Internet Domain Names: Background and Policy Issues

Lennard G. Kruger
Specialist in Science and Technology Policy

October 28, 2009

Congressional Research Service
7-5700
www.crs.gov
97-868

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

Navigating the Internet requires using addresses and corresponding names that identify the location of individual computers. The Domain Name System (DNS) is the distributed set of databases residing in computers around the world that contain address numbers mapped to corresponding domain names, making it possible to send and receive messages and to access information from computers anywhere on the Internet.

The DNS is managed and operated by a not-for-profit public benefit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN). Because the Internet evolved from a network infrastructure created by the Department of Defense, the U.S. government originally owned and operated (primarily through private contractors) the key components of network architecture that enable the domain name system to function. A 1998 Memorandum of Understanding (MOU) between ICANN and the Department of Commerce (DOC) initiated a process intended to transition technical DNS coordination and management functions to a private-sector not-for-profit entity. While the DOC has played no role in the internal governance or day-to-day operations of the DNS, ICANN remained accountable to the U.S. government through the MOU, which was superseded in 2006 by a Joint Project Agreement (JPA). On September 30, 2009, the JPA between ICANN and DOC expired and was replaced by an Affirmation of Commitments (AoC), which provides for review panels to periodically assess ICANN processes and activities.

Many of the technical, operational, and management decisions regarding the DNS can have significant impacts on Internet-related policy issues such as intellectual property, privacy, e-commerce, and cybersecurity. With the expiration of the ICANN-DOC Joint Project Agreement on September 30, 2009, and the announcement of the new AoC, Congress and the Administration continue to assess the appropriate federal role with respect to ICANN and the DNS, and examine to what extent ICANN is positioned to ensure Internet stability and security, competition, private and bottom-up policymaking and coordination, and fair representation of the global Internet community. A related issue is whether the U.S. government's unique authority over the DNS root zone should continue indefinitely. Foreign governments have argued that it is inappropriate for the U.S. government to have exclusive authority over the worldwide DNS, and that technical coordination and management of the DNS should be accountable to international governmental entities. On the other hand, many U.S. officials argue that it is critical for the U.S. government to maintain authority over the DNS in order to guarantee the stability and security of the Internet.

The expiration of the JPA, the implementation of the Affirmation of Commitments, and the continuing U.S. authority over the DNS root zone remain issues of keen interest to the 111th Congress, the Administration, foreign governments, and other Internet stakeholders worldwide. Other specific issues include the possible addition of new generic top-level domain names (gTLDs), the security and stability of the DNS, and the status of the WHOIS database. How all of these issues are ultimately addressed could have profound impacts on the continuing evolution of ICANN, the DNS, and the Internet.

Contents

Figures

Appendixes

Contacts

Background and History

The Internet is often described as a "network of networks" because it is not a single physical entity but, in fact, hundreds of thousands of interconnected networks linking many millions of computers around the world. Computers connected to the Internet are identified by a unique Internet Protocol (IP) number that designates their specific location, thereby making it possible to send and receive messages and to access information from computers anywhere on the Internet. Domain names were created to provide users with a simple location name, rather than requiring them to use a long list of numbers. For example, the IP number for the location of the THOMAS legislative system at the Library of Congress is 140.147.248.9; the corresponding domain name is thomas.loc.gov. Top Level Domains (TLDs) appear at the end of an address and are either a given country code, such as .jp or .uk, or are generic designations (gTLDs), such as .com, .org, .net, .edu, or .gov. The Domain Name System (DNS) is the distributed set of databases residing in computers around the world that contain the address numbers, mapped to corresponding domain names. Those computers, called root servers, must be coordinated to ensure connectivity across the Internet.

The Internet originated with research funding provided by the Department of Defense Advanced Research Projects Agency (DARPA) to establish a military network. As its use expanded, a civilian segment evolved with support from the National Science Foundation (NSF) and other science agencies. While there were (and are) no formal statutory authorities or international agreements governing the management and operation of the Internet and the DNS, several entities played key roles in the DNS. For example, the Internet Assigned Numbers Authority (IANA), which was operated at the Information Sciences Institute/University of Southern California under contract with the Department of Defense, made technical decisions concerning root servers, determined qualifications for applicants to manage country code TLDs, assigned unique protocol parameters, and managed the IP address space, including delegating blocks of addresses to registries around the world to assign to users in their geographic area.

NSF was responsible for registration of nonmilitary domain names, and in 1992 put out a solicitation for managing network services, including domain name registration. In 1993, NSF signed a five-year cooperative agreement with a consortium of companies called InterNic. Under this agreement, Network Solutions Inc. (NSI), a Herndon, VA, engineering and management consulting firm, became the sole Internet domain name registration service for registering the .com, .net., and .org. gTLDs.

After the imposition of registration fees in 1995, criticism of NSI's sole control over registration of the gTLDs grew. In addition, there was an increase in trademark disputes arising out of the enormous growth of registrations in the .com domain. There also was concern that the role played by IANA lacked a legal foundation and required more permanence to ensure the stability of the Internet and the domain name system. These concerns prompted actions both in the United States and internationally.

An International Ad Hoc Committee (IAHC), a coalition of individuals representing various constituencies, released a proposal for the administration and management of gTLDs on February 4, 1997. The proposal recommended that seven new gTLDs be created and that additional registrars be selected to compete with each other in the granting of registration services for all new second level domain names. To assess whether the IAHC proposal should be supported by the U.S. government, the executive branch created an interagency group to address the domain

name issue and assigned lead responsibility to the National Telecommunications and Information Administration (NTIA) of the Department of Commerce (DOC). On June 5, 1998, DOC issued a final statement of policy, "Management of Internet Names and Addresses." Called the White Paper, the statement indicated that the U.S. government was prepared to recognize and enter into agreement with "a new not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system."[1] In deciding upon an entity with which to enter such an agreement, the U.S. government would assess whether the new system ensured stability, competition, private and bottom-up coordination, and fair representation of the Internet community as a whole.

The White Paper endorsed a process whereby the divergent interests of the Internet community would come together and decide how Internet names and addresses would be managed and administered. Accordingly, Internet constituencies from around the world held a series of meetings during the summer of 1998 to discuss how the New Corporation might be constituted and structured. Meanwhile, IANA, in collaboration with NSI, released a proposed set of bylaws and articles of incorporation. The proposed new corporation was called the Internet Corporation for Assigned Names and Numbers (ICANN). After five iterations, the final version of ICANN's bylaws and articles of incorporation were submitted to the Department of Commerce on October 2, 1998. On November 25, 1998, DOC and ICANN signed an official Memorandum of Understanding (MOU), whereby DOC and ICANN agreed to jointly design, develop, and test the mechanisms, methods, and procedures necessary to transition management responsibility for DNS functions—including IANA—to a private-sector not-for-profit entity.

On September 17, 2003, ICANN and the Department of Commerce agreed to extend their MOU until September 30, 2006. The MOU specified transition tasks which ICANN agreed to address. On June 30, 2005, Michael Gallagher, then-Assistant Secretary of Commerce for Communications and Information and Administrator of NTIA, stated the U.S. government's principles on the Internet's domain name system. Specifically, NTIA stated that the U.S. government intends to preserve the security and stability of the DNS, that the United States would continue to authorize changes or modifications to the root zone, that governments have legitimate interests in the management of their country code top level domains, that ICANN is the appropriate technical manager of the DNS, and that dialogue related to Internet governance should continue in relevant multiple fora.[2]

On September 29, 2006, DOC announced a new Joint Project Agreement (JPA) with ICANN which was intended to continue the transition to the private sector of the coordination of technical functions relating to management of the DNS. The JPA extended through September 30, 2009, and focused on institutionalizing transparency and accountability mechanisms within ICANN. On September 30, 2009, DOC and ICANN announced agreement on an Affirmation of Commitments (AoC) to "institutionalize and memorialize" the technical coordination of the DNS globally and by a private-sector-led organization.[3] The AoC affirms commitments made by DOC and ICANN to ensure accountability and transparency; preserve the security, stability, and resiliency of the

[1] Management of Internet Names and Addresses, National Telecommunications and Information Administration, Department of Commerce, *Federal Register*, Vol. 63, No. 111, June 10, 1998, 31741.

[2] See http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.pdf.

[3] Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers, September 30, 2009, available at http://www.ntia.doc.gov/ntiahome/domainname/Affirmation_of_Commitments_2009.pdf.

DNS; promote competition, consumer trust, and consumer choice; and promote international participation.

ICANN Basics

ICANN is a not-for-profit public benefit corporation headquartered in Marina del Rey, CA, and incorporated under the laws of the state of California. ICANN is organized under the California Nonprofit Public Benefit Law for charitable and public purposes, and as such, is subject to legal oversight by the California attorney general. ICANN has been granted tax-exempt status by the federal government and the state of California.[4]

ICANN's organizational structure consists of a Board of Directors (BOD) advised by a network of supporting organizations and advisory committees that represent various Internet constituencies and interests (see **Figure 1**). Policies are developed and issues are researched by these subgroups, who in turn advise the Board of Directors, which is responsible for making all final policy and operational decisions. The Board of Directors consists of 15 international and geographically diverse members, composed of one president, eight members selected by a Nominating Committee, two selected by the Generic Names Supporting Organization, two selected by the Address Supporting Organization, and two selected by the Country-Code Names Supporting Organization. Additionally, there are six non-voting liaisons representing other advisory committees.

The explosive growth of the Internet and domain name registration, along with increasing responsibilities in managing and operating the DNS, has led to marked growth of the ICANN budget, from revenues of about $6 million and a staff of 14 in 2000, to revenues of $60 million and a staff of 110 in 2009. ICANN is funded primarily through fees paid to ICANN by registrars and registry operators. Registrars are companies (e.g., GoDaddy, Google, Network Solutions) with which consumers register domain names.[5] Registry operators are companies and organizations who operate and administer the master database of all domain names registered in each top level domain (for example VeriSign, Inc. operates .com and .net, Public Interest Registry operates .org, and Neustar, Inc. operates .biz).[6] In 2009, ICANN is receiving 92% of its total revenues from registry and registrar fees (41% from registry fees, 51% from registrar fees).[7]

[4] ICANN, *2008 Annual Report*, December 31, 2008, p. 24, available at http://www.icann.org/en/annualreport/annual-report-2008-en.pdf.

[5] A list of ICANN-accredited registrars is available at http://www.icann.org/en/registries/agreements.htm.

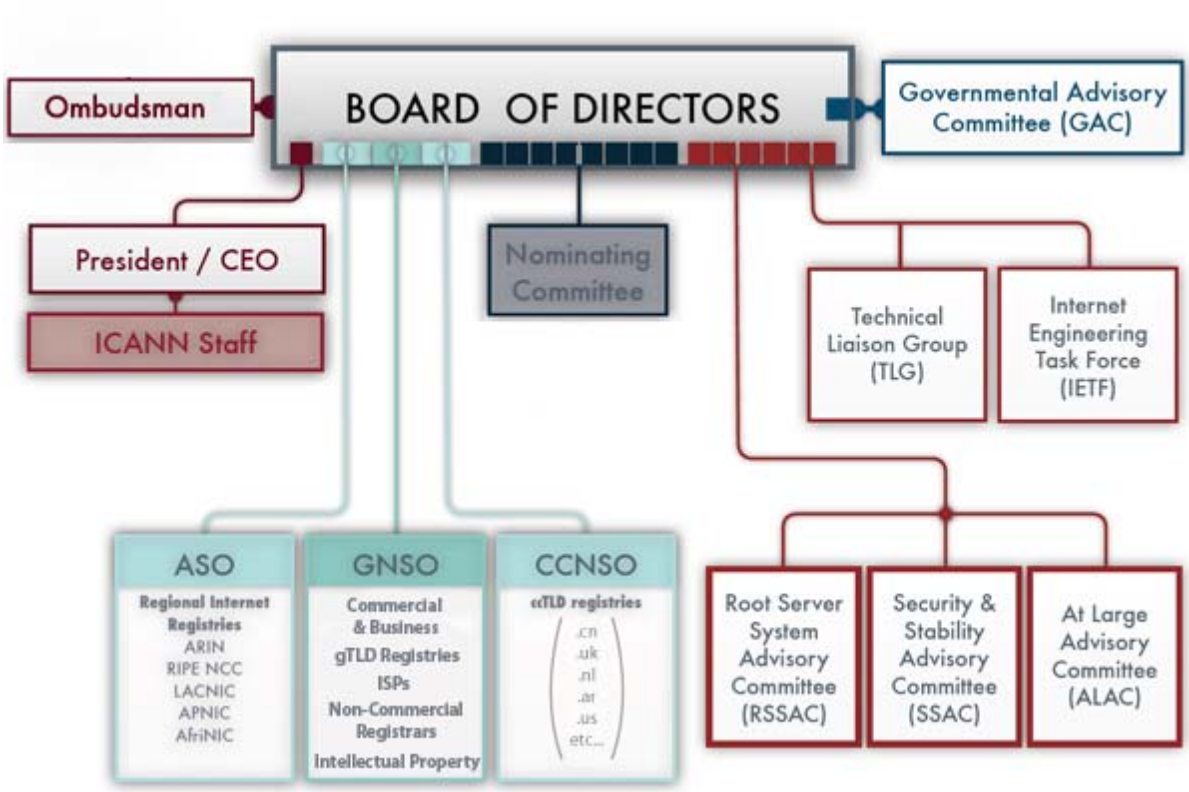
[6] A list of current agreements between ICANN and registry operators is available at http://www.icann.org/en/registries/agreements.htm.

[7] ICANN, Draft FY10 Operating Plan and Budget, May 17, 2009, p. 47, available at http://www.icann.org/en/financials/proposed-opplan-budget-v1-fy10-17may09-en.pdf.

Issues in the 111th Congress

Congressional Committees (primarily the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce) maintain oversight on how the Department of Commerce manages and oversees ICANN's activities and policies. Other Committees, such as the House and Senate Judiciary Committees, maintain an interest in other issues affected by ICANN, such as intellectual property and privacy. Specific issues of Congressional interest include ICANN's relationship with the U.S. government and the international community, the proposal to add new generic top level domains, and privacy. The **Appendix** shows a complete listing of Congressional committee hearings on ICANN and the domain name system dating back to 1997.

Figure 1. Organizational Structure of ICANN



Source: ICANN (http://www.icann.org/en/structure/).

ICANN's Relationship with the U.S. Government

The Department of Commerce (DOC) has no statutory authority over ICANN or the DNS. However, because the Internet evolved from a network infrastructure created by the Department of Defense, the U.S. government originally owned and operated (primarily through private contractors such as the University of Southern California, SRI International, and Network Solutions Inc.) the key components of network architecture that enable the domain name system to function. The 1998 Memorandum of Understanding between ICANN and the Department of

Commerce initiated a process intended to transition technical DNS coordination and management functions to a private-sector not-for-profit entity. While the DOC plays no role in the internal governance or day-to-day operations of ICANN, the U.S. government, through the DOC, retains a role with respect to the DNS via three separate contractual agreements. These are:

- the Affirmation of Commitments (AoC) between DOC and ICANN, which was signed on September 30, 2009;
- the contract between IANA/ICANN and DOC to perform various technical functions such as allocating IP address blocks, editing the root zone file, and coordinating the assignment of unique protocol numbers; and
- the cooperative agreement between DOC and VeriSign to manage and maintain the official DNS root zone file.

Affirmation of Commitments

On September 30, 2009, DOC and ICANN announced agreement on an Affirmation of Commitments (AoC) to "institutionalize and memorialize" the technical coordination of the DNS globally and by a private-sector-led organization.[8] The AoC succeeds the concluded Joint Project Agreement (which in turn succeeded the Memorandum of Understanding between DOC and ICANN). The AoC has no expiration date and would conclude only if one of the two parties decided to terminate the agreement.

Buildup to the AoC

Various Internet stakeholders disagreed as to whether DOC should maintain control over ICANN after the impending JPA expiration on September 30, 2009. Many U.S. industry and public interest groups argued that ICANN was not yet sufficiently transparent and accountable, that U.S. government oversight and authority (e.g., DOC acting as a "steward" or "backstop" to ICANN) was necessary to prevent undue control of the DNS by international or foreign governmental bodies, and that continued DOC oversight was needed until full privatization is warranted. On the other hand, many international entities and groups from countries outside the United States argued that ICANN had sufficiently met conditions for privatization, and that continued U.S. government control over an international organization was not appropriate. In the 110th Congress, Senator Snowe introduced S.Res. 564 which stated the sense of the Senate that although ICANN had made progress in achieving the goals of accountability and transparency as directed by the JPA, more progress was needed.[9]

On April 24, 2009, NTIA issued a Notice of Inquiry (NOI) seeking public comment on the upcoming expiration of the JPA between DOC and ICANN.[10] According to NTIA, a mid-term

[8] Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers, September 30, 2009, available at http://www.ntia.doc.gov/ntiahome/domainname/Affirmation_of_Commitments_2009.pdf.

[9] In the 110th Congress, S.Res. 564 was referred to the Committee on Commerce, Science, and Transportation. It did not advance to the Senate floor.

[10] Department of Commerce, National Telecommunications and Information Administration, "Assessment of the Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System," 74 *Federal Register* 18688, April 24, 2009.

review showed that while some progress had been made, there remained key areas where further work was required to increase institutional confidence in ICANN. These areas included long-term stability, accountability, responsiveness, continued private-sector leadership, stakeholder participation, increased contract compliance, and enhanced competition. NTIA asked for public comments regarding the progress of transition of the technical coordination and management of the DNS to the private sector, as well as the model of private-sector leadership and bottom-up policy development which ICANN represents. Specifically, the NOI asked whether sufficient progress had been achieved for the transition to take place by September 30, 2009, and if not, what should be done.

On June 4, 2009, the House Committee on Energy and Commerce, Subcommittee on Communications, Technology, and the Internet, held a hearing examining the expiration of the JPA and other issues. Most Members of the Committee expressed the view that the JPA (or a similar agreement between DOC and ICANN) should be extended. Subsequently, on August 4, 2009, Majority Leadership and Majority Members of the House Committee on Energy and Commerce sent a letter to the Secretary of Commerce urging that rather than replacing the JPA with additional JPAs, the DOC and ICANN should agree on a "permanent instrument" to "ensure that ICANN remains perpetually accountable to the public and to all of its global stakeholders." According to the committee letter, the instrument should: ensure the permanent continuance of the present DOC-ICANN relationship; provide for periodic reviews of ICANN performance; outline steps ICANN will take to maintain and improve its accountability; create a mechanism for implementation of the addition of new gTLDs and internationalized domain names; ensure that ICANN will adopt measures to maintain timely and public access to accurate and complete WHOIS information; and include commitments that ICANN will remain a not-for-profit corporation headquartered in the United States.

Critical Elements of the AoC

Under the AoC, ICANN commits to remain a not-for-profit corporation "headquartered in the United States of America with offices around the world to meet the needs of a global community." According to the AoC, "ICANN is a private organization and nothing in this Affirmation should be construed as control by any one entity."

Specifically, the AoC calls for the establishment of review panels which will periodically make recommendations to the ICANN Board in four areas:

- *Ensuring accountability, transparency and the interests of global Internet users*—the panel will evaluate ICANN governance and assess transparency, accountability, and responsiveness with respect to the public and the global Internet community. The panel will be composed of the Chair of ICANN's Government Advisory Committee (GAC), the Chair of the Board of ICANN, the Assistant Secretary for Communications and Information of the Department of Commerce (i.e., the head of NTIA), representatives of the relevant ICANN Advisory Committees and Supporting Organizations, and independent experts. Composition of the panel will be agreed to jointly by the Chair of the GAC and the Chair of ICANN.
- *Preserving security, stability, and resiliency*—the panel will review ICANN's plan to enhance the operational stability, reliability, resiliency, security, and global interoperability of the DNS. The panel will be composed of the Chair of

the GAC, the CEO of ICANN, representatives of the relevant Advisory Committees and Supporting Organizations, and independent experts. Composition of the panel will be agreed to jointly by the Chair of the GAC and the CEO of ICANN.

- *Impact of new gTLDs*—starting one year after the introduction of new gTLDs, the panel will periodically examine the extent to which the introduction or expansion of gTLDs promotes competition, consumer trust, and consumer choice. The panel will be composed of the Chair of the GAC, the CEO of ICANN, representatives of the relevant Advisory Committees and Supporting Organizations, and independent experts. Composition of the panel will be agreed to jointly by the Chair of the GAC and the CEO of ICANN.
- *WHOIS policy*—the panel will review existing WHOIS policy and assess the extent to which that policy is effective and its implementation meets the legitimate needs of law enforcement and promotes consumer trust. The panel will be composed of the Chair of the GAC, the CEO of ICANN, representatives of the relevant Advisory Committees and Supporting Organizations, independent experts, representatives of the global law enforcement community, and global privacy experts. Composition of the panel will be agreed to jointly by the Chair of the GAC and the CEO of ICANN.

DOC Agreements with IANA and VeriSign

A contract between DOC and ICANN, which currently extends through September 30, 2011, authorizes the Internet Assigned Numbers Authority (IANA) to perform various technical functions such as allocating IP address blocks, editing the root zone file, and coordinating the assignment of unique protocol numbers. Additionally, a cooperative agreement between DOC and VeriSign (operator of the .com and .net registries) authorizes VeriSign to manage and maintain the official root zone file that is contained in the Internet's root servers that underlie the functioning of the DNS.[11]

By virtue of these legal agreements, the DOC has policy authority over the root zone file,[12] meaning that the U.S. government can approve or deny any changes or modifications made to the root zone file (changes, for example, such as adding a new top level domain). The June 30, 2005, U.S. government principles on the Internet's domain name system stated the intention to "preserve the security and stability" of the DNS, and asserted that "the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file."[13]

[11] "The root zone file defines the DNS. For all practical purposes, a top level domain (and, therefore, all of its lower-level domains) is in the DNS if and only if it is listed in the root zone file. Therefore, presence in the root determines which DNS domains are available on the Internet." National Research Council, Committee on Internet Navigation and the Domain Name System: Technical Alternatives and Policy Implications, Signposts on Cyberspace: The Domain Name System and Internet Navigation, National Academy Press, Washington DC, 2005, p. 97.

[12] Milton Mueller, *Political Oversight of ICANN: A Briefing for the WSIS Summit*, Internet Governance Project, November 1, 2005, p. 4.

[13] See http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.pdf.

The JPA is separate and distinct from the DOC legal agreements with ICANN and VeriSign. As such, the expiration of the JPA would not directly affect U.S. government authority over the DNS root zone file. Although ICANN has not advocated ending U.S. government authority over the root zone file, foreign governmental bodies have argued that it is inappropriate for the U.S. government to maintain exclusive authority over the DNS.

ICANN and the International Community

Because cyberspace and the Internet transcend national boundaries, and because the successful functioning of the DNS relies on participating entities worldwide, ICANN is by definition an international organization. Both the ICANN Board of Directors and the various constituency groups who influence and shape ICANN policy decisions are composed of members from all over the world. However, many in the international community, including foreign governments, have argued that it is inappropriate for the U.S. government to maintain its legacy authority and control over ICANN and the DNS, and have suggested that management of the DNS should be accountable to a higher intergovernmental body.

The United Nations (U.N.), at the December 2003 World Summit on the Information Society (WSIS), debated and agreed to study the issue of how to achieve greater international involvement in the governance of the Internet and the domain name system in particular. The study was conducted by the U.N.'s Working Group on Internet Governance (WGIG). On July 14, 2005, the WGIG released its report, stating that no single government should have a preeminent role in relation to international Internet governance. The report called for further internationalization of Internet governance, and proposed the creation of a new global forum for Internet stakeholders. Four possible models were put forth, including two involving the creation of new Internet governance bodies linked to the U.N. Under three of the four models, ICANN would either be supplanted or made accountable to a higher intergovernmental body. The report's conclusions were scheduled to be considered during the second phase of the WSIS held in Tunis in November 2005. U.S. officials stated their opposition to transferring control and administration of the domain name system from ICANN to any international body. Similarly, the 109th Congress expressed its support for maintaining U.S. control over ICANN (H.Con.Res. 268 and S.Res. 323).[14]

The European Union (EU) initially supported the U.S. position. However, during September 2005 preparatory meetings, the EU seemingly shifted its support towards an approach which favored an enhanced international role in governing the Internet. Conflict at the WSIS Tunis Summit over control of the domain name system was averted by the announcement, on November 15, 2005, of an Internet governance agreement between the United States, the EU, and over 100 other nations. Under this agreement, ICANN and the United States remained in control of the domain name system. A new international group under the auspices of the U.N. was formed—the Internet Governance Forum—which provides an ongoing forum for all stakeholders (both governments and nongovernmental groups) to discuss and debate Internet policy issues. The Internet Governance Forum does not have binding authority. It is slated to run through 2010, at which point the U.N. will consider whether to continue the body.

[14] In the 109th Congress, H.Con.Res. 268 was passed unanimously by the House on November 16, 2005. S.Res. 323 was passed in the Senate by Unanimous Consent on November 18, 2005.

Adding New Generic Top Level Domains (gTLDs)

Top Level Domains (TLDs) are the suffixes that appear at the end of an address (after the "dot"). TLDs can be either a country code such as .us, .uk, or .jp, or a generic TLD (gTLD*)* such as .com, .org, or .gov. Prior to ICANN's establishment, there were eight gTLDs (.com, .org, .net, .gov, .mil, .edu, .int., and .arpa). In 2000 and 2004, ICANN held application rounds for new gTLDs; there are currently 21 gTLDs. Some are reserved or restricted to particular types of organizations (e.g., .museum, .gov, .travel) and others are open for registration by anyone (.com, .org, .info).[15] Applicants for new gTLDs are typically commercial and non-profit organizations who seek to become ICANN-recognized registries that will establish and operate name servers for their TLD registry, as well as implement a domain name registration process for that particular TLD.

With the growth of the Internet and the accompanying growth in demand for domain names, debate has focused on whether and how to further expand the number of gTLDs. In October 2007, the Generic Names Supporting Organization (GNSO) approved a recommendation to initiate a process that could yield an indefinite number of new generic top-level domains. Although previous gTLD application rounds in 2000 and 2004 were competitions designed to award a limited number of gTLDs, the new process is intended to award gTLDs to any applicant that meets ICANN's set criteria and that withstands any objections (if any) raised by outside parties. The result could be an unlimited number of new gTLDs, depending on the volume of applications.

The ICANN Board of Directors approved the GNSO recommendations in June 2008, and in October 2008, ICANN published a draft applicant guide book, available for public comment, which detailed how new gTLDs would be made available to applying prospective registries. Among the major criticisms raised in the public comments were the magnitude of ICANN's suggested gTLD application and registry fees, and concerns over the impact of multiple new gTLDs on trademark holders who, many argued, would be compelled to assume high costs of addressing the possible proliferation of cybersquatters inhabiting an unlimited number of new gTLDs.

ICANN released a revised applicant guide book ("Second Draft Applicant Guidebook") in February 2009. ICANN identified four particularly controversial and/or complex issues that "need more examination and discussion before they can be changed in a future draft guidebook."[16] These are: security and stability, malicious conduct, trademark protection, and the need for a demand/economic analysis that examines whether additional gTLDs will result in increased competition and consumer choice.

Regarding trademark protection, the ICANN board, on March 6, 2009, authorized the GNSO's Intellectual Property Constituency to form an Implementation Recommendation Team (IRT) to provide possible solutions to trademark issues raised by the implementation of new gTLDs.[17] On May 29, the IRT released its recommendations for addressing trademark issues.[18] The third

[15] The 21 current gTLDs are listed at http://www.iana.org/domains/root/db/#.

[16] ICANN, *New gTLD Draft Applicant Guidebook: Analysis of Public Comment*, February 18, 2009, p. 3, available at http://www.icann.org/en/topics/new-gtlds/agv1-analysis-public-comments-18feb09-en.pdf.

[17] See http://www.icann.org/en/announcements/announcement-26mar09-en.htm. The final report was released on May 29, 2009, and is available at http://www.icann.org/en/announcements/announcement-4-29may09-en.htm.

[18] See http://www.icann.org/en/announcements/announcement-4-29may09-en.htm.

Applicant Guidebook was released on October 4, 2009, for public comment. Specific trademark protection mechanisms are still to be decided upon by the ICANN Board, either as part of the guidebook or separately.

ICANN and Cybersecurity

The security and stability of the Internet has always been a preeminent goal of DNS operation and management. One issue of recent concern is an intrinsic vulnerability in the DNS which allows malicious parties to distribute false DNS information. Under this scenario, Internet users could be unknowingly redirected to fraudulent and deceptive websites established to collect passwords and sensitive account information.

A technology called DNS Security Extensions (DNSSEC) has been developed to mitigate those vulnerabilities. DNSSEC assures the validity of transmitted DNS addresses by digitally "signing" DNS data via electronic signature. "Signing the root" (deploying DNSSEC on the root zone) is a necessary first and critical step towards protecting against malicious attacks on the DNS.[19] On October 9, 2009, NTIA issued a Notice of Inquiry (NOI) seeking public comment on the deployment of DNSSEC into the Internet's DNS infrastructure, including the authoritative root zone.[20] On June 3, 2009, NTIA and the National Institute of Standards and Technology (NIST) announced they will work with ICANN and VeriSign to develop an interim approach for deploying DNSSEC in the root zone by the end of 2009.[21]

Meanwhile, section 8 of S. 773, the Cybersecurity Act of 2009, would require that any renewals or modifications made to DOC contracts regarding the operation of IANA be subject to review by a Cybersecurity Advisory Panel. S. 773 would also require NTIA to "develop a strategy to implement a secure domain name addressing system."

Privacy and the WHOIS Database

Any person or entity who registers a domain name is required to provide contact information (phone number, address, email) which is entered into a public online database (the "WHOIS" database). The scope and accessibility of WHOIS database information has been an issue of contention. Privacy advocates have argued that access to such information should be limited, while many businesses, intellectual property interests, law enforcement agencies, and the U.S. government have argued that complete and accurate WHOIS information should continue to be publicly accessible. Over the past several years, ICANN has debated this issue through its Generic Names Supporting Organization (GNSO), which is developing policy recommendations on what data should be publicly available through the WHOIS database. On April 12, 2006, the GNSO approved an official "working definition" for the purpose of the public display of WHOIS information. The GNSO supported a narrow technical definition favored by privacy advocates,

[19] Internet Corporation for Assigned Names and Numbers, "DNSSEC – What Is It and Why Is It Important?" October 9, 2008, available at http://icann.org/en/announcements/dnssec-qaa-09oct08-en.htm.

[20] Department of Commerce, National Telecommunications and Information Administration, "Enhancing the Security and Stability of the Internet's Domain Name and Addressing System," 73 *Federal Register* 59608, October 9, 2008.

[21] Department of Commerce, National Institute of Standards and Technology, *NIST News Release*, "Commerce Department to Work With ICANN and VeriSign to Enhance the Security and Stability of the Internet's Domain Name and Addressing System," June 3, 2009.

registries, registrars, and non-commercial user constituencies, rather then a more expansive definition favored by intellectual property interests, business constituencies, Internet service providers, law enforcement agencies, and the Department of Commerce (through its participation in ICANN's Governmental Advisory Committee). At ICANN's June 2006 meeting, opponents of limiting access to WHOIS data continued urging ICANN to reconsider the working definition. On October 31, 2007, the GNSO voted to defer a decision on WHOIS database privacy and recommended more studies. The GNSO also rejected a proposal to allow Internet users the option of listing third party contact information rather than their own private data. Currently, the GNSO is exploring several extensive studies of WHOIS.[22]

Concluding Observations

Many of the technical, operational, and management decisions regarding the DNS can have significant impacts on Internet-related policy issues such as intellectual property, privacy, e-commerce, and cybersecurity. As such, decisions made by ICANN affect Internet stakeholders around the world. In transferring management of the DNS to the private sector, the key policy question has always been how to best ensure achievement of the White Paper principles: Internet stability and security, competition, private and bottom-up policymaking and coordination, and fair representation of the global Internet community. What is the best process to ensure these goals, and how should various stakeholders—companies, institutions, individuals, governments—fit into this process?

ICANN has established governance processes that are intended to give access to Internet stakeholders into important decisions. With the expiration of the ICANN-DOC Joint Project Agreement on September 30, 2009, and with the subsequent implementation of the Affirmation of Commitments, Congress and the Administration are examining whether those processes are sufficient to give the full range of Internet stakeholders meaningful input into ICANN decisions, and whether ICANN is sufficiently accountable to those Internet stakeholders. [23]

A related issue is whether the U.S. government's unique authority over the DNS root zone should continue indefinitely. Foreign governments have argued that it is inappropriate for the U.S. government to have exclusive authority over the worldwide DNS, and that technical coordination and management of the DNS should be accountable to international governmental entities. On the other hand, many U.S. officials argue that it is critical for the U.S. government to maintain authority over the DNS in order to guarantee the stability and security of the Internet.

Meanwhile, the Affirmation of Commitments establishes a mechanism to review ICANN activities and policies regarding new gTLDs, DNS security and stability, and the WHOIS database. Ultimately, how these issues are addressed could have profound impacts on the continuing evolution of ICANN, the DNS, and the Internet.

[22] See ICANN "Whois Services" page, available at http://www.icann.org/topics/whois-services/.

[23] ICANN has established internal accountability mechanisms (an Ombudsman, a Reconsideration Committee, and an independent review process) which are intended to address complaints and disputes over ICANN decisions. See http://www.icann.org/en/general/accountability_review.html.

Appendix. Congressional Hearings on the Domain Name System

Date	Congressional Committee	Topic
September 23, 2009	House Judiciary	"Expansion of Top Level Domains and its Effects on Competition"
June 4, 2009	House Energy and Commerce	"Oversight of the Internet Corporation for Assigned Names and Numbers (ICANN)"
September 21, 2006	House Energy and Commerce	"ICANN Internet Governance: Is It Working?"
September 20, 2006	Senate Commerce, Science and Transportation	"Internet Governance: the Future of ICANN"
July 18, 2006	House Financial Services	"ICANN and the WHOIS Database: Providing Access to Protect Consumers from Phishing"
June 7, 2006	House Small Business	"Contracting the Internet: Does ICANN Create a Barrier to Small Business?"
September 30, 2004	Senate Commerce, Science and Transportation	"ICANN Oversight and Security of Internet Root Servers and the Domain Name System (DNS)"
May 6, 2004	House Energy and Commerce	"The 'Dot Kids' Internet Domain: Protecting Children Online"
July 31, 2003	Senate Commerce, Science and Transportation	"Internet Corporation for Assigned Names and Numbers (ICANN)"
September 4, 2003	House Judiciary	"Internet Domain Name Fraud – the U.S. Government's Role in Ensuring Public Access to Accurate WHOIS Data"
September 12, 2002	Senate Commerce, Science and Transportation	"Dot Kids Implementation and Efficiency Act of 2002"
June 12, 2002	Senate Commerce, Science and Transportation	"Hearing on ICANN Governance"
May 22, 2002	House Judiciary	"The Accuracy and Integrity of the WHOIS Database"
November 1, 2001	House Energy and Commerce	"Dot Kids Name Act of 2001"
July 12, 2001	House Judiciary	"The Whois Database: Privacy and Intellectual Property Issues"
March 22, 2001	House Judiciary	"ICANN, New gTLDs, and the Protection of Intellectual Property"
February 14, 2001	Senate Commerce, Science and Transportation	"Hearing on ICANN Governance"
February 8, 2001	House Energy and Commerce	"Is ICANN's New Generation of Internet Domain Name Selection Process Thwarting Competition?"
July 28, 1999	House Judiciary	"Internet Domain Names and Intellectual Property Rights"

Date	Congressional Committee	Topic
July 22, 1999	Senate Judiciary	"Cybersquatting and Internet Consumer Protection"
July 22, 1999	House Energy and Commerce	"Domain Name System Privatization: Is ICANN Out of Control?"
October 7, 1998	House Science	"Transferring the Domain Name System to the Private Sector: Private Sector Implementation of the Administration's Internet 'White Paper'"
June 10, 1998	House Commerce	"Electronic Commerce: The Future of the Domain Name System"
March 31, 1998	House Science	"Domain Name System: Where Do We Go From Here?"
February 21, 1998	House Judiciary	"Internet Domain Name Trademark Protection"
November 5, 1997	House Judiciary	"Internet Domain Name Trademark Protection"
September 30, 1997	House Science	"Domain Name System (Part 2)"
September 25, 1997	House Science	"Domain Name System (Part 1)"

Author Contact Information

Lennard G. Kruger
Specialist in Science and Technology Policy
lkruger@crs.loc.gov, 7-7070