov* domain named hosts (e.g., *name.mil* must not redirect to *name.com*). The only exception is for an approved and accredited service that provides redirection not readily apparent to the end user (e.g., use of a content delivery service or cloud service).

e. Use DoD IP number resources only on networks that are approved to operate by the responsible authorizing official, in accordance with Reference (d) and Reference (e).

f. Assign and register DoD IP address space in accordance with the DoD NIC Registry Protocol 9802 (Reference (f)).

4. RESPONSIBILITIES. See Enclosure 4.

5. PROCEDURES. See Enclosure 5.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction is effective December 4, 2015.

Terry A. Halvorsen
DoD Chief Information Officer

Enclosures

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 8410.01, "Internet Domain Name Use and Approval," April 14, 2008 (hereby cancelled)
(b) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(c) Office of Management and Budget Memorandum, "Policies for Federal Agency Public Websites," December 17, 2004[1]
(d) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014
(e) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(f) DoD Network Information Center Registry Protocol 9802, "Assignment and Registration of Internet Protocol (IP) Address Space and IP Number Resources," January 2015[2]
(g) International Organization for Standardization Standard Number 3166-1, "Country Name Codes," current edition[3]
(h) Network Working Group Memorandum, Request for Comments 1480, "The US Domain," June 1993[4]
(i) DoD Instruction 1015.10, "Military Morale, Welfare, and Recreation (MWR) Programs," July 6, 2009
(j) Title 41, Code of Federal Regulations
(k) DoD 5500.7-R, "The Joint Ethics Regulation," November 17, 2011
(l) National Institute of Standards and Technology, "Codes for the Identification of Federal and Federally Assisted Organizations," April 25, 2008

[1] http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-04.pdf
[2] https://www.nic.mil/webmenu/docfiles/registry_protocol_9802.pdf
[3] http://www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm
[4] http://tools.ietf.org/pdf/rfc1480.pdf

ENCLOSURE 2

INTERNET DOMAIN NAME STRUCTURE AND DELEGATION

1. The Domain Name System (DNS) includes a hierarchy of names that begins with a set of TLD names, including the generic top-level domains (gTLDs), the two-letter country code top-level domains (ccTLDs), and others. The Internet Assigned Numbers Authority provides a complete list of all TLDs at https://data.iana.org/TLD/tlds-alpha-by-domain.txt. Each of the gTLDs was created for a general category of organization and is used internationally. The ccTLDs (e.g., *.fr*, *.nl*, *.kr*, *.us*) are based on codes in the International Organization for Standardization Standard Number 3166-1 (Reference (g)) and each is organized by an administrator for that country. Under each TLD exists sublevels separated by periods. 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).

2. All gTLDs are international in nature, with the exception of *.mil* and *.gov*, which are restricted to use by entities in the United States.

a. The *.com* domain is for commercial entities or companies.

b. The *.edu* domain is for certain educational entities. Registrations are limited to U.S. postsecondary institutions (i.e., after K-12) that an agency on the Department of Education's list of Nationally Recognized Accrediting Agencies institutionally accredits. Only an entire accredited institution—not merely one accredited program—may use this domain. Registration for K-12 and other schools not meeting the above criteria should use the *.us* country domain. (See paragraph 4h of this enclosure)

c. The *.net* domain is for the computers of network providers, including network information center and network operation center computers, their administrative computers, and their network node computers. The customers of the network provider should have domain names of their own (not in the *.net* TLD).

d. The *.org* domain is the miscellaneous TLD for organizations that do not fit elsewhere. Certain non-government and non-profit organizations fall into this category.

e. The *.int* domain is for organizations established by international treaties or international databases.

f. The *.gov* domain is for the exclusive use of agencies of the U.S. Government, the State and local governments, and federally-recognized Indian tribes and Alaskan Native groups. DoD Components generally do not qualify for use of this domain. The use of the *.gov* domain in the DoD must be approved by the DoD Component Chief Information Officer (CIO), the DoD CIO, and the OMB, in accordance with section 3 of Enclosure 5 of this instruction.

g. The *.mil* domain is for the exclusive use of the DoD.

h. The *.us* country domain provides for the registration of various types of entities in the United States on the basis of political geography: a hierarchy of <entity-name>.<locality>.<state-code>.*us* (e.g., "*nationalguard.richmond.virginia.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 the Network Working Group Memorandum (Reference (h)).

ENCLOSURE 3

SPECIFIC RULES FOR DOD INTERNET DOMAIN NAME USE AND APPROVAL

1. DoD cybersecurity policies and requirements for handling DoD information apply regardless of the Internet domain name or hosts used.

2. Use of the non-*.mil* and non-*.gov* domains must be consistent with the exceptions in paragraphs 2a through 2i of this enclosure and be approved by the DoD Component CIOs. For the purposes of this instruction, DoD Component CIOs include senior information resources management officials in the DoD Components that do not have a CIO.

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. Public recruiting websites may use the *.com* domain.

d. Morale, Welfare, and Recreation and Armed Services Exchanges may operate non-*.mil* domains in accordance with DoDI 1015.10 (Reference (i)) and section 4 of this enclosure.

e. Other domains may be used in the temporary, direct support of national security and emergencies as permitted by applicable laws.

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

g. A DoD or OSD Component may acquire a non-*.mil* SLD or non-*.gov* SLD to protect a DoD or OSD Component trademark or to prevent the domain name from being used in a manner that would be confusing to the public or have conflicting purposes, provided the domain name is held in reserve or used to redirect visitors to a corresponding *.mil* or *.gov* domain. In cases involving trademarks, the DoD Component must obtain legal review before 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 that are not connected to the Non-classified IP Router Network or the Secret IP Router Network (SIPRNet) and are not reliant on access control mechanisms used in the *.mil* domain (e.g., Common Access

Card credentials). Generic services such as website hosting and e-mail services do not constitute specialized business services.

3. The DoD Components generally do not qualify for use of the *.gov* domain. The General Services Administration (GSA) Government Domain Registration and Services Website (referred to in this instruction as the "dotGov Website" and found at http://www.dotgov.gov) requires both OMB and DoD CIO approval to process applications for *.gov* domain names, in accordance with parts 102 through 173 of Title 41, Code of Federal Regulations (Reference (j)). Applications for DoD CIO approval must clearly describe special needs or requirements that are not satisfied in the *.mil* domain or an existing SLD. The DoD Component CIOs must endorse applications before DoD CIO approval. Possible examples of special needs or requirements for use of the *.gov* domain include:

a. Inability of DoD information enterprise 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 DoD is the lead agency representing the United States.

d. A government-wide program for which the DoD is chartered as the executive agent or that is hosted and funded to represent multiple federal, State, and local governments or non-government entities.

4. Websites and other DoD Internet services in domains specifically funded by, registered to, or exclusively used by the DoD and visible to or distributed to the public must 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 DoD endorses or favors any specific commercial or not-for-profit product, commodity, or service in accordance with DoD 5500.07-R (Reference (k)).

5. The DoD Component CIOs must maintain a list of all SLDs acquired or used by their DoD and OSD Components. Tracking additional subdomains is encouraged, but optional.

ENCLOSURE 4

RESPONSIBILITIES

1. DOD CIO. In addition to the responsibilities in section 3 of this enclosure, the DoD CIO:

a. Develops policies and procedures for use of all Internet domains in the DoD.

b. Develops policies and procedures for the allocation of IP number resources for organizations utilizing DoD IP networks.

c. Reviews and approves DoD Component requests to use the *.gov* domain.

d. Adjudicates DoD Component appeals concerning requests for *.mil* SLDs that are disapproved by the Defense Information Systems Agency (DISA).

2. DIRECTOR, DISA. In addition to the responsibilities in section 3 of this enclosure and under the authority, direction, and control of the DoD CIO, the Director, DISA:

a. Manages and administers the *.mil*, *.smil.mil*, *.sgov.gov*, and associated subdomains on the classified and unclassified DoD IP networks and maintains the associated registration databases.

b. Operates enterprise DNS for DoD IP networks.

c. Serves as the registrar for *.mil* and maintains the *.mil* and IP number resource registration database.

d. Manages domain name registration and IP number resource allocation on an enterprise basis to promote interoperability and security.

3. DOD AND OSD COMPONENT HEADS. The DoD and OSD Component heads:

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

b. Ensure DoD Component CIOs:

(1) Maintain a list of all SLDs used by their components.

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

(3) Verify annually that the DoD Network Information Center (NIC) and the dotGov Website have maintained correct administrative and technical contact information.

ENCLOSURE 5

APPLICATION 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 accept applications only from or endorsed by government civilian and military designees in the offices of DoD Component CIOs. New SLDs will be issued only 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 DoD NIC Website and the dotGov Website, respectively.

2. APPLICATION FOR .MIL SLDs

a. Subcomponents under major DoD Components cannot be registered as SLDs 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 or functions they will serve. A domain name length of 12 characters or less is preferred and must be unique (generally, the first application will receive the domain name should duplicate applications occur). Only the characters A through Z (upper and lowercase), numerals 0 through 9, and hyphens may be used in domain names.

c. At least two name servers will support each SLD under *.mil*.

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

(2) The name servers must be registered as hosts at the DoD NIC.

(3) At least two of the authoritative name servers for the SLD must be engineered with path diversity to avoid any single point of failure to the extent possible.

(4) SLD name servers must be addressed from registered DoD IP address space.

(5) SLD name servers run only DNS services. Other server functions cannot co-exist on SLD servers.

(6) SLD name servers must be protected by an uninterrupted power supply and backup power source.

(7) Local routers front-ending for SLD name servers must be configured with no IP Source Route function.

(8) 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.

(9) The administrative contact and the technical contact must have e-mail addresses that are in the *.mil* domain (i.e., must end with *.mil*). The host servers for these addresses must be registered with the DoD NIC. The administrative and technical contact information must be updated and verified annually. The administrative contact for an SLD must be a government civilian or an active military member. Technical contacts may be contractor personnel.

d. The DoD Component CIOs or their designees must use the domain template in the registration section of the DoD NIC Website to request the creation of a *.mil* SLD.

e. The DoD NIC 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 will assess initial submissions and provide guidance within 72 hours. The approval decision will be made routinely 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 will notify the administrative and technical contacts of its decision via e-mail.

3. APPLICATION FOR .SMIL.MIL OR .SGOV.GOV SUBDOMAINS

a. All customers must use the SIPRNet domain template in the registration section of the DoD NIC Classified Website to request the creation of third-level domains under either *.smil.mil* or *.sgov.gov*.

b. The DoD NIC will process the request on receipt of an error-free application consisting of the domain template, supporting justification, and the organizational charter. The DoD NIC will assess initial submissions and provide guidance within 72 hours. The approval decision will be completed within 2 weeks of complete and accurate submission of required information and documentation. Priority actions will be handled on an expedited basis.

c. The DoD NIC will only make the *.sgov.gov* domain available to non-DoD customers requiring access to SIPRNet. Only those U.S. Government-level agencies that would qualify for

an SLD under the *.gov* domain, as listed in the National Institute of Standards and Technology Special Publication 800-87 (Reference (l)), may register 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 *.sgov.gov*.

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

(3) Cross-agency collaborative organizations (e.g., Federal Networking Council, Information Infrastructure Task Force) are eligible for registration under *.sgov.gov* on presentation of their chartering documents. These are the only organizations not listed in Reference (k) that are eligible for registration under *.sgov.gov.*

(4) Subsidiary, non-autonomous components of top-level or other entities are not eligible for separate registration. International organizations listed in Reference (l) are not eligible for registration under *.sgov.gov*.

(5) Organizations listed as "Federally Aided Organizations" in Reference (l) are not eligible for registration under *.sgov.gov* and should register under *.org* or another appropriate TLD.

(6) A domain name should be derived from the official name for the organization (e.g., *doc.sgov.gov* or *commerce.sgov.gov*). The registration database must list the domain name registration under the official name for the organization or under the name in the organization's chartering document.

d. Only registered customers of the *.sgov.gov* domain will receive the services provided by DoD NIC personnel for *.sgov.gov* domains.

e. All name servers supporting a third-level or lower level domain under *.sgov.gov* or *.smil.mil* must be registered at the DoD NIC. 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 or connected to the same router).

f. All hosts in the *.sgov.gov* domain or in any of its subdomains must be registered at the DoD NIC.

g. Registration at the DoD NIC will provide reverse address name service for networks (DoD NIC maintains the *.arpa*, *in-addr.arpa*, and *ip6.arpa* domains for the SIPRNet).

4. APPLICATION FOR .GOV SLDS

a. Applications must comply with the registration guidance and procedures published at the dotGov Website and in this instruction. Additionally, 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 GSA.

b. The DoD Component CIOs and the DoD CIO must approve the acquisition and use of a *.gov* SLD before it is registered at the dotGov Website.

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 Figures 1 and 2). The DoD Component CIO .Gov Domain Request Letter must identify three distinct contacts:

(a) Administrative – the government employee who ensures that the domain is used in compliance with federal and DoD policies.

(b) Technical – the government employee or contractor under the direction of DoD who can take immediate action to control the name servers hosting the domain.

(c) Billing – the government employee or contractor under the direction of DoD that pays the annual registration fee.

(2) Send copies as attachments to a digitally-signed e-mail to osd.mc-alex.dod-cio.mbx.domain-applications@mail.mil.

(3) Initiate the registration process at the dotGov Website on receipt of DoD CIO approval. The *.gov* SLD will be held until final approval and activation by the dotGov Registrar.

Figure 1. DoD Component .GOV Domain Approval Justification Template

DOD COMPONENT .GOV DOMAIN APPROVAL JUSTIFICATION

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 Authorization to Operate (ATO) or Interim ATO to verify that the IT system supported by the domain is certified and approved as required by DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014.

7. If the domain will be used in a manner that allows public viewing of information, identify the office or person (including contact information) that will conduct the public affairs and Operations Security reviews as required by DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008.

8. Contact information for questions about this justification:
[NAME, E-MAIL ADDRESS, TELEPHONE]

d. The DoD CIO will review the DoD Component Internet Domain Approval Justification and the DoD Component CIO .Gov Domain Request Letter. Upon approval, the DoD CIO will send the required cabinet-level CIO endorsement to the dotGov Registrar, and a copy to the requesting DoD Component CIO.

Figure 2. DoD Component CIO .GOV Domain Request Letter Template

DoD COMPONENT CIO .GOV DOMAIN REQUEST LETTER TEMPLATE

Department of Defense Chief Information Officer
Information and Performance Management Directorate
6000 Defense Pentagon
Washington, D.C. 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 also will ensure that use of the requested domain name conforms to DoD's Internet regulations and guidelines.

Use of this domain name will be consistent with DoD 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 e-mail at [E-MAIL ADDRESS ENDING IN .MIL]. [MR./MS. FIRST NAME, LAST NAME] is the billing contact and can be reached at [PHONE NUMBER] or via e-mail at [E-MAIL ADDRESS]. [MR./MS. FIRST NAME, LAST NAME] is the technical contact and can be reached at [PHONE NUMBER] or via e-mail at [E-MAIL ADDRESS]. Thank you for your assistance in this matter.

Sincerely,

[DOD COMPONENT NAME] Chief Information Officer

Attachments:

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

f. The DoD Component billing contact must then log in to the dotGov Website and pay the registration fee with a credit card before the new *.gov* SLD will be activated.

5. MONITORING OF DOMAINS

a. The *.mil*, *.smil.mil*, and *.sgov.gov* domains are automatically registered as part of the application process via the DoD NIC. No additional procedures are necessary.

b. The DoD Component CIOs must establish a system for maintaining a list of all other domains acquired and used by their components.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ATO	authorization to operate
ccTLD	country code top-level domain
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoDI	DoD Instruction
GSA	General Services Administration
gTLD	generic top-level domain
IP	Internet protocol
NIC	Network Information Center
SIPRNet	Secret IP Router Network
SLD	second-level domain
TLD	top-level domain

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this instruction.

dotGov Website. The GSA Government Domain Registration and Services Website located at http://www.dotgov.gov/.

forward address name service. A service that translates a domain name address to its assigned machine-readable IP address.

name servers. The machines and software services that translate between human-readable domain names and machine-readable IP addresses.

private. Limited availability to authorized users through effective access control measures, such as restricting the collection, dissemination, storage, or processing of information that has not been cleared and authorized for release to the public. Domain and IP restriction is not an effective method of access control; such restrictions are easily defeated.

public. Unlimited availability to authorized users. This definition includes websites and other information technologies that have very limited access controls, such as domain or IP address restrictions. Collecting, disseminating, storing, or otherwise processing information that has been cleared and authorized for release to the public also falls within the definition of "public." Access controls may be used on public sites, though only to provide for equitable service measurement, customization, and enhancement to all public users with opt in and opt out options (as appropriate) and not for restrictive purposes.

reverse address name service. A service that translates a machine-readable IP address to its assigned domain name. Referred to as "in-addr.arpa" in the case of IP Version 4, and "ip6.arpa" in the case of IP Version 6.

subnet. A logical grouping of connected network devices on an IP network. The practice of dividing a network into two or more networks is called subnetting.

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