ICANN and the IETF

ICANN Office of the Chief Technology Officer

David Huberman
OCTO-043
16 April 2026

TABLE OF CONTENTS

This document is part of ICANN's Office of the Chief Technical Officer (OCTO) document series. Please see the OCTO publication page for a list of titles in the series. If you have questions or suggestions on any of these documents, please send them to octo@icann.org.

This document supports ICANN's strategic goal to sustain and improve openness, inclusivity, accountability, and transparency. It is part of ICANN's strategic objective to improve the effectiveness of ICANN's multistakeholder model of governance.

Introduction

The Internet's infrastructure is maintained by the coordinated efforts of many. The engagement of the Internet Corporation for Assigned Names and Numbers (ICANN) with the Internet Engineering Task Force (IETF) constitutes one essential thread in that fabric. Both communities work to keep the global Internet functioning as a single, interoperable network. Although ICANN and the IETF have different mandates, their missions are deeply intertwined.

This relationship is the main theme of this paper. The IETF is fundamentally important to ICANN and has been since day one of ICANN's formation.

Part One of this report explores the relationship between ICANN and the IETF. It describes how the two organizations and their communities interact, and why the time and energy ICANN commits to the work of the IETF is warranted.

Part Two provides an update on several key Domain Name System (DNS)-related activities that occurred at the IETF in 2025 that participants in the ICANN ecosystem may find useful and informative.

All three pillars of the ICANN community regularly participate in the IETF. This paper, however, focuses on how staff inside ICANN Org interact with the IETF.

Part One

1. Two Organizations, One Internet

ICANN's engagement with the IETF is a mission-critical activity for ICANN. The protocols that underpin ICANN's responsibilities originate at the IETF, and those protocols continue to evolve. Participating in the IETF means being present where technical decisions that affect the Internet's unique identifier system are made.

ICANN's relationship with the IETF is also a formal one: the two organizations signed a Memorandum of Understanding (MoU) more than a quarter century ago, memorialized in Request for Comments (RFC) 2860, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority". The MoU establishes ICANN as the technical operator that assigns Internet protocol parameters on behalf of the IETF. Those assignments are governed by IETF policy (not ICANN policy). Supplements to this RFC formalize mutual support of these activities. In the RFC and the supplements, ICANN commits to service levels and transparency in carrying out its duties, while the IETF commits to providing expertise and guidance.

ICANN staff contribute to the IETF, serving as authors on Internet-Drafts, Area Directors, working group chairs, Designated Experts reviewing IANA registration requests, and active contributors to working group discussions on mailing lists. ICANN staff also attend IETF meetings three times a year. Many ICANN staff members were active in the IETF long before joining the ICANN organization, bringing with them decades of experience and the trust that comes from sustained engagement in the standards community. ICANN benefits enormously from having these people on staff.

The IETF operates on rough consensus and running code, and therefore no organization can simply impose its preferences. ICANN invests in staff engagement with the IETF to ensure that the perspectives of the unique identifier system's operators and stakeholders are heard as protocols are designed and extended. This engagement also helps all of ICANN to stay informed about technical developments that may affect ICANN's operations or policy work.

The IETF is also where adjacent communities convene. The root server operators hold their technical coordination meetings at IETF events. ICANN's Root Server System Advisory Committee (RSSAC) Caucus meets at even-numbered IETF meetings. Security researchers, DNS software developers, and registry operators gather in IETF working groups to solve shared technical problems.

2. The IANA Functions

The IANA functions sit at the intersection of protocol development and operational reality. When the IETF publishes a new standard, it often requires entries in an IANA registry. These registries are the authoritative lists of protocol parameters: port numbers, DNS record types, cryptographic algorithm identifiers, error codes, and thousands of other technical values that implementations rely on to interoperate. When software developers write code that speaks an Internet protocol, they often consult IANA registries to ensure they are using values that other implementations will recognize.

To maintain this infrastructure, IANA staff review every document that progresses through the IETF's standards process, ensuring that new protocol parameters are properly registered and that the registries remain accurate and consistent. IANA also publishes monthly performance reports against their service level agreements negotiated with the IETF, runs an active help desk at every IETF meeting, and meets regularly with IETF leadership to address potential concerns. This operational relationship, built over decades of collaboration, requires continuous engagement. The source of this relationship is the agreements between ICANN and the IETF, although this document does not attempt to describe the full scope of the IANA Protocol Parameters Function.

3. Informing the ICANN Community

The relationship between the IETF and ICANN benefits both communities.

ICANN's engagement in the IETF does not only serve the needs of protocol development, it also generates knowledge that benefits the broader ICANN community. When new protocols are standardized, ICANN staff bring that information back to the community. And when IETF working groups address topics that may affect ICANN policy, early and ongoing awareness allows the ICANN community to understand technical constraints and opportunities as they develop. ICANN uses many communication channels to convey this important information. The OCTO team publishes blogs (and papers like this). The OCTO Technical Engagement team regularly conveys changes in the protocol landscape in its technical talks and trainings.

When ICANN's Security and Stability Advisory Committee (SSAC) decides which work parties to start, it considers what is currently happening at the IETF. The SSAC cites many RFCs in its publications. One recent example of this is RFC 9859, "Generalized DNS Notifications" (co-

authored by SSAC member John Levine). This RFC addresses a problem that was identified and studied in the SSAC's "DS Automation" work party.

Many IETF participants, in turn, serve on ICANN supporting organizations, advisory committees, and the ICANN Board, bringing technical expertise into ICANN's multistakeholder governance processes. This cross-pollination strengthens both communities and the Internet more generally.

Part Two

This section covers protocol development in IETF working groups in 2025 that may be important to those interested in the ICANN ecosystem.

4. Working Group: DELEG

Introduction

When someone types a domain name into their browser, the DNS does not look up the answer in one place. Instead, it follows a chain of *referrals*. The root zone points to the servers for ".com," and .com points to the servers for "example.com," and so on down the hierarchy. Each instance of "points to" is called a referral.

Referrals in the DNS have worked the same way since the 1980s, using a record type called the *NS record*. An NS record does only one thing: It provides the hostname of a nameserver for the next zone in the chain. A resolver must then gather any additional information on its own. This process was sufficient for four decades. However, in recent years the DNS has become far more sophisticated than its delegation mechanism reflects.

Because NS records carry little information, no standardized way for a parent zone (like .com) to communicate richer details about a child zone's nameservers (like those for example.com) exists. For example, a domain holder who outsources their DNS hosting to a third-party provider is unable to easily signal that change back up to the parent. Similarly, as the Internet community has developed encrypted transport options for DNS, such as DNS-over-TLS and DNS-over-HTTPS, no place exists in the current delegation model to advertise support for those protocols.

The DNS Delegation (DELEG) protocol addresses these shortcomings.

The DELEG Working Group at the IETF is tackling the problem of modernizing DNS delegation by designing a new DNS record type called DELEG that would supplement the NS record for delegation purposes. A DELEG record is extensible, meaning it can carry structured parameters beyond just a nameserver's hostname. It can include IP addresses (which would help solving issues around the fact that NS records only give names, not addresses), signal support for encrypted transports, and support "delegation aliasing," where a domain holder points to a service provider who then supplies the full delegation details.

Importantly, unlike NS records, DELEG records will be authoritative at a delegation point of a zone and thus can be signed with Domain Name System Security Extensions (DNSSEC). This closes a longstanding gap where referral responses could not be cryptographically

authenticated. The goal is an incremental, backwards-compatible upgrade. Existing DNS software would continue to work with NS records as it always has, while DELEG-aware resolvers and servers would gain access to a much richer and more secure delegation mechanism.

DELEG's 2025 Work

The DELEG working group entered 2025 with a central unresolved question: Which of two competing protocol proposals should serve as the foundation for its work? At IETF 122 in Bangkok (March 2025), the working group held an informal poll showing a majority favoring the DELEG proposal (draft-wesplaap-deleg) over the alternative proposal. The session concluded without a formal decision, signaling that further analysis and refinement were needed before the group committed to a direction.

By mid-2025, however, the working group had effectively coalesced around the DELEG proposal, and the specification was adopted as a working group document (draft-ietf-deleg).

A requirements document (draft-ietf-deleg-requirements) progressed through multiple revisions alongside the base specification. The working group also held a virtual interim meeting in June 2025 to work through open issues and met again at IETF 123 in Madrid (July 2025), where document author (and ICANN Board member) David Lawrence presented improvements to the draft. By IETF 123, the specification supported two modes of delegation: "DELEG DIRECT" for cases where the nameserver target is within the delegated domain, and "DELEG INCLUDE" for cases where the target is external.

At IETF 124 in Montreal (November 2025), the working group continued to refine the specification. At this point, two new record types were proposed in the draft, DELEG and DELEGPARAM. In addition, the draft also defined a new EDNS flag bit ("DE") to allow resolvers to signal their DELEG awareness enabling servers to omit traditional NS records in referrals. Open design questions persisted around details like "nameless delegations" (omitting the target name in DELEG DIRECT records) and the reuse of SVCB records as the target for DELEG INCLUDE.

Work on DELEG affects many parts of the DNS protocol. At the IETF 124 meeting, the DELEG and the Domain Name System Operations (DNSOP) working groups agreed that while the main DELEG protocol work would be done in the DELEG WG, the DNSOP WG would coordinate the resource record types that could be used by DELEG and future delegation changes to DNS. To that end, "DNS Protocol Modifications for Delegation Extensions" (draft-arends-dnsop-delext), driven by ICANN Distinguished Technologist Roy Arends, has been adopted as a DNSOP working group document.

In December 2025 and January 2026, various software developers announced initial support for the DELEG protocol, with none stating that they found any significant issues with the specification.

It is worth noting that DELEG is not without its skeptics in the broader DNS community. Some experienced observers have questioned whether the added complexity is justified by the real-world problems it addresses. Nevertheless, the working group has maintained momentum, and the protocol's potential to modernize how the entire DNS delegation chain works makes it one of the most significant DNS standardization efforts underway at the IETF.

5. Working Group: DCONN

The Domain Connect Working Group (DCONN), formally chartered in September 2025 within the Applications and Real-Time Area (ART), is one of the newest working groups at the IETF. ICANN Principal Engineer Andy Newton serves as one of the Area Directors helping lead ART. Before coming to the IETF, a group of DNS operators created the Domain Connect protocol, an open, application-level standard that lets service providers automatically configure the DNS records they need in a customer's zone. The DCONN Working Group's mission is taking the existing Domain Connect protocol and producing a full Standards Track RFC from what has until now been a community-maintained specification.

Domain Connect works by replacing manual DNS record editing with a template-based system. A service provider publishes a template describing the DNS records its product requires, and the customer's DNS provider applies those records after authenticating the domain owner, all through a simple web flow.

For the ICANN community, DCONN matters because it directly addresses one of the persistent barriers to domain name utility: the gap between registering a domain and putting it in production. Registries benefit when domains in their namespaces are actively configured and renewed rather than sitting idle, and registrars benefit when their customers can connect domains to services without filing support tickets about mail exchange (MX) records and canonical name (CNAME) records.

The WG milestone calls for submitting the specification to the Internet Engineering Steering Group (IESG) for Standards Track publication by June 2026.

6. Working Group: PQUIP

The Post-Quantum Use In Protocols Working Group (PQUIP), co-chaired by ICANN Distinguished Technologist Paul Hoffman, was formed in January 2023 to address one of the most consequential long-term challenges facing internet security: preparing the protocols that protect online communications for a future in which quantum computers may be able to break the cryptographic algorithms those protocols currently rely upon.

Today's widely deployed encryption and digital signature schemes, namely RSA, elliptic curve cryptography, and Diffie-Hellman key exchange, are mathematically secure against conventional computers. However, they would be vulnerable to a sufficiently powerful quantum computer running algorithms like Shor's. While experts disagree on when (or whether) quantum computers will exist, the threat is real enough that encrypted data captured today could be stored and decrypted years later once quantum capability arrives, a scenario known as "harvest now, decrypt later."

PQUIP does not itself define new cryptographic algorithms or update existing protocols. That work happens in other IETF working groups like LAMPS, TLS, and IPSECME, while the algorithm selection stems from external bodies like NIST. Instead, PQUIP serves as a coordination and guidance forum. It helps the broader IETF community understand the operational challenges of migrating to post-quantum cryptography. It also documents best practices for hybrid schemes that combine classical and post-quantum algorithms during the

transition period and provides a “venue of last resort” for discussing PQC issues in protocols that lack an active maintenance working group.

The group published RFC 9794, “Terminology for Post-Quantum Traditional Hybrid Schemes”, (June 2025), which standardizes terminology for post-quantum/traditional hybrid schemes. The WG is advancing a “Post-Quantum Cryptography for Engineers” document designed to help implementers understand how this transition differs from past algorithm updates.

For the ICANN community, PQUIP matters because DNSSEC relies on signature algorithms that will eventually need to be replaced with post-quantum alternatives. ICANN’s Office of the CTO has published guidance on this topic. The broader question of how to transition DNSSEC to post-quantum cryptography without breaking the installed base of signers and validators is an active area of research that PQUIP helps coordinate.

7. Working Group: REGEXT

Introduction

The Registration Protocols Extensions working group, commonly known as REGEXT, is the IETF’s home for standards work on the two protocols that underpin domain name registration operations worldwide: the Extensible Provisioning Protocol (EPP) and the Registration Data Access Protocol (RDAP). REGEXT is co-chaired by ICANN Board Member James Galvin.

Evolving EPP

EPP, designated as Internet Standard 69, is the client-server protocol that registries and registrars use to provision and manage domain names, contacts, and hosts.

Since its standardization in 2009, EPP has relied exclusively on TCP with TLS (RFC 5734) as its transport layer. This is a design that predates modern, web-based architectures. Therefore, it can be unfamiliar to some developers and cannot take advantage of tooling geared toward HTTP.

REGEXT is now advancing two companion drafts that define alternative transports while preserving full compatibility with EPP’s existing command set and stateful session model. One draft enables EPP over HTTPS (draft-ietf-regext-epp-https). The other enables EPP over QUIC (draft-ietf-regext-epp-quic). The working group adopted both drafts in early 2025, and they are progressing through review with input from the IETF’s HTTP and QUIC communities on alignment with best practices for application protocol mappings. For registries and registrars, these new transports promise operational flexibility without requiring changes to existing EPP business logic or extensions.

Extending RDAP

REGEXT is also advancing extensions to RDAP. RDAP, designated as Internet Standard 95, is the modern replacement for the legacy WHOIS protocol. It provides structured, machine-readable access to registration data.

The working group most recently adopted a JSContact extension (draft-ietf-regext-rdap-jscontact) which provides an improved, more flexible mechanism for expressing domain contact information.

REGEXT is also working on an extension (draft-ietf-regext-rdap-referrals) that would allow registry RDAP servers to offer lightweight redirects to the sponsoring registrar's RDAP server. This would enable clients to efficiently obtain registration data from the authoritative source, while reducing the load on registry RDAP servers. ICANN Principal Engineers Gavin Brown and Andy Newton are the co-authors of this document.

8. Working Group: RPP

As an outgrowth of the EPP over HTTPS work in the REGEXT Working Group, the IETF has created a RESTful Provisioning Protocol (RPP) Working Group to standardize a new protocol that is more aligned with modern web paradigms, particularly "RESTful" applications programming interfaces (APIs). This new working group is co-chaired by ICANN Principal Engineer Gavin Brown. It held its first meeting at IETF 122 (Bangkok, March 2025).

The working group is not seeking to replace EPP. Both protocols are intended to co-exist in the DNS provisioning environment. Instead, RPP is intended to improve domain provisioning by taking advantage of modern web architecture protocols that EPP cannot use. RPP is based on JSON and fully HTTP-native, which means it can use tools and infrastructure already built for other common RESTful protocols.

The working group is also considering using the JSContact protocol, which would allow for better reuse of software and data storage with RDAP, reducing the risk of inconsistencies in domain registration.

The IETF's work on RPP is important to the ICANN community because it would allow domain provisioning to work like other common APIs. Provisioning could use the same JSON data formats, HTTP conventions, and off-the-shelf tools that developers already know. For registrars, this would mean lower development costs. For registries, it would mean simpler operations and better alignment with modern software development practices.

9. Working Group: DNSOP

Introduction

The DNSOP (DNS Operations) Working Group is one of the longest-running working groups at the IETF. It functions as the Internet community's primary venue to develop and refine the technical standards that govern how the DNS works in practice. Its scope is broad: It includes everything from how resolvers initialize themselves, to how DNSSEC signatures are validated, to how parent and child zones keep their delegation data in sync falls under DNSOP's remit.

For the ICANN community, DNSOP is arguably the single most consequential IETF working group to track, because the protocols and operational practices it produces directly shape what registries, registrars, and DNS operators must implement and support. Changes to DNSSEC algorithm requirements, new mechanisms for automating DS record management between

parent and child zones, updates to how delegation data is validated by resolvers, and guidance on DNS transport and error handling all flow through DNSOP before becoming the standards that underpin the domain name ecosystem ICANN helps coordinate.

During 2025, DNSOP published eight new RFCs and advanced more than a dozen active drafts, several of which have direct operational implications for registry and registrar operations. This report, however, highlights one work item which is critical to ICANN's mission.

Managing DNSSEC Algorithms in the Modern World

DNSSEC constitutes the set of security extensions that lets the DNS prove that the answers it returns are authentic and have not been tampered with in transit. It works by cryptographically signing DNS records, and the entire chain of trust depends on specific cryptographic algorithms being used consistently by everyone involved, including the organizations that sign zones, the software that validates signatures, and the resolvers that protect end users.

Since 2019, the authoritative list of which algorithms are required, recommended, optional, or deprecated for DNSSEC has lived inside a single document, RFC 8624, "Algorithm Implementation Requirements and Usage Guidance for DNSSEC". That means that any time the DNS community had to adjust the status of an algorithm, even in a minor way, it had to go through the full process of revising and republishing that RFC. In a field where cryptographic best practices evolve continuously and aging algorithms can become genuine security liabilities, this is an unwieldy arrangement.

RFC 9904, "DNSSEC Cryptographic Algorithm Recommendation Update Process", (published in November 2025 and co-authored by ICANN Board Member Wes Hardaker and SSAC member Warren Kumari) solves this problem by moving the canonical list of DNSSEC algorithm requirements out of the RFC itself and into an IANA registry. IANA registries are purpose-built tables maintained by the IANA that can be updated through a simpler process than revising an entire RFC. This might sound like a bureaucratic reshuffling; however the practical effect is significant. When a cryptographic algorithm is found to be weak or a new one gains broad support, the community can now update the official guidance more quickly and with less procedural overhead.

The document also lays the groundwork for two companion RFCs, published in December 2025, that formally deprecate SHA-1 and the Russian GOST algorithms from active use in DNSSEC. The deliberate packaging of these three documents as a coordinated set demonstrated the practical value of the approach. The registry mechanism was established and then immediately exercised, delivering both the framework and its first real-world application in a single effort.

The importance of this work goes beyond process improvement. DNSSEC's value as a security mechanism depends substantially on the strength of the cryptographic algorithms it uses. If the community cannot retire compromised algorithms quickly, signed DNS data offers a false sense of security. (In addition, as the prospect of a future with quantum computers moves algorithm agility from a theoretical nicety to an operational imperative, possessing a streamlined mechanism for managing DNSSEC's cryptographic foundations becomes genuinely critical infrastructure work.)

Conclusion

The technical foundations on which the security, stability, and resilience of the Internet's unique identifier system depend are constantly evolving. The work described in Part Two of this report demonstrates this clearly. From modernizing DNS delegation, to preparing for post-quantum cryptography, to streamlining how DNSSEC algorithms are managed, these efforts illustrate both the pace of change and why ICANN's engagement with the IETF is so important.

ICANN's continued investment in the IETF through staff time, meeting participation, and sustained relationship building ensures that the ICANN community has both a voice in shaping these protocols and the knowledge to respond as they change.