SAC067

Overview and History of the IANA Functions

SSAC
ICANN Security and Stability
Advisory Committee

A Report from the ICANN Security and Stability Advisory Committee (SSAC)
15 August 2014

Preface

This is a Report to the Internet Corporation for Assigned Names and Numbers (ICANN) Board of Directors, the ICANN community, and the Internet community more broadly from the ICANN Security and Stability Advisory Committee (SSAC). It provides an overview of the Internet Assigned Numbers Authority (IANA) Functions—what they are—and a history of how they evolved from the informal activities of a single person[1] into the structured set of activities that are performed today in the context of a variety of contracts and agreements. Understanding this background is particularly important as the community considers the transfer of IANA Functions stewardship from the United States government to some other, yet–to–be–determined structure.

This Report was prepared from public information collected by SSAC members and from their own personal recollections and therefore does not include any information or insights from confidential or proprietary sources. As such, some of the information contained in this Report may be incorrect or incomplete, or reflect the honest recollection biases of individual SSAC members. Where possible, references to publicly available documents used for the development of this Report are provided either as uniform resource locators (URLs) in the body of the text or in footnotes.

The SSAC focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), administrative matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

A list of the contributors to this Report, references to SSAC members' biographies and disclosures of interest, and SSAC members' objections to the findings or recommendations in this Report are at end of this document.

[1] The original IANA was Dr. Jon Postel—see RFC 2468 (http://tools.ietf.org/html/rfc2468).

Table of Contents

1 Introduction

The Internet Assigned Numbers Authority (IANA) is a traditional name used "to refer to the technical team making and publishing assignments of Internet protocol technical parameters."[2] This technical team performs a set of tasks that involve the administration or coordination of many of the identifiers that allow the global Internet to operate. These tasks are currently performed by the Internet Corporation for Assigned Names and Numbers (ICANN) under a set of agreements including:

1) a contract with the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce;[3]
2) a Memorandum of Understanding (MoU) with the Internet Engineering Task Force (IETF);[4]
3) an MoU with the Regional Internet Registries;[5]
4) agreements with some root server operators;
5) contracts, MoUs, and other agreements with country code Top-Level Domain (ccTLD) administrators; and
6) a number of contracts with generic Top-Level Domain (gTLD) administrators.

As described in the current IANA Functions contract between ICANN and NTIA,[6] the IANA Functions are:

1) Domain Name System (DNS) Root Zone Management;
2) Internet Numbers Registry Management;
3) Protocol Parameter Registry Management, including management of the "Address and Routing Parameter Area" (.ARPA) TLD; and
4) Management of the "INTernational treaty organizations" (.INT) top-level domain.

This Report describes the activities included in the IANA Functions contract as well as the functions performed under the IETF MoU in order to establish a baseline of understanding for those interested in how the upper-most level of the Internet's system of unique identifiers is managed. It will focus primarily on the IANA Functions contract, but is intended to describe all of the activities related to the IANA Functions as they are currently performed, including those that lie outside of the IANA Functions contract.

[2] See the definition of IANA in RFC 2860 (http://tools.ietf.org/html/rfc2860), section 3.

[3] http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf

[4] The original March 2000 MoU is at https://www.icann.org/resources/unthemed-pages/ietf-icann-mou-2000-03-01-en and http://tools.ietf.org/html/rfc2860. A number of Supplemental Agreements have been executed since then.

[5] See https://archive.icann.org/en/aso/aso-mou-29oct04.htm.

[6] Unless otherwise specified, the term "IANA Functions contract" refers in this Report to the ICANN/NTIA contract at http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

2 Background and History

The IANA Functions are a set of activities that provide a coordination service for the upper–most level Internet identifiers. These functions work to ensure the secure, stable, and reliable allocation, assignment, and distribution of those identifiers, their uniqueness with respect to a well-defined identifier space, and the recording of to whom and/or for what purpose they are assigned.

This section provides some background and a brief history of how the IANA Functions came to be this set of activities, both in the context of the IANA Functions contract and in relation to the IETF.

2.1 Pre-IANA Functions Contract History

In August 1968 representatives from the first four ARPAnet sites met in Santa Barbara. The attendees agreed to meet periodically to discuss how to make use of the ARPAnet, a communications network established through funding from the U.S. Department of Defense Advanced Research Projects Agency (ARPA). At that time, ARPA was in the process of receiving bids to build the routers (Internet Message Processors or IMPs). The contractor had not yet been chosen (it would be Bolt, Beranek and Newman, later BBN), and there was no specific plan in place for what applications or protocols would exist.

Over the next several months the ARPAnet participants visited each of the sites and had broad–ranging discussions about possible applications and possible architectures for the protocols. In March 1969 the participants assigned themselves writing tasks related to the various topics they had been discussing. Steve Crocker documented one of the discussion topics, which eventually became RFC 1, and also took on the task of organizing the discussion drafts and notes. This latter task was described in what became Request for Comment (RFC) 3, “Document Conventions,” and established the term Request for Comments. As part of the creation of the RFCs, Crocker handed out an RFC number to each author. He also coined the term Network Working Group for this ad hoc group of representatives, which at first included only the people from the first four sites but gradually grew to more than fifty attendees. In June 1971 Crocker left the University of California, Los Angeles (UCLA) to join ARPA and asked Jon Postel, then a UCLA graduate student, to take over the RFCs.

In addition to handing out RFC numbers, Crocker and Postel assigned port numbers for the various services, e.g., port 21 for File Transfer Protocol (FTP), port 23 for Telnet, etc. Addresses for the IMPs were chosen by BBN and were just the sequence number corresponding to when they were delivered. There wasn’t enough involved in assigning numbers for either RFCs or ports to raise it to the level of an identified function.

However, in May 1972 Postel wrote RFC 349, which stated:

> *I propose that there be a czar (me?) who hands out official socket numbers for use by standard protocols. This czar should also keep track of and publish a list of those socket numbers where host specific services can be obtained.*[7]

RFC 349 also contained a proposed list of initial allocations. This served as the model of what would become the IANA Functions.

The IANA Functions were originally performed by Postel while he was a graduate student at UCLA; when he moved to USC/ISI after finishing his PhD, the IANA role moved with him. They were performed largely on an *ad hoc* basis as an unwritten component of various U.S. Department of Defense (DOD)–funded research projects, including multi–computer architectures, database technology, signal processing, modeling the climate, human/computer communications, and others.[8] These research projects developed the protocols upon which the Internet would operate as well as the documentary and administrative structures by which the protocols would be made publicly available. As coordination needs grew, the network research community continued to rely on Dr. Jon Postel to record the authoritative list of a growing number of identifiers. These functions, undertaken at the request and with the consent of the community, came to be known as the "Internet Assigned Numbers Authority." However, these documentary and administrative structures performed for and on behalf of the Network Working Group—and later the IETF[9]—weren't formally recognized in contractual language until the late 1990s. As a result, the IANA Functions can be viewed in two ways: as services to the IETF, and as activities performed under contract.

2.2 IANA Functions as Services to the IETF

Since the beginning of the development of the networking protocols that would evolve to define the Internet, there has been a need to document the various operational parameters that characterized those protocols and their use. Initially, these operational parameters were recorded in RFCs resulting from meetings of a group of network engineers and protocol designers who called themselves the "Network Working Group" (NWG).[10] As discussed previously, Dr. Jon Postel volunteered to take on the role of recording those operational parameters.

[7] http://tools.ietf.org/html/rfc349

[8] For example, ARPA project AF30(602)-4277 "Graphical Man/Machine Communications" (http://www.dtic.mil/dtic/tr/fulltext/u2/726623.pdf) was cited in RFC 33 (http://www.rfc-editor.org/rfc/rfc33.txt) as sponsoring the development of a "HOST-HOST Protocol."

[9] The IETF (http://www.ietf.org) is an "open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet."

[10] http://tools.ietf.org/html/rfc3

As documented in RFC 82, the “Network Information Center” (NIC) was established in 1970 at the Stanford Research Institute as “an *ad hoc* thing, with no specific directives from ARPA.”[11] The NIC housed the various documents the NWG developed, including the RFC series, which included the “Assigned Numbers” RFCs that aggregated all of the numbers and other parameters that had been assigned. These Assigned Numbers RFCs were published periodically in various forms between 1972 and 1994, with the last Assigned Numbers RFC (RFC 1700[12]) indicating that the most up-to-date assignment information was kept in online text files and the content of that RFC was “assembled by catinating *[sic]* these files together with a minimum of formatting ‘glue’.” RFC 1060, published in 1990, provides the first documented use of the term Internet Assigned Numbers Authority[13] in the context of the Assigned Numbers RFCs. RFC 3232,[14] published in 2002, officially obsoleted the Assigned Numbers RFCs, moving RFC 1700 to historic.

The day-to-day assignment of Internet addresses and autonomous system numbers was officially assumed by the Defense Data Network Network Information Center (DDN–NIC) in 1987,[15] and a separate track of RFCs documented their assignment until 1990.[16] As for the assigned numbers RFCs, publication of the assignment of Internet addresses and autonomous system numbers later moved to an online format, and RFC 1366,[17] published in 1992, began the establishment of the Regional Internet Registry system.

In 1992, the Internet Architecture Board (IAB)[18] was formally chartered by the Internet Society, with the responsibility for the “administration of the various Internet assigned numbers” and the designation of “an Internet Assigned Numbers Authority (IANA) to administer the assignment of Internet protocol numbers.”[19]

As the IETF has evolved and become more formalized, clarity in the policies by which IANA assignments were made became more critical to the ongoing development of the Internet protocols. In 1998, the Internet Engineering Steering Group (IESG)[20] imposed a requirement that all Internet Drafts provide explicit instructions, known as “IANA Considerations,” any time a registry or the contents of a registry needed to be created, modified, or removed.[21]

[11] See http://www.rfc-editor.org/rfc/rfc82.txt.
[12] See http://tools.ietf.org/html/rfc1700.
[13] See http://tools.ietf.org/html/rfc1060.
[14] See http://tools.ietf.org/html/rfc3232.
[15] See http://tools.ietf.org/html/rfc1020.
[16] See http://tools.ietf.org/html/rfc1166.
[17] See http://tools.ietf.org/html/rfc1366.
[18] The IAB (http://www.iab.org) provides architectural oversight of IETF activities.
[19] http://tools.ietf.org/html/rfc1601, sections 2(d) and 2.4.
[20] The IESG (http://www.ietf.org/iesg) is responsible for the technical management of IETF activities and the Internet standards process.
[21] See http://tools.ietf.org/html/rfc2434.

In 2000, the IETF entered into an MoU with ICANN that defined "the technical work to be carried out by the IANA on behalf of the IETF and the Internet Research Task Force." This MoU, documented as RFC 2860,[22] specifies that ICANN will "cause IANA to comply" with the requirement that "IANA will assign and register Internet protocol parameters only as directed by the criteria and procedures specified in RFCs" and that the assignment of domain names and Internet Protocol (IP) address blocks "are outside of the scope of this MoU."

Since 2000, the IETF has published a number of additional RFCs and has entered into a number of agreements that relate to the IANA Functions. These RFCs and other agreements are discussed in section 8.2.

2.3 IANA Functions Contract History

The IANA Functions, which were originally performed in an *ad hoc* fashion as requirements demanded, became formalized in contracts as the Internet experienced increased growth and commercialization during the 1990s. This trend accelerated with the decision by the National Science Foundation (NSF) in 1995 to allow Network Solutions, which provided the "registration services" portion of the InterNIC[23] under a 1993 cooperative agreement with NSF,[24] to charge a fee for assigning domain names.[25]

In 1997, the IANA Functions were documented within the U.S. Department of Energy's Tera-node Network Technology contractual vehicle.[26] These functions were specified to include:

1) "Parameter assignment";
2) "Address management"; and
3) "Domain name system supervision."

In February 2000, the NTIA entered into the first stand-alone IANA Functions contract.[27] This contract was established with ICANN, an organization incorporated in 1998 as a California (U.S.) not-for-profit public benefit corporation.[28] The activities called out in the initial IANA Functions contract were:

1) "Coordination of the assignment of technical protocol parameters";

[22] See http://tools.ietf.org/html/rfc2860.
[23] InterNIC was an NSF project to extend and coordinate directory and database services and information services for the NSFNET and provide registration services for non-military Internet networks. The original InterNIC awardees were Network Solutions for "Registration Services," General Atomics for "Information Services," and AT&T for "Directory and Database Services." The program guidelines can be found at http://www.nsf.gov/pubs/stis1992/nsf9224/nsf9224.txt.
[24] See http://archive.icann.org/en/nsi/coopagmt-01jan93.htm.
[25] See http://archive.icann.org/en/nsi/coopagmt-amend4-13sep95.htm.
[26] See "Tera-node Network Technology (TASK 4) Network Infrastructure Activities (NIA) Final Report," Jon Postel and Joe Bannister, 15 March 2000 (http://www.osti.gov/scitech/biblio/802104).
[27] See http://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf.
[28] See https://www.icann.org/resources/pages/articles-2012-02-25-en.

2) "Administrative functions associated with root management";
3) "Allocation of IP address blocks"; and
4) "Other services."

The functions that comprise the IANA have evolved over time. The current set of functions, defined in the latest version of the IANA Functions contract issued in July 2012[29] by NTIA and performed by the IANA Functions Operator (ICANN), consist of:

1) DNS Root Zone Management;
2) Internet Numbers Registry Management;
3) Protocol Parameter Registry and .ARPA TLD Management; and
4) Management of .INT.

Each of these functions will be described in detail in subsequent sections.

3 DNS Root Zone Management Function

The DNS, as a component of the global Internet, consists of:

1) A set of protocol specifications defined by the IETF;
2) A variety of software server and client application programs that implement those protocols;
3) A network infrastructure upon which that software is deployed that includes root name servers, other authoritative domain name servers,[30] and caching resolvers operated by Internet Service Providers (ISPs) and others; and
4) A "namespace," *i.e.*, all of the unique names that can be looked up (resolved) via the DNS protocol by clients (*e.g.*, applications like web browsers or email servers) sending queries via the DNS infrastructure. The infrastructure is considered by the IETF to also include names "for technical use," which are intended to be syntactically and functionally compatible with DNS names but are not intended to be looked up in the DNS. One example is .local.[31]

The DNS Root Zone Management function allows for changes to the highest level of the DNS namespace (the "root") by updating the databases that represent that namespace. In the context of the public Internet, the top level of the DNS namespace is defined to be the set of names (known as top-level domain names or TLDs) coordinated by ICANN as the IANA Root Zone Management function operator in cooperation with Verisign as the Root Zone Maintainer and NTIA as the Root Zone Administrator. When resolvers obtain these coordinated data, e.g., by using the root name servers through which the coordinated root zone is published, consistency of the namespace is assured. This

[29] See http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

[30] Authoritative name servers are servers that authoritatively answer queries for names for which they are responsible, and include top–level domain name servers, second–level domain name servers, etc.

[31] See http://www.ietf.org/rfc/rfc6761.txt.

coordination implements the "single root" required by the DNS protocol,[32] which ensures that looking up a domain name on the public Internet always and everywhere results in the response intended by the administrator of the domain.[33]

According to existing convention and agreements, the IANA Root Zone Management function is the only agreed–upon mechanism by which the root zone of the Internet DNS can be modified. Therefore, any requested change to any TLD—a ccTLD, a gTLD, or the .INT or .ARPA TLDs—or a change to the root zone itself must go through the IANA Root Zone Management function. Since September 2013 ICANN has published "Audit Reports" that describe the changes implemented by the Root Zone Management Function.[34]

Due to the distributed and hierarchical nature of the DNS, it is worth noting explicitly that the Root Zone Management Function affects only the contents of the root zone (i.e., the delegations and related resources of TLDs) and information about the root zone itself (e.g., the root name servers and their associated addresses and the DNS Security Extensions (DNSSEC) signatures of the root zone). Changes related to lower levels of the DNS, such as the contents of top–level domains (second–level domains such as EXAMPLE.ORG) and domains further down the namespace hierarchy, are not managed via the Root Zone Management Function and are not involved in or affected by the IANA Functions contract.

The DNS Root Zone Management function is by far the most politically sensitive of the IANA Functions. This focus arises from three primary factors:

1) The NTIA is involved in the Root Zone Management function in a role in which it (a) verifies that ICANN (as the IANA Functions operator) has followed established policies and procedures in processing a change request, and then (b) authorizes modifications to data and resources. This involvement, although limited and process–oriented, has periodically been perceived to be (and criticized for being) undue influence by the U.S. government, particularly with respect to changes related to ccTLDs, which are often considered to be national resources.[35]
2) Root Zone Management entails non–trivial and potentially immediate risk to the operation of the Internet as a whole, as it may involve changes to the apex of the public namespace upon which all Internet users and their applications rely.

[32] See http://www.ietf.org/rfc/rfc2826.txt.

[33] There is no restriction in the DNS protocol that limits the number of namespaces even within a single domain name class (essentially all DNS transactions are in class "IN" for Internet); however, all namespaces must be entirely disjoint to ensure consistency of resolution.

[34] See https://www.iana.org/performance/root-audit for more information.

[35] See for example the recent lawsuits against ICANN in which claimants assert that ccTLDs are properties (http://domainincite.com/17008-terror-victims-try-to-seize-five-cctlds), and ICANN's response that ccTLDs are **not** properties.

3) Policy decisions about what names are valid in the DNS root zone tend to be sensitive. Unlike its role with respect to the other IANA Functions, ICANN has both policy and implementation responsibility for these decisions. The IANA Functions contract currently stipulates[36] the separation of ICANN's policy development from the staff designated for IANA Functions operations, but different perceptions persist regarding the appropriateness or inappropriateness of policy and operations being housed within the same organization.

3.1 Root Zone Management Categories

The Root Zone Management function includes five broad categories of responsibility:

1) root zone changes;
2) registration ("Whois") data changes;
3) delegations and re-delegations;
4) root name server changes; and
5) root zone "Key Signing Key" (KSK) management.

The first four of these categories involve modifications that can directly and immediately affect the operation of the Internet. As such, the NTIA explicitly authorizes these changes by verifying that ICANN has followed established policies and procedures in processing the requests. The fifth category can have operational impact, but that impact would be delayed, and as such authorization is implicitly provided by NTIA by their authorizing the Key-Signing-Key (KSK)-signed Zone Signing Key to sign the root zone with DNSSEC.[37]

3.1.1 Root Zone Changes

Root zone changes are requests that cause modifications to the root zone of the Internet's DNS. These changes include:

1) adding or removing a delegation for a TLD;
2) adding, changing, or deleting the name servers, and their associated address or "glue" records, for a TLD;
3) adding, changing, or deleting the "delegation signer" (DS) resource records used by TLDs that have enabled DNSSEC; and
4) adding, changing, or deleting the name servers, and their associated address or "glue" records, for the root zone itself.

[36] See the IANA Functions Contract award, 2012-10-01, Section C.2.5, "Separation of Policy Development and Operational Roles," at http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

[37] More specifically, NTIA authorizes the use of a Secure Key Response (SKR) by the Root Zone Maintainer (Verisign). The SKR is the product of an ICANN key ceremony, and hence the result of ICANN exercising the KSK.

A root zone change involves five (mostly) independent parties:[38]

1) the change requester, usually the manager(s) or administrator(s) of the TLD;[39]
2) ICANN, as the IANA Functions Operator;
3) NTIA, as the Root Zone Administrator;
4) Verisign, as the Root Zone Maintainer; and
5) the Root Server Operators.

Within the latest version of the IANA Functions Contract, ICANN, NTIA, and Verisign are referred to as the Root Zone Management Partners (the change requester and the Root Server Operators are not subject to the IANA functions contract). While there are agreements between ICANN and NTIA (the IANA Functions contract) and between Verisign and NTIA (a Cooperative Agreement),[40] there is no agreement directly between ICANN and Verisign in the context of root zone management.[41]

Figure 1 provides a high level diagram of the Root Zone Management process for a root zone change. The steps shown in the diagram are:

1) The change requester creates a root zone change request, typically by logging into ICANN's Root Zone Management System and updating appropriate fields. The requester then submits that change request to ICANN (as the IANA Functions operator).[42]
2) After ICANN accepts and validates the change request, it is forwarded to NTIA (as the Root Zone Administrator), with a copy sent in parallel to Verisign.
3) After NTIA verifies that ICANN followed established policies and procedures in processing the change request, NTIA authorizes implementation of the change in a notification sent to Verisign. This notification enables implementation of the change request that ICANN had sent directly to Verisign in step 2.

[38] Some of the parties play multiple roles: ICANN is the IANA Functions Operator as well as a root server operator; Verisign is the Root Zone Maintainer as well as the operator of two root servers and TLD administrator for .COM, .NET, and other TLDs; and NTIA is the Root Zone Administrator as well as a TLD Administrator.

[39] Current practice is to partition the role of TLD administration among three roles—the "Sponsoring Organization" or "Manager," the "Administrative Contact" (AC), and the "Technical Contact" (TC)—the latter two of which are (in theory) appointed by the Manager. Root Zone changes typically require the concurrence of both the AC and the TC.

[40] Amendments to the Cooperative Agreement since October, 1998 are posted at http://www.ntia.doc.gov/page/verisign-cooperative-agreement.

[41] See footnote 1 on page 15 and footnote 2 on page 16 of http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

[42] The TLD administrators need not update their zone prior to submitting the request; however, in most cases the zone will need to be updated prior to ICANN attempting to validate the change request (step 2).

4) After Verisign implements the change request (by modifying the root zone file), it DNSSEC–signs the updated zone and place the newly–signed zone on Verisign–operated "distribution master servers" twice daily. Once the updated zone is placed on distribution master servers, the 13 root servers can deliberately or automatically pull the updated zone from the distribution master servers.
5) After the updated root zone has been signed and placed on the distribution master servers, Verisign notifies ICANN and NTIA that the change is complete.
6) Once Verisign notifies ICANN that the change is complete[43] and ICANN has verified that the change is correctly reflected in the Internet's root zone, ICANN notifies the requester that its change has been processed.

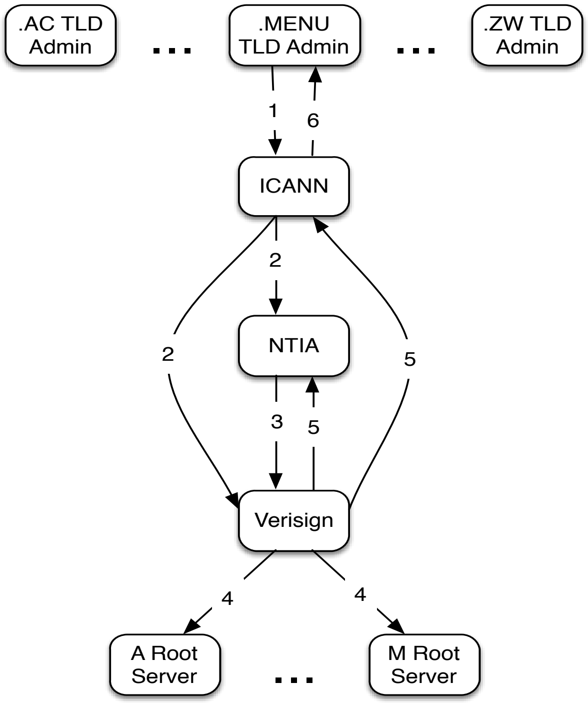

Figure 1. Root Zone Name Server Change Process

3.1.2 Registration ("WHOIS") Data Changes

Registration data changes result in creating, changing, or deleting the registration (aka "WHOIS") data associated with a TLD. These changes include modifying the TLD's contact information of one or more of the "sponsoring organization," the "administrative contact," and the "technical contact." The changes also may update other non–DNS–

[43] ICANN monitors the root servers and may notify the requester of the completed change either when it detects the change in the root zone or when it receives notification from Verisign.

related information (e.g., "WHOIS" server) associated with the TLD. These data are not required for successful resolution of names in the DNS root zone, but are required for correct and reliable functioning of administrative processes.

A Registration Data change involves three parties:

1) the change requester, usually a TLD administrator or manager;
2) ICANN, as the IANA Functions Operator; and
3) NTIA, as the Root Zone Administrator.

Since Registration Data changes do not involve the DNS but instead only modify the IANA TLD registration database administered by ICANN, neither Verisign as the Root Zone Maintainer nor the root server operators are involved.

Figure 2 provides a high level diagram of the Root Zone Management process for a Registration Data change with each of the steps labeled. These steps are:

1) The change requester creates and submits a change request to ICANN (as the IANA functions operator).
2) After ICANN accepts and validates the change request, it is forwarded to NTIA (as the Root Zone Administrator) for verification that ICANN followed established policies and procedures. After verifying that ICANN followed the appropriate procedures, NTIA authorizes ICANN to make the change.
1) After NTIA authorizes the change, ICANN updates the IANA TLD registration database.
2) ICANN notifies the requester that the change is complete.

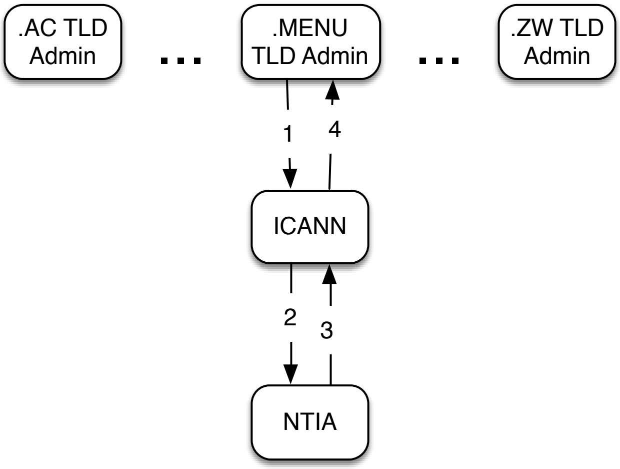

Figure 2. Registration Data Change Process

3.1.3 Delegation and Redelegation

Delegation is the original transfer of control of a TLD to an administrator. Redelegation is the transfer of control of a TLD from an existing administrator (incumbent or pre-delegation administrator) to a new one (post-delegation administrator). These operations involve four key parties:

1) the pre-delegation TLD administrator (in the case of a redelegation);
2) the post-delegation TLD administrator;
3) ICANN, as the IANA Functions Operator; and
4) NTIA, as the Root Zone Administrator.

Such requests involve either registration data changes only or a combination of registration data changes and root zone changes. When a change request involves both registration data and root zone changes (i.e., the TLD administrator is changing the technical configuration of the domain in concert with the change of administrative control), ICANN will perform the parts of the process that relate to technical configuration changes. Verisign, as the Root Zone Maintainer, will make the appropriate Root Zone Change, as described in section 3.1.1.

A delegation is a simplified case of a redelegation, in that there is no pre-redelegation administrator, and it occurs only when the TLD is first put into the root zone.[44] This simplification reduces both the number of parties involved and the potential for contention or delay. However, the steps in a delegation are otherwise the same as in a redelegation.

Figure 3 provides a high level diagram of the Root Zone Management process for a redelegation change, with each of the steps labeled. These steps are:

1) The change requester creates and submits a change request to ICANN (as the IANA Functions operator).
2) After ICANN accepts and validates the change request, it is forwarded to both the pre-redelegation and post-redelegation TLD administrators, with a request that each responds with a positive acknowledgement of the change request.
3) After both the pre-redelegation and post-redelegation TLD administrators receive notification of the change, each responds with a positive acknowledgement to ICANN.
4) After ICANN receives a positive acknowledgement from both administrators, the request is forwarded to NTIA (as the Root Zone Administrator) to verify that ICANN followed established policies and procedures and for authorization to implement the change.
5) After NTIA authorizes implementation of the change, ICANN updates the IANA TLD registration database.
6) ICANN notifies both the pre-redelegation and post-redelegation TLD administrators that the request has been completed.

[44] Technically, a delegation would also occur if a TLD were removed from the root zone and later put back in.

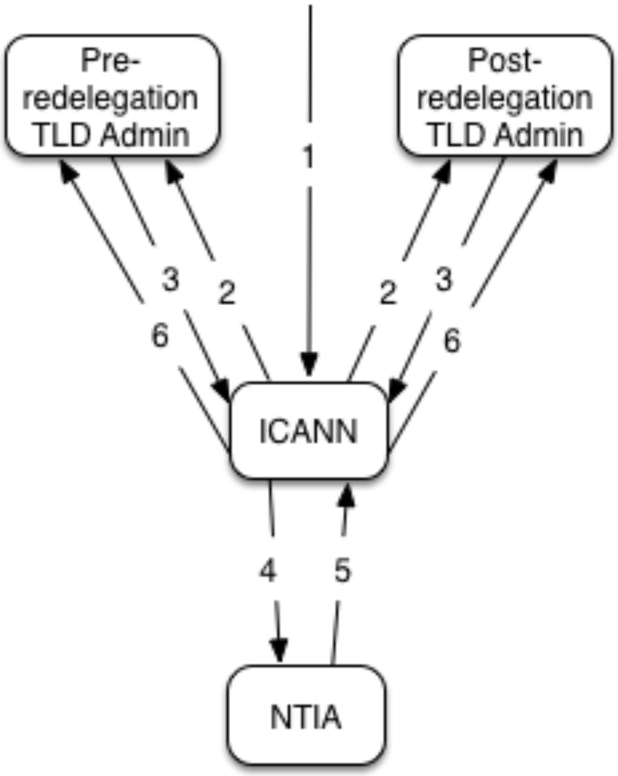

Figure 3. Root Zone Redelegation Process

A key and somewhat controversial aspect of the redelegation process is the requirement in RFC 1591[45] that IANA staff verify the existence of "local community support" for a redelegation. This requires ICANN staff to solicit input from relevant community members and ask whether they object to the transfer of control. Occasionally, this has resulted in controversy when a government has asserted that a transfer must be made and local Internet community participants have objected. In such cases, the traditional IANA methodology for resolving conflicts—not proceeding with the redelegation request until there is consensus among all parties—can result in significant delays in processing the redelegation request.

In the vast majority of redelegations, the transfer of control is mutually agreeable. However, there have been cases in which the incumbent TLD administrator has refused to cooperate with a redelegation, or has been unable or unwilling to positively acknowledge a redelegation request. Reasons for the lack of positive acknowledgement have included internal conflict—government breakdown, civil wars, etc.—but more frequently have been due to a lack of agreement between the incumbent TLD

[45] http://tools.ietf.org/html/rfc1591

administrator and the post-redelegation TLD administrator concerning how the TLD should be run, who should get paid what, etc.

These non–mutually agreeable cases can take a long time (on the order of years) to resolve. They have, however, become increasingly rare as TLD administrative processes, both at ICANN and within the TLD administrators, have become more formalized.

In many cases, a root zone change forms part of a redelegation request, as the post-redelegation TLD administrator usually wants to change the name servers when it assumes control of the TLD. The point in time at which the root zone changes occur may vary, but typically the requests are treated sequentially: the administrative redelegation (or initial delegation) is done first, followed by the root zone change.

3.1.4 Root Name Server Changes

While not explicitly a part of the IANA Functions contract, the maintenance of the list of root servers is an activity performed as part of the IANA Root Zone Management Function. Due to the way in which the DNS operates, most resolvers require prior knowledge of at least one IP address for at least one root name server in order to know where to send queries when they don't have name server information for TLDs. When these resolvers start up, they issue a "priming query" to one of the root server addresses configured in a list most commonly known as the "root hints." These root hints are derived from a file maintained by ICANN as the IANA Root Zone Management Function Operator.[46]

While extremely infrequent, there have been times when root name servers needed to change their IP version 4 (IPv4) addresses. In addition, there has been an ongoing effort to enable the root name servers for IP version 6 (IPv6), which requires the addition of IPv6 addresses for the IPv6-capable root name servers. These requests are handled similarly to Root Zone Changes, except that the zone that is being updated is the ROOT-SERVERS.NET zone instead of the root zone. The steps associated with a Root Name Server Change are:

1) A root server operator sends a request to ICANN as the IANA Functions Operator to update their ROOT-SERVERS.NET entry.
2) After ICANN accepts and validates the change request, it is forwarded to NTIA (as the Root Zone Administrator), with a copy sent to Verisign.
3) After NTIA verifies that ICANN followed established policies and procedures in processing the change request, NTIA authorizes implementation of the change in a message sent to Verisign. This notification enables implementation of the change request that ICANN had sent directly to Verisign in step 2.

[46] The root hints file can be found at http://www.iana.org/domains/root/files and ftp://ftp.internic.net/domain/named.root.

4) After Verisign implements the change request (modifying the ROOT-SERVERS.NET zone), it DNSSEC-signs the updated zone, and places the newly signed zone on the Verisign-operated distribution master servers, thereby allowing the 13 root servers to automatically obtain the updated zone.
5) After the updated ROOT-SERVERS.NET zone has been signed and placed on the master distribution servers, Verisign notifies ICANN and NTIA that the change is complete.
6) Once Verisign notifies ICANN that the change is complete and ICANN has verified that the change has been correctly reflected in the ROOT-SERVERS.NET zone, ICANN notifies the root server operator that their change request has been processed. ICANN also updates the "root.hints" file and makes that file available on the IANA.ORG website and the FTP.INTERNIC.NET FTP site.

3.1.5 Root Zone DNSSEC "Key Signing Key" Management

As originally specified, the DNS protocol has a flaw that permits DNS data to be altered as they travel from the source (the "authoritative server") to the requester. The requester typically is a server called a "recursive resolver" that performs a DNS lookup on behalf of a client application (e.g., web browser, email client, etc.). The IETF created a fix for this flaw, known as the "DNS Security Extensions" (DNSSEC), which uses public key cryptography to create a digital signature of zone data,[47] carried as DNS data in query responses. Validating the digital signature ensures that the data have not been changed while in transit.

A fundamental requirement of DNSSEC is that there be a well–known "trust anchor" embedded in every recursive resolver that will attempt to validate the zone data it receives. This trust anchor serves as the starting point for verification of signed data, typically implemented in recursive resolvers that validate responses (known as "validating recursive resolvers" or just "validating resolvers"). In July 2010, ICANN (as the IANA Functions operator) generated this trust anchor as part of the project to deploy DNSSEC in the Root Zone.[48] This key generation event occurred during the first Root Zone Key Signing Ceremony, and subsequent ceremonies have been held at regular intervals. Each ceremony is held as an open and transparent exercise that is webcast and archived, and involves 34 people known as the "Trusted Community Representatives" (TCRs). These TCRs perform various roles such as Recovery Key Share Holders, Crypto Officers, and their backups. A listing of the individuals currently acting as TCRs and the roles they perform can be found at http://www.root-dnssec.org/tcr/selection-2010/.

[47] Technically, each set of resource records in a zone that has the same domain name, resource record type, and class will have its own digital signatures.

[48] The project to deploy DNSSEC in the Root Zone is described at http://www.root-dnssec.org.

The purpose of the ongoing Root Zone Key Signing Ceremonies is to use the "Key Signing Key" (KSK) to sign the Root Zone "Zone Signing Key."[49] The current Root Zone KSK was generated in the first Root Zone Key Signing Ceremony (from which the Root trust anchor is the public part). The Root Zone "Zone Signing Key" is then used by Verisign, as the Root Zone Maintainer, to DNSSEC-sign the root zone prior to its distribution to the Root Servers.[50]

Each Key Signing Ceremony's core function is to receive a set of unsigned public key materials, known as a Key Signing Request (KSR), from the Root Zone Maintainer and to produce a corresponding set of signed public key materials, known as a Secure Key Response (SKR). The authenticity of each KSR is confirmed within the Key Signing Ceremony, and the resulting SKR is transmitted to the Root Zone Maintainer. The Root Zone Administrator is responsible for authorizing the SKR before it is used by the Root Zone Maintainer to publish signed root zones.

The role of the IANA Functions Operator in Root Zone DNSSEC KSK Management is to perform the Root Zone Key Signing Ceremonies, ensuring that they are done in a trustworthy fashion; to maintain the root KSK in a way that ensures that it can be trusted;[51] and to publish an accurate root trust anchor for use by validating recursive resolvers.

3.2 Change Request Processing

This section provides an overview of the processing performed by the IANA Functions Operator when it receives a change request.

3.2.1 Change Validation

In all three of the root zone management change categories, ICANN, as the IANA Functions Operator, is responsible for validating the change request. Beyond verifying that the request is syntactically correct, ICANN ensures that the administrator(s) of the TLD, specifically the authorized "administrative contact(s)" and the "technical contact(s)," agree with the requested change. Historically, this has meant that ICANN has

[49] More accurately, multiple DNSKEY RRSets are individually signed during a key ceremony. Those DNSKEY RRSets include the public part of the KSK as well as the public part of one or more ZSKs.

[50] While the Root Zone DNSSEC architecture is outside the scope of this document, briefly, the separation of the Key Signing Key from the Zone Signing Key allows for the Zone Signing Key to be changed frequently without requiring every resolver on the planet to be modified with a new trust anchor. More information can be found in https://www.iana.org/dnssec/icann-dps.txt.

[51] ICANN's implementation of the KSK Facilities includes two geographically distributed, access-controlled facilities, with multiple layers of physical security along with U.S. Federal Information Processing Standard (FIPS) 140-3 certified Hardware Security Modules, and various security controls. The system as a whole was designed to meet all SP 800-53 technical security controls required by a HIGH IMPACT system with regards to integrity and availability as defined in FIPS 199. See https://www.iana.org/dnssec/icann-dps.txt for a full statement of the KSK DNSSEC practices.

needed to obtain consent via email, telephone, fax, and even postal mail and has needed to ensure that changes were being done with the approval of all parties.[52] Today, with Root Zone Management System automation, determining whether a requester is authorized is largely deferred to whether the administrator has login credentials. However, this does not address the question of gaining agreement from all parties. Perhaps unsurprisingly, this process of getting agreement from all parties can be quite time consuming, particularly when TLDs are being operated in places with unreliable infrastructure or when the contact details for the TLD administrator have not been kept up–to–date.

3.2.2 Technical Checks

In the case of a root zone change, IANA staff verify that the baseline technical conformance criteria for authoritative name servers are met. The requirements that make up this baseline are described at http://www.iana.org/help/nameserver-requirements. The verification of these requirements has been automated to a high degree and is part of the Root Zone Management System implemented among the Root Zone Management Partners.

3.2.3 Exceptional Instructions

In unusual cases, top–level domains will have requirements that fall outside of normal processing. Examples of these requirements include when a TLD administrator has provided additional instructions on how it can be reached for change validation or when additional administrative steps are necessary for IANA staff to process a request such as contacting specific ministries or departments in order to obtain full permission (e.g., in cases in which territories are administered from home countries or there is a need to obtain exemptions for entities under sanction). In these cases, IANA staff maintain a set of "exceptional instructions" that are implemented as appropriate in order to meet the exceptional circumstances associated with the TLD. Of course, by their exceptional nature, these instructions can result in challenges for the Root Zone Management System automation as they require human intervention and are potential sources of delay. As such, the use of these Exceptional Instructions is discouraged.

3.2.4 Automation

As discussed previously, the Root Management Partners have deployed the "Root Zone Management System" (RZMS), software that automates much of the root zone management process. The RZMS provides TLD administrators with a web-based user interface that allows change requests to be entered by editing fields on forms, e.g., updating the postal address for the TLD administrative contact, submitting those change

[52] See https://www.iana.org/help/obtaining-consent for a brief overview.

requests to ICANN for validation, and tracking change requests as they are processed. The processing of requests performed by ICANN generally occurs much more quickly with the RZMS. According to a "customer satisfaction" survey performed by ICANN in 2013,[53] 80 percent of respondents indicated that they were "satisfied" or "very satisfied" with the timeliness of changes in TLD and root zone data using the RZMS.

3.3 U.S. Government Involvement

Under the current Root Zone Management Function architecture, every request that affects the root zone or the IANA TLD registration database requires explicit authorization by the Root Zone Administrator, NTIA. This involvement by the U.S. government is controversial, particularly in the context of authorizing changes to ccTLDs. Over time, ccTLDs have come to be seen by some, particularly governments, as national resources. The Root Zone Administrator requirement of authorizing all change requests for those resources has therefore been perceived by some to be an encroachment on national sovereignty (in the case of ccTLDs) or interference in national commercial affairs (in the case of gTLDs), even though the Root Zone Administrator's involvement is limited to verifying that ICANN (as the IANA Functions Operator) has followed established policies and procedures in processing the request and then authorizing the implementation of that change. The Root Zone Administrator's role has nothing to do with the substance of the change being requested, despite the perception that somehow the Root Zone Administrator is judging the validity of the request.

Today, the Root Zone Administrator verifies that ICANN has followed established policies and procedures, and authorization to implement the change is performed via a web-based interface into RZMS. Root zone change requests by the TLD administrator are entered in RZMS, where the IANA Functions Operator validates them. Once validated, notification is sent to the Root Zone Administrator who logs in to a web interface,[54] reviews the requested changes solely with respect to whether or not ICANN has followed established policies and procedures, and (assuming that it has) authorizes the implementation of the changes. This authorization releases the changes to the Root Zone Maintainer for implementation (including DNSSEC-signing and distribution to the root servers).

In addition, the IANA Functions contract mandates reporting requirements that include monthly performance progress reports, performance standards reports, the results of customer service surveys, and a final report that documents "standard operating procedures, including a description of the techniques, methods, software, and tools

[53] See http://www.iana.org/reports/2013/customer-survey-20131210.pdf.

[54] Clients attempting to connect to the web interface must present valid X.509 (SSL) client certificates.

employed in the performance of the IANA functions."[55] It also includes a requirement to maintain audit data on security processes and root zone management.[56]

4 Internet Numbers Registry Management

This function manages IPv4 addresses (e.g., 192.0.2.123), IPv6 addresses (e.g., 2001:db8::1:be3f), and Autonomous System Numbers (ASNs, e.g., AS 64496 and AS 65551). ASNs can be thought of as tags used by ISPs to group their blocks of addresses for use in the Internet's routing system. The IANA Internet Numbers Registry Management function follows a set of global policies defined via a regionally managed, bottom-up, consensus-driven policy definition process within the Regional Internet Registry (RIR) system. The complete set of these policies, which must have full consensus among all five RIRs before they are submitted to ICANN for ratification, are collected at http://www.icann.org/en/resources/policy/global-addressing. These policies describe the processes by which and under what conditions Internet numbers can be allocated to the RIRs.

The numbers that the IANA Internet Numbers Registry Management function allocates derive their usefulness and value in the uniqueness explicit in their management. That is, and taking IPv4 as an example, IPv4 addresses are simply 32-bit integers ranging in value from 0 to 4,294,967,295, and any device can be configured with essentially any number in that range.[57] However, if that device is to be successfully connected to the Internet, the number (address) assigned to that device **must** be unique with respect to every other address assigned to every other device directly connected to the Internet. The Internet Numbers Registry system, of which the IANA Internet Numbers Registry Management Function is at the apex, ensures that uniqueness.

4.1 Internet Numbers Registry Management Functions

In day-to-day practice, the Internet Numbers Registry Management Function consists of:

1) allocating blocks of IPv4 addresses to RIRs and recording those allocations in the IPv4 address registry found at http://www.iana.org/assignments/ipv4-address-space;
2) creating, modifying, or deleting IN-ADDR.ARPA delegations associated with IPv4 address blocks to facilitate IPv4 address to name mappings in the DNS;[58]

[55] See http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf, sections C.4.2, C.4.4, C.4.5, and C.4.6.

[56] See http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf, sections C.5.1 and C.5.2.

[57] Some ranges of addresses have special meanings, e.g. "this machine" or "multicast," defined by software that limit their usability as regular addresses.

[58] An IN-ADDR.ARPA delegation allows an IP address, e.g., 192.0.2.143, to be mapped back to a name by reversing the order of the octets, appending ".IN-ADDR.ARPA" and using a DNS "pointer" (PTR)

3) allocating blocks of IPv6 addresses to RIRs and recording those allocations in the IPv6 address registry found at http://www.iana.org/assignments/ipv6-unicast-address-assignments;
4) creating, modifying, or deleting IP6.ARPA delegations associated with IPv6 address blocks to facilitate IPv6 address to name mappings in the DNS;[59]
5) allocating blocks of autonomous system numbers to RIRs and recording those allocations in the autonomous system number registry found at http://www.iana.org/assignments/as-numbers;
6) receiving returns of blocks of addresses or autonomous system numbers from regional registries or others who received allocations prior to the establishment of the RIRs; and
7) updating the IPv4, IPv6, and autonomous system number registries located on the IANA web site.

4.1.1 IPv4 Address Management Historical Context

The management of the IPv4 address pool has a long history, with the initial allocations as documented in the earliest "Assigned Numbers" RFCs being done in the early 1980s. As the Internet has evolved, the management of those addresses has undergone significant change. Initially, the assumption made by the Internet Protocol designers was that there would be a small number of very large networks, along the lines of the national monopoly telephone networks. As a result, the first addressing model allowed for up to 256 networks, and each network could have up to 16,777,216 hosts.

Allocation of the networks was a simple matter: the people responsible for a network, most of whom were known within a very small community of network researchers, would contact "the numbers czar" (Dr. Jon Postel) and ask for a network number. The next number in the list of network numbers would be provided at no cost and with no explicit or written terms of use; this was appropriate, since the networks being connected were all part of a research activity that defined a context of trust and mutual adherence to unwritten norms of behavior and interaction.

However, early on, network operators found that one size did not fit all and that there were likely to be a large number of small networks in addition to the small number of very large networks. Since network numbers had been assigned sequentially, a cute hack was devised: if the first bit of the address was "0", that would be a "class A" network able to have up to 16,777,216 hosts. If the first two bits were "10", that would be a "class

resource record to associate that domain name (i.e., "143.2.0.192.IN-ADDR.ARPA") with its hostname (e.g., "MYPC.EXAMPLE.COM"), a mapping specification defined in RFC 1034. Today, this functionality is mostly used in logging systems to associate human friendly names with IP addresses and some anti-spam systems since many machines transmitting spam are home computers that have been hijacked by malware and which haven't had their IN-ADDR.ARPA domains set up.

[59] IP6.ARPA serves the same function for IPv6 as IN-ADDR.ARPA does for IPv4, as specified in RFC 3596 (http://tools.ietf.org/html/rfc3596).

B" network, able to have up to 65536 hosts, and if the first three bits were "110", that would signify a "class C" network, able to have up to 256 hosts. The math of this partitioning meant that there could be up to 128 "class A" networks (covering the addresses 0.0.0.0–127.255.255.255), up to 32,768 "class B" networks (covering 128.0.0.0–191.255.255.255), and up to 2,097,152 "class C" networks (covering 192.0.0.0–223.255.255.255).

This "classfull" partitioning of the address space according to the first three[60] bits of the address meant that all of the allocations that had been made earlier could be grandfathered in, and still provide flexibility in the size of new network assignments that could be made. Allocations were still largely a matter of "ask and you shall receive," although a requester would be asked "why?" if they requested a "class A," and the logistics of maintaining the list of network numbers was migrated from Dr. Jon Postel doing the work himself to "the NIC" operated by the Stanford Research Institute (now SRI International) under a DoD contract.

In the mid–80s, most of the network numbers being allocated were "class Bs" since "class As" were considered to be too large and "class Cs" were considered to be too small.[61] Projections of network number consumption suggested that the "class Bs" would be exhausted by the mid-90s.[62] In addition to triggering the beginnings of the development of what would become IPv6, these projections of "class B" exhaustion resulted in a move towards "classless" addressing, in which the fixed class boundaries were relaxed and instead of a medium-sized requester getting a "class B" they'd get a contiguous set of "class C" networks sufficient to meet their actual requirements.

By the mid–90s, with the increased commercial use of the Internet (particularly within the U.S.[63]), a proliferation of "class C" networks resulting from "classless" addressing was causing significant strain on the Internet's routing system—the routers of the day, only being aware of "classfull" addressing, didn't have sufficient memory to hold all of the networks being announced, and the update messages indicating whether a network was reachable or not were using up all of the routers' Central Processing Unit (CPU) capacity. In addition, growth of the Internet internationally was resulting in political pressure for a distributed allocation system instead of one centralized within the U.S. In an effort both to limit the growth of the routing system as well as to distribute the

[60] There are two additional classes of addresses: "Class D" (first four bits "1110"), used for "multicast"; and "Class E" (first four bits "1111"), which was reserved for future use. However, discussion of these classes is out of scope for this document.

[61] See http://tools.ietf.org/html/rfc1517, section 1.

[62] See http://www.watersprings.org/pub/id/draft-solensky-csharp-00.txt, "Background" section.

[63] Outside of the U.S., most organizations assumed the eventual uptake of OSI-based protocols, and therefore requests for addresses were dominated by U.S.-based organizations. Some of this debate can be found within RFCs in the late 1980s to early 1990s period, e.g., in RFC 1287 (http://www.ietf.org/rfc/rfc1287.txt) section 1.2.

network allocation mechanisms, the RIR system[64] was created and tasked with ensuring that only allocations that could be justified by actual network requirements would be made.

The result of this history and how the Internet was deployed is an unequal distribution of IPv4 addresses: organizations such as universities that were involved in the Internet in the very early days (before the late 80s) were able to get huge blocks of addresses with essentially no justification, whereas later entrants—even national-sized networks—had to make do with only what they could justify to the allocating body. This unequal distribution continues to be a political issue today, particularly as the pool of unallocated IPv4 addresses is consumed.

4.1.2 IPv4 Address Management

The process by which IPv4 addresses are allocated as part of the IANA Functions was documented in https://www.icann.org/resources/pages/allocation-ipv4-rirs-2012-02-25-en. However, as of 3 February 2011 that policy has been made obsolete by the consumption of the free pool of IPv4 addresses managed as part of the IANA Internet Numbers Management Function. Today, the relevant policy for the IANA Internet Numbers Management Function is entitled "Global Policy for Post Exhaustion IPv4 Allocation Mechanisms by the IANA,"[65] which describes the process by which address space returned to the IANA Internet Numbers Management Function provider can be reallocated to the RIRs. Once the criteria of that policy have been met, IANA staff modify the IPv4 address registry[66] to reflect the assignments made as dictated by the policy.

4.1.3 IPv6 Address Management

The IPv6 address space is so much larger than the IPv4 space that even the fraction (⅛) that has been designated by the IETF to be used for "normal" ("global unicast") IPv6 addresses and allocated by the Internet Numbers Registry system is incomprehensibly larger than the entire space for IPv4 addresses.[67] In addition, as a result of global policy,[68] the size of IPv6 address blocks allocated by the IANA Internet Numbers Registry Management function to the RIRs is so large—each RIR gets 1/4096th of the global unicast address space[69]—that it is unlikely under current sub-allocation policies that the

[64] At the time at which this Report was written there were five RIRs, each responsible for a particular geographic region: AfriNIC (Africa), APNIC (Asia Pacific), ARIN (North America and parts of the Caribbean), LACNIC (Latin America and parts of the Caribbean), and the RIPE-NCC (Europe, the Middle East, and the Former Soviet Union countries).

[65] See https://www.icann.org/resources/pages/allocation-ipv4-post-exhaustion-2012-05-08-en.

[66] See http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml.

[67] It's actually 42,535,295,865,117,307,932,921,825,928,971,026,432 addresses.

[68] See http://www.icann.org/en/resources/policy/global-addressing/allocation-ipv6-rirs.

[69] That is, 83,076,749,736,557,242,056,487,941,267,521,536 addresses.

RIRs will require a significant number of additional blocks in the foreseeable future.[70] It is also true, of course, that when the original 32-bit IP address space was defined in 1974, the same "could not possibly ever be exhausted" language was used by its designers.

The process by which IPv6 address blocks are allocated to the RIRs is similar to the process by which the IANA Internet Numbers Management Function Operator allocated IPv4 address blocks prior to the exhaustion of the IPv4 free pool. The global policy by which IPv6 addresses are allocated specifies when IANA staff can perform the allocation (when the RIRs' "available space" falls below a defined threshold, or is insufficient to satisfy their requirements for the next 9 months) and the size of the allocation. Upon receipt of a request from an RIR that meets the global policy criteria, IANA staff modify the IPv6 "IPv6 Global Unicast Address Assignments" registry[71] and inform the RIR of their assignment.

4.1.4 Autonomous System Number Management

The IANA Internet Numbers Registry Management function allocates blocks of Autonomous System Numbers (ASNs) to the RIRs for sub-allocation to requesting organizations. Initially, there were only 65,536 ASNs (that is, the protocol field for ASNs was 16 bits wide); however, the IETF expanded the ASN space to 32 bits or over 4 billion ASNs, and in 2006 the first blocks of 32-bit ASNs were handed out to the RIRs.

Although fewer than 500 unallocated 16-bit ASNs remain in the IANA free pool, the transition to 32-bit ASNs has progressed sufficiently that significant issues are unlikely to arise with the exhaustion of the 16-bit ASN space.

4.2 Change Request Processing

Since there are only five RIRs and the exhaustion of Internet Number resource blocks allocated by the IANA Internet Numbers Function to the RIRs is both infrequent and somewhat predictable, requests for changes or additional resources by the RIRs are validated by interactions between IANA functions staff and RIR staff directly.

ICANN has developed software[72] to automate changes to the IN-ADDR.ARPA and IP6.ARPA zones, using ICANN–allocated client certificates given to the 5 RIRs. With a small number of exceptions[73] that are managed by ICANN as the IANA Function

[70] The blocks allocated by the IANA Internet Numbers Registry function to each of the RIRs represents sufficient address space for each RIR to provide IPv6 addresses to over 1 million ISPs (with each ISP being able to supply over 65,000 customers). Currently, the combined membership of all of the RIRs is fewer than 20,000 ISPs.

[71] See http://www.iana.org/assignments/ipv6-unicast-address-assignments.

[72] The technical process and protocol ICANN developed for this purpose is documented at http://tools.ietf.org/html/draft-manderson-rdns-xml-01.

[73] The exceptions are related to delegations associated with private IPv4 addresses—10.IN-ADDR.ARPA (see RFC 1918, http://tools.ietf.org/html/rfc1918)—and IPv4 multicast addresses.

Operator directly, the RIRs manage all of the delegations under the IN-ADDR.ARPA and IP6.ARPA zones.

4.3 US Government Involvement in Internet Number Resource Management

Historically, NTIA has not authorized individual allocations of blocks of addresses or autonomous system numbers by the IANA Function Operator. In the past, NTIA did review the global policies as accepted by the ICANN Board of Directors prior to their implementation, but there was no approval role associated with this review.

5 Protocol Parameter Registry and .ARPA TLD Management Function

This IANA function consumes the most human resources associated with the IANA Functions Contract at ICANN due to the number of registries involved.[74] Protocol parameters are well-known (that is, publicly documented) numbers or strings of characters that are used by implementations of protocols defined (primarily) by the IETF.

The "Address and Routing Parameter Area" TLD is used in protocols that use the DNS as a globally distributed database to look up particular values of interest. In most cases, these values are used by applications rather than being intended to be seen directly by Internet users. Originally used by the U.S. Department of Defense to reference hosts on the ARPAnet (a predecessor to the Internet), during 2000 the ".ARPA" domain name label was re-designated[75] and is now used for protocol purposes.

5.1 Protocol Parameter Registry Management

As mentioned, protocol parameters are values used within the implementations of protocols. These values are defined so that different implementations of a protocol can interoperate without additional information. Protocol parameters include the following, as examples:

1) the version number (4) for the most commonly used Internet Protocol, IPv4;[76]
2) the "port" (80) or "service name" (Hypertext Transfer Protocol (http)) used for the world wide web;[77]

[74] The list of all protocol parameter registries is available at http://www.iana.org/protocols.

[75] See http://tools.ietf.org/search/rfc3172, Appendix A.

[76] The Protocol Parameter registry for IP version numbers is found at http://www.iana.org/assignments/version-numbers/version-numbers.xhtml#version-numbers-1.

[77] The ports/service name registry is found at http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

3) Private Enterprise Numbers, *e.g.*, “1.3.6.1.4.1.5901” (or using mnemonics, “iso.org.dod.internet.private.enterprise.nominum”), used primarily in network management applications;[78] and
4) the DNS Resource Record Type code (99) and mnemonic (SPF) for the “Send Policy Framework” resource record.[79]

There are over 1000 individual protocol parameter registries, each consisting of a text file that describes the parameter and the values that have been registered. Each of the registries has its own policy for creation, modification, and deletion. Some registries contain only one or two values, whereas other registries contain tens of thousands of values. Some registries are rarely if ever modified, and others are updated on a daily or weekly basis. The IETF, IESG, or IAB define the protocol parameters and the policy by which those parameters are created, modified, or deleted, most commonly in the (required) “IANA Considerations” section of RFC documents. In the vast majority of cases, the protocol parameter registries can be seen as primarily archival—the information defined within the registries is the permanent record of value assignments, but changes to those registries do not affect the operation of the Internet directly. For a change to one of these registries to affect the operation of the Internet, protocol implementers would need to create or update their implementations to reflect the new values and then have those implementations deployed on the Internet.

Examining how one particular registry—the IP version number registry, where the terms IPv4 and IPv6 come from—works may be helpful in understanding the role of the IANA Protocol Parameters registry function. Conventions established very early in what would become the Internet defined the first 4 bits of every packet on the network to be the version of the protocol used by that packet. This allowed multiple versions of the Internet Protocol to be used on the network simultaneously—a computer could look at the first four bits of a packet it received and hand that packet off to software that was capable of understanding the version of IP being used by the packet. As new versions of the Internet Protocol were developed, the community of protocol developers would agree to assign the next sequential version number and have Dr. Jon Postel, who was acting as “the Internet Assigned Numbers Authority,” record that number.

RFC 750, the “Assigned Numbers” RFC published in 1978, documents 5 different Internet Protocol versions as shown in Table 1.

[78] The PEN registry is found at http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers.

[79] The DNS Resource Record registry is found at http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4.

Bits	Decimal	Description
0000	0	March 1977 version
0001	1	January 1978 version
0010	2	February 1978 version A
0011	3	February 1978 version B
0100	4	September 1978 version 4

Table 1. IP Version Registry (as of 1979)

The "September 1978 version 4" Internet Protocol became the basis for what would eventually become the Internet's underlying protocol, IPv4.

However, Internet protocol development did not stop. By 1980, a new protocol known as "Stream Protocol" was developed; its author requested an IP version number, and was assigned version "0101" (decimal 5). The next major development in the Internet Protocol came in the early 1990s, when the limitations of IPv4 were addressed and the community of protocol developers in the IETF created a number of different alternatives for "Internet Protocol Next Generation." In 1994, Dr. Jon Postel (still acting as "the IANA") assigned Internet Protocol versions 6 through 9. In addition, as the earlier versions of the Internet Protocol (versions 0–3) were no longer in use, he removed version numbers 0 through 3 from the IP version number registry. The resulting registry is shown in Table 2.

Bits	Decimal	Keyword	Version
0000	0	(reserved)	
0001	1	(unassigned)	
0010	2	(unassigned)	
0011	3	(unassigned)	
0100	4	IP	Internet Protocol
0101	5	ST	ST Datagram Mode
0110	6	SIP	Simple Internet Protocol
0111	7	TP/IX	The Next Internet
1000	8	PIP	The P Internet Protocol
1001	9	TUBA	TCP and UDP over Bigger Addresses

Table 2 IP Version Registry (as of 1994)

As the Internet continues to evolve, new versions of the Internet Protocol may be standardized by the IETF. If this occurs, the next version number to be allocated will be "1010" in binary, 10 in decimal. However, instead of Dr. Jon Postel performing this function, the IANA Functions Operator performing the Protocol Parameter Registry Management function will do the actual registry modification using the normal, routine protocol and parameter registry processes, just as it would for any other protocol parameter.

5.2 Management of Address and Routing Area (.ARPA) TLD

The management of the .ARPA TLD consists of adding delegations to second level domains under .ARPA and modifying the delegation (and DNSSEC) information associated with the .ARPA zone itself. Changes to the .ARPA zone are authorized[80] by the IAB, typically at the direction of IETF working groups.

The contents of the .ARPA zone are managed by ICANN as IANA Functions Operator; signing the .ARPA zone using DNSSEC and distribution of the resulting signed zone to name servers is currently carried out by Verisign, although the IANA Functions Contract specifies that this responsibility will transition to ICANN.[81]

Each of the second level domains in the .ARPA zone, the management of which is **not** included in the IANA Functions contract, corresponds to a particular protocol use. At the time at which this Report was written, the sub-zones and their purpose are:

- E164.ARPA. This sub-domain is used for the ENUM protocol,[82] which facilitates the translation of telephone numbers (ITU-T Recommendation E.164 identifiers) for use in the Internet. The IAB has delegated administration of this zone to RIPE-NCC, which has an exchange of letters with the ITU for the management of the zone. The IAB instructions for the management of E164.ARPA can be found at http://www.ripe.net/data-tools/dns/enum/iab-instructions.

- IN-ADDR.ARPA. This sub-domain is used by the DNS to enable the mapping of IPv4 addresses to domain names. For example, if you have the IPv4 address 192.0.2.1, you can discover the domain name that corresponds to that address by reversing the order of the numbers, putting "." between them, appending ".IN-ADDR.ARPA", and doing a PTR (pointer) lookup of the resulting domain name "1.2.0.192.IN-ADDR.ARPA". Termed "reverse DNS," these mappings are now primarily used to make log messages that have IP addresses in them more easily readable by humans.

  228 entries in the IN-ADDR.ARPA zone correspond to the highest-level blocks of addresses that have been allocated (or, in some cases, reserved) as part of the IANA Internet Numbers Registry Management function, ranging from 1.IN-ADDR.ARPA to 239.IN-ADDR.ARPA.[83] Most of these delegations are made to the name servers operated by the RIRs that received the allocation of the block. However, in the cases in which assignments were made of blocks of over

[80] The IAB's responsibility for authorizing changes to the ARPA zone is described in RFC 3172 (http://tools.ietf.org/html/rfc3172).

[81] ICANN's response to the IANA Functions Contract RFP volume 1, section 1.2.9.1.4, http://www.ntia.doc.gov/files/ntia/publications/icann_volume_i_elecsub_part_1_of_3.pdf

[82] http://tools.ietf.org/rfc/rfc6116.txt

[83] The blocks in the range from 240 to 255 are reserved for future use (they are the former "Class E" addresses defined by RFC 1112). Within the 255 block, the "all ones" address 255.255.255.255 is reserved by RFC 919 for "limited broadcast." Of the possible blocks between 1 and 239, only 228 are represented in IN-ADDR.ARPA.

16 million contiguous addresses,[84] the delegations are made to the companies that received the blocks; e.g., Hewlett Packard (HP) was allocated 16.0.0.0/8, and the name servers for 16.IN-ADDR.ARPA are managed by HP. Changes to these "legacy" delegations are made through the RIR responsible for the region in which the end-user is based, not by direct interaction between the end-user organization and ICANN.

- IN-ADDR-SERVERS.ARPA. This sub-domain contains the name servers used for doing lookups in the IN-ADDR.ARPA zone.[85]

- IP6.ARPA. This sub-domain serves the same purpose for IPv6 that IN-ADDR.ARPA serves for IPv4. For example, given the IPv6 address 2001:db8:1000:9700::dead:beef, one may discover the domain name that corresponds to that address by reversing the order of the hexadecimal digits (inserting the appropriate number of zeros for the "::" shorthand[86]), putting "." between them, appending ".IP6.ARPA", and performing a PTR (pointer) lookup of the resulting domain name "F.E.E.B.D.A.E.D.0.0.0.0.0.0.0.0.0.0.0.7.9.0.0.0.1.8.B.D.0.1.0.0.2.IP6.ARPA."

  As with IN-ADDR.ARPA, the entries in the IP6.ARPA zone reflect the top-level block allocations made to the RIRs by the IANA Functions operator as part of the Internet Numbers Registry Management function. However, unlike IN-ADDR.ARPA, there are no "legacy" allocations—all of the allocations in the IPv6 address space either have been made to the RIRs or are IETF–specified reservations.

- IP6-SERVERS.ARPA. This sub-zone contains the name servers used for performing lookups in the IP6.ARPA zone.

- IPV4ONLY.ARPA. This sub-zone is used for one of the IPv6 transition protocols, providing a way to detect the presence of the DNS64 transition technology (RFC 6147) and to learn the IPv6 prefix used for protocol translation on an access network.

- IRIS.ARPA. This sub-zone is used for the "Internet Registry Information Service," an implementation of the "Cross Registry Internet Service Protocol"

[84] Actually, a multiple of 16,777,216 reflecting at least 24 bits of address, known as "/8s". Since IN-ADDR.ARPA domain names are broken down by the octets of the addresses (in reverse), an organization that has received an entire /8 can be delegated the octet in the IN-ADDR.ARPA zone.

[85] The use of IN-ADDR-SERVERS.ARPA and IP6-SERVERS.ARPA is specified in RFC 5855 (http://tools.ietf.org/html/rfc5855).

[86] See http://tools.ietf.org/html/rfc5952.

(CRISP)[87] that was intended to eventually replace the "WHOIS" protocol as a mechanism by which registration information could be looked up over the Internet. The IRIS/CRISP protocol failed to gain significant acceptance.

- URI.ARPA. This sub-zone is used within the Dynamic Delegation Discovery System (DDDS)[88] to register "Uniform Resource Identifiers." Defined in 2002, this system has failed to gain significant acceptance.

- URN.ARPA. This sub-zone is used within the Dynamic Delegation Discovery System (DDDS) to register "Uniform Resource Names." Defined in 2002, this system has failed to gain significant acceptance.

The only other entries in the .ARPA zone are the "start of authority" (SOA), name server (NS), and DNSSEC-related records for the zone itself.

5.3 U.S. Government Involvement

There is essentially no direct U.S. government involvement in the protocol parameter registry management function.

The management of the .ARPA zone is theoretically somewhat complicated due to separate, potentially competing claims of authority between the IETF community and NTIA vis-à-vis the IANA functions contract and RFC 3172.

IETF RFC 3172 states:

> *The Internet Architecture Board (IAB) has the responsibility, in cooperation with the Internet Corporation for Assigned Names and Numbers (ICANN), to manage the "arpa" domain.*

and

> *The operational administration of this [arpa] domain, in accordance with the provisions described in this document, shall be performed by the IANA under the terms of the MoU between the IAB and ICANN concerning the IANA [RFC 2860].*

However, section C.2.9.1 of the IANA Functions contract[89] explicitly includes management of the .ARPA zone as one of the IANA Functions.

In practice, this potential issue has not come up. As the .ARPA zone and the sub-zones administered by the IANA Functions operator are quite stable, receiving perhaps one update request per year on average, there have been no cases in which contention has

[87] See http://tools.ietf.org/html/rfc3707.

[88] See http://www.ietf.org/rfc/rfc3401.txt.

[89] See http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf, page 6.

arisen regarding the role of the U.S. government in administering the .ARPA zone.[90] Furthermore, NTIA does not play a role in the day–to–day management of the .ARPA zone.

6 Management of the .INT TLD

The .INT zone, introduced into the root zone in 1988 and documented in RFC 1591 in 1994, was originally established to house

> *[…] organizations established by international treaties, or international databases.*[91]

Originally, the IETF intended to relocate the IN-ADDR.ARPA domain to the .INT zone as IP4.INT, and to establish the IP6.INT domain for the same use as IP6.ARPA; and to delegate .INT to the International Telecommunications Union (ITU) Secretariat. However, with the publication of RFC 3172, the IETF community decided to re-designate the .ARPA zone for the purpose of "international databases."

The current definition of what constitutes "organizations established by international treaties" is found at http://www.iana.org/domains/int/policy and is not without some controversy. Specifically, criterion 3 states:

> *The organization that is established must be widely considered to have **independent international legal personality** and must be the subject of and governed by international law. The declaration or the treaty must have created the organization. If the organization created is a secretariat, it must have a legal personality. For example, it must be able to enter into contracts and be party to legal proceedings.*

This requirement for a legal personality has blocked some organizations associated with treaties from obtaining a .INT delegation.

As of 15 July 2014, there were 184 delegations in the .INT zone. While there are a few historical oddities (e.g., TPC.INT[92] and YMCA.INT[93]), the vast majority of entries in the .INT zone correspond to international treaty organizations according to all of the criteria documented in the .INT policy.

[90] In the past, concerns were expressed about NTIA's involvement in the administration of some .ARPA sub-zones; those concerns were allayed when it was understood that NTIA's involvement relates only to the .ARPA zone, not its sub-zones.

[91] See RFC 1591 (http://tools.ietf.org/html/rfc1591), section 2 (page 2).

[92] The domain TPC.INT refers to "The Phone Company" (a reference to the movie "*The President's Analyst*," http://www.imdb.com/title/tt0062153/) and was an early (circa 1993) experiment at using the Internet to bypass standard telephone services for faxes. A brief description of TPC.INT can be found at http://museum.media.org/invisible.net/project/tpc.int.html and its principles of operation are documented in http://tools.ietf.org/html/rfc1703.

[93] The domain YMCA.INT is associated with the Young Mens' Christian Association.

6.1.1 US Government Involvement in .INT TLD Management

The NTIA has no role in the day-to-day operation of the .INT domain. As .INT management is considered to be an IANA Function, questions relating to the U.S. government involvement in setting management policy—e.g., criteria for obtaining a .INT domain—remain open.

7 Current IANA Functions Work Effort

This section provides information to give the reader some context regarding the scale of work currently involved in performing some of the IANA Functions. The data are derived from statistics published by IANA from September 2013 to April 2014 in accordance with Section C.4.4 of the IANA Functions Contract with the U.S. Government.[94]

7.1 DNS Root Zone Management

Over the 8 month measurement period 485 DNS Root Zone Management transactions were processed, the majority of which were related to ICANN's new gTLD program. In Table 3, "Change Requests" refers to changes made to the root zone file or the IANA TLD registration ("WHOIS") database. The rows labeled "ccTLD Redelegation" and "gTLD Delegations" describe the redelegation or delegation of ccTLDs and gTLDs respectively.

Transactions	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
Change Request	21	22	25	24	57	24	35	18
ccTLD Redelegation	0	1	0	0	0	0	0	3
gTLD Delegation	0	4	28	41	49	41	35	58
Totals	**21**	**27**	**53**	**65**	**106**	**65**	**70**	**78**

Table 3. DNS Root Zone Management Transactions

Table 4 provides data related to the amount of time taken to process requests,[95] with the columns "Median," "90th Percentile," "Maximum," and "SLC" describing respectively the median number of days to process a request, the number of days within which 90 percent of the requests were processed, the maximum number of days it took to process a request, and ICANN's Service Level Commitment (the number of days ICANN has committed to processing the particular requests in the IANA Functions Contract).

[94] The data are available at http://www.iana.org/performance/metrics.

[95] The processing times for the 3 ccTLD delegation/redelegation requests were not included in this table since the small sample size means that the data lack statistical significance. The median time measures the end-to-end time from receipt of a request by IANA to the final fulfillment of the request by Verisign. In other words, this measures the system performance of the requestor, IANA, NTIA, and Verisign.

Transaction	Median	90th Percentile	Maximum	SLC
Change Request	5	14	39	21
gTLD Redelegation	6	13.5	23	30

Table 4. DNS Root Zone Management Processing Times (in days)

7.2 Internet Numbers Registry Management

Over the 8 month measurement period 3 Internet Numbers Registry management requests were processed. Two of those requests occurred in September 2013 and one occurred in February 2014. The median time to complete these three requests was 1.92 days, the 90th percentile was 3.56 days, and the maximum was 3.71 days, all well within the service level commitment of 7 days specified by the ASO-MoU.

7.3 Protocol Parameter Registry Management

Over the 8 month measurement period 2695 protocol parameter registry management transactions were processed. In Table 5, these transactions are broken down into the following categories:

1) "IANA Considerations"—IANA staff implements the instructions specified in the "IANA Considerations" section of RFCs and some Internet Drafts.[96]
2) "Draft Review"—IANA staff review all Internet Drafts during the IETF "Last Call" process or when the IESG requests a review.
3) "Port Registry"—Create, modify, or delete entries in the IANA Port Registry.
4) "PEN Registry"—Create, modify, or delete entries in the IANA Private Enterprise Number Registry.
5) "Other Registry"—Create, modify, or delete either a registry or the contents of a registry, e.g., media types, TRIP ITAD numbers, etc.

[96] This category also counts updating references to Internet drafts.

Transactions	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14	Apr-14
IANA Considerations	51	46	48	36	71	64	45	75
Draft Review	67	62	55	64	53	59	37	44
Port Registry	19	12	8	16	22	22	15	17
PEN Registry	177	197	183	174	187	173	181	176
Other Registries	38	28	17	17	29	19	42	49
Totals	**352**	**345**	**311**	**307**	**362**	**337**	**320**	**361**

Table 5: Protocol Parameter Registry Transactions

At the time at which this Report was written, data on processing times for protocol parameter registry management requests were not available.

8 Agreements

This section gives an overview of the agreements, formal or otherwise, that are related to the IANA Functions contract.

8.1 IANA Functions Contract

The NTIA maintains a web page[97] that provides copies of all of the IANA Functions contracts and their modifications since October 1, 2000.

Between 1997 and 1 October 2000, the IANA Functions were performed as Task 4 of the DARPA Tera-Node project.[98] Task 4 was created in reaction to increased scrutiny of the IANA Functions as a result of NSF permitting Network Solutions to charge for domain names. Explicit references to "the IANA Functions" prior to 1997 have been difficult to locate, and anecdotal information suggests that no documentation of the IANA Functions prior to 1997 exists.

Following the termination of DARPA funding for the Tera-Node project (which included funding for the IANA Functions) and prior to the institution of the NTIA IANA Functions Contract there was a short period of time during which the IANA Functions had no explicit funding. During this period, the RIRs that existed at the time (RIPE-NCC and APNIC) provided funding directly to USC/ISI to fund IANA Functions operations.

[97] See http://www.ntia.doc.gov/page/iana-functions-purchase-order.

[98] See http://www.osti.gov/scitech/servlets/purl/802104.

The current IANA Functions contract is explicitly zero–cost to the U.S. government, and any fees charged by ICANN for the provision of the IANA Functions must be on a cost–recovery basis.

8.2 Between ICANN and the IETF

RFC 2860, entitled "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority," documents the MoU between the IETF and ICANN. Published in June 2000, it provides the mutually–agreed basis for the administration of the IETF–related resources by ICANN. These resources explicitly include:

1) Internet protocol parameters (section 4.1);
2) Domain names used for technical purposes (section 4.3(a));
3) Address blocks used for specialized purposes (section 4.3(b)); and
4) Experimental assignments of domain names or addresses that are not considered policy issues (section 4.3(c)).

The MoU also requires ICANN to make "information about each current assignment, including contact details for the assignee" publicly available free of charge; to provide on-line facilities to request protocol parameter assignments; and to review all documents in IETF "Last Call" to identify issues or concerns and raise those issues or concerns with the IESG.

RFC 3172, entitled "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ('arpa')," describes the agreement between the IETF (specifically, the IAB) and ICANN concerning how the .ARPA domain should be managed. Included in that RFC as an Appendix is a letter from NTIA to ICANN requesting that ICANN "undertake administration of the arpa TLD in cooperation with the Internet technical community under the guidance of the IAB."

RFC 6220, entitled "Defining the Role and Function of IETF Protocol Parameter Registry Operators," provides a description of, and the requirements for, registry functions to record assigned protocol parameter values and their associated semantic intentions.

In addition to the various RFCs, the IETF community has also entered into specific agreements with ICANN relating to the performance of the IANA Functions. These agreements, published as "Supplemental Agreements" in the IANA section of http://iaoc.ietf.org/contracts.html, detail the services and specific service levels required for the performance of the IANA Functions.

It is the view of many within the IETF community that the IETF is solely responsible for the delegation of authority for the various IANA Functions, since all of those delegations proceed from activities necessary for the proper administration of protocols defined by the open, consensus-driven processes of the IETF; and therefore that NTIA's involvement in the activities described by the IANA Functions contract is from an authority standpoint orthogonal to the implementation and administration of those protocols.

8.3 Between ICANN and the RIRs

ICANN entered into an MoU with the Number Resource Organization (NRO)[99] in October 2004.[100] The MoU designates the NRO to fulfill the role of ICANN's Address Supporting Organization (ASO), and defines, in broad policy terms, the interaction between IANA and the RIRs with respect to the pools of available IP addresses and ASNs.

As the IETF has within its domain, the RIRs have historically asserted policy authority over further distribution of IP addresses and ASNs, with IANA functioning primarily as the implementer of regionally–based, bottom–up, consensus–driven policy processes undertaken within the RIR communities.

8.4 Between ICANN and the Root Server Operators

The operators of the Root Servers are independent entities, and with the exception of the A-root server operated by Verisign under a Cooperative Agreement with NTIA[101] provide root service without any formal agreement or service level commitment.

In July 2002, Internet Systems Consortium (ISC) as the operator for the F-root server entered into an MoU with ICANN "Concerning Root Server Operation."[102] This MoU acknowledges the relationship between ICANN and ISC as the operators, respectively, of the IANA Root Zone Management function and the F-root server. Subsequently, in December 2007, ISC and ICANN entered into a "Mutual Responsibilities Agreement" (MRA)[103] that reiterated the understandings specified in the previous MoU, committed adequate resources to their respective responsibilities, and pledged cooperation on issues of mutual interest. It was formally ratified by the ICANN Board of Directors on 23 January 2008.[104]

Although other root server operators have contemplated similar MRAs, the F-root agreement remains unique. However, ICANN and Netnod (the operator of I-root) have exchanged letters[105,106] recognizing each other's roles as root zone authority and root server operator respectively; and RIPE-NCC (the operator of K-root) and WIDE (the operator of M-root) have exchanged similar recognition instruments with ICANN.[107,108]

[99] See https://www.nro.net.

[100] See http://archive.icann.org/en/aso/aso-mou-29oct04.htm.

[101] See http://www.ntia.doc.gov/files/ntia/publications/amend11_052206.pdf.

[102] See http://www.icann.org/en/groups/rssac/model-root-server-mou-21jan02-en.htm.

[103] See http://archive.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf.

[104] See https://www.icann.org/news/announcement-2008-01-23-en.

[105] See http://www.icann.org/en/news/correspondence/lindqvist-to-twomey-08may09-en.pdf.

[106] See http://www.netnod.se/sites/default/files/ICANN-AUTONOMICA-Iroot.pdf.

[107] See http://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-ripe/ripe-ncc-and-icann-commit-to-ongoing-dns-root-name-service-coordination.

[108] See https://www.icann.org/en/system/files/files/murai-to-twomey-06may09-en.pdf.

These agreements are not contracts like those typically executed between commercial parties for "managed DNS" or similar services. They do provide the basis for more detailed agreements in the future if desired. It is also worth noting that the L-root server is operated by ICANN; however, there are no formal agreements or service level commitments under which that root server is operated. It is important also to note that these agreements are with ICANN and are not subject to the IANA Functions contract.

ICANN's Bylaws define an advisory committee—the "Root Server System Advisory Committee" (RSSAC)[109]—to provide input to ICANN's Board and community on topics related to the operation of the Root Server System. In January 2013, ICANN's Bylaws were revised to modify how the RSSAC is constituted.[110] RSSAC has reorganized since then to include formal representation from all of the root server operator organizations. It has put formal mechanisms in place for participation in the broader ICANN community such as the Board and the NomCom. It has also designated a pool of experts in DNS and related network technology to work with the root server operators in generating analysis and advice to the operators, the Board, and the wider community as described in its charter. This may provide a more organized platform for ICANN community interactions with the root server operators than has previously been available.

8.5 Between ICANN and ccTLD Administrators

ICANN has entered into a number of agreements with various ccTLD administrators, which are documented at http://www.icann.org/en/about/agreements/cctlds. These agreements are with ICANN and are not subject to the IANA Functions contract.

8.6 Between ICANN and gTLD Administrators

ICANN has entered into a large number of contractual agreements with the administrators of gTLDs, which are documented at http://www.icann.org/en/about/agreements/registries. These agreements are with ICANN and are not subject to the IANA Functions contract.

9 Summary

The IANA Functions comprise activities that are critical to the ongoing coordination of unique identifiers necessary for the operation of the Internet. Historically performed on an *ad hoc* basis by Dr. Jon Postel and his team at USC/ISI at the request and with the consent of the technical research community, the IANA Functions have more recently become subject to obligations through more formal contracts with the U.S. government and MOUs with organizations such as the IETF and the RIRs.

[109] See http://rssac.icann.org

[110] See http://www.icann.org/en/about/governance/bylaws/proposed-revisions-rssac-03jan13-en.pdf.

The IANA Functions, as defined by the IANA Functions contract, include:

1) DNS Root Zone Management, i.e., making modifications to the DNS root zone and related databases;
2) Internet Numbers Registry Management, i.e., making allocations from and modifications to the IPv4, IPv6, and Autonomous System Number registries;
3) Protocol Parameter Registry and .ARPA TLD Management, i.e., creating protocol parameter registries and creating, modifying, and deleting entries within those registries; and
4) Management of the .INT zone.

RFC 2860 documents an MOU between the IETF and ICANN that designates ICANN as the entity responsible for ensuring that the protocol parameters registries are updated. RFC 3172 describes the re-designation of the .ARPA domain to “Address and Routing Parameter Area” and places administration of that domain with the IAB.

The primary role of the U.S. government, through NTIA, is in the context of DNS Root Zone Management, acting as the Root Zone Administrator. However, the U.S. government may also provide a number of implied services including a mechanism that ensures some level of accountability of ICANN.

10 Acknowledgments, Disclosures of Interest, Dissents, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members, outside experts, and ICANN staff who contributed directly to this particular document. The Disclosures of Interest section points to the biographies of all SSAC members, which disclose any interests that might represent a conflict—real, apparent, or potential—with a member’s participation in the preparation of this Report. The Dissents section provides a place for individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have recused themselves from discussion of the topic with which this Report is concerned. Except for members listed in the Dissents and Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

10.1 Acknowledgments

SSAC thanks the following members and external experts for their time, contributions, and review in producing this Report.

SSAC members

Joe Abley
Jaap Akkerhuis
Don Blumenthal
Lyman Chapin

David Conrad[111]
Steve Crocker
Patrik Fältström
Jim Galvin
Mark Kosters
Jason Livingood
Danny McPherson
Ram Mohan
Russ Mundy
Suzanne Woolf

ICANN staff

Julie Hedlund
Patrick Jones
Barbara Roseman
Steve Sheng
Jonathan Spring

10.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at https://www.icann.org/resources/pages/biographies-2014-06-06-en.

10.3 Dissents

There were no dissents.

10.4 Withdrawals

There were no withdrawals.

[111] David Conrad participated in the preparation of this Report as an SSAC member prior to assuming his current position as ICANN CTO.