Before the
U.S. DEPARTMENT OF HOMELAND SECURITY
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
Washington, D.C. 20528

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements	)))	Docket No. CISA-2022-0010

COMMENTS OF THE INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

The Internet Corporation for Assigned Names and Numbers (ICANN) welcomes this opportunity to respond to the request for comment issued by the Cybersecurity and Infrastructure Security Agency (CISA) on its proposed implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[1]

Introduction and background

ICANN is a California-based, public-benefit organization accountable to a global community of stakeholders. ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems that enable the Internet to work. ICANN's wholly owned affiliate, Public Technical Identifiers (PTI), performs the Internet Assigned Numbers Authority (IANA) functions. These functions include the allocation and assignment of names in the root zone of the Domain Name System (DNS), the coordination of the assignment of Internet protocol parameters and the allocation of Internet numbering resources to Regional Internet Registries, including the American Registry for Internet Numbers (ARIN). Monthly dashboards and performance reports for the IANA functions are available at https://www.iana.org/performance.

PTI is also responsible for various administrative functions associated with the management of the Internet's DNS root zone, including reviewing the appropriateness of changes to the content of the root zone. The root zone represents the top level of the DNS hierarchy and is usually the first resource consulted whenever a device on the Internet needs to find a network location with a domain name. For example, when trying to connect to "www.example.com," the root zone will direct queries to databases for the top-level domains.

[1] Proposed Rule: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Notice), Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, 89 FR 23644, Docket No. CISA-2022-0010 (April 4, 2024).

The root zone is served by a broadly distributed set of servers known as the "root servers." There are 13 root servers operated by 12 independent organizations that have deployed more than 1,300 root server instances across the globe. Each instance is composed of one or more machines, meaning availability of the root zone is spread widely geographically in a way that is resilient to operational challenges. ICANN operates one the 13 root servers, the ICANN Managed Root Server, or L-Root (L.ROOT-SERVERS.NET). Monthly activity and incident reporting for the IMRS are available at https://www.dns.icann.org/imrs/reports/.

ICANN also facilitates the development and implementation of policies related to the coordination and administration of these unique identifier systems to ensure that the Internet remains secure, stable and resilient. The oversight of the IANA functions and the related policy development process take place under ICANN's multistakeholder system of governance.

Multistakeholder governance at ICANN

ICANN is made up of three components: the ICANN community, the ICANN Board of Directors, and the ICANN organization. The ICANN community develops policies and provides advice to the Board; the Board reviews and adopts those policies and oversees the organization's performance; and the ICANN organization implements the policies, performs technical functions, and maintains and enforces agreements with domain name registries and registrars.

The technical aspects of the Internet's unique Identifiers are governed through the ICANN multistakeholder system. Through this system, the ICANN community, which is composed of technical experts, businesses, intellectual property owners, cybersecurity researchers, academics, civil society leaders, governments, and other stakeholders, play important roles in consensus-driven policymaking. These policies are incorporated into ICANN's agreements with generic Top-Level Domain (gTLD) registries and ICANN accredited registrars. ICANN Compliance enforces these policies, ensuring that the ICANN community's consensus-based policies are implemented to support a secure, stable, and resilient Internet.

The efficient management of the DNS and maintenance of the IANA functions by ICANN demonstrate the strength and capability of the multistakeholder system. The DNS has operated without interruption for more than four decades. The multistakeholder system governing these foundational technologies has allowed for the creation and growth of a single, global, interoperable Internet.

The multistakeholder system also allows for the development and implementation of global policies. Global policies enable the Internet to remain a single, unified and interoperable platform. By contrast, regulation by local, national or regional governmental bodies risks fragmenting the Internet and creating conflicting obligations for Internet stakeholders. Regulation by one jurisdiction incentivizes other jurisdictions to intervene with their own policy objectives.

The multistakeholder system at work: Combating DNS abuse

A recent example of how ICANN's multistakeholder system can bring about change that is enforceable across all of ICANN's gTLD registry operators and accredited registrars is how those contracted parties came together to develop enforceable commitments to combat DNS abuse.

ICANN Consensus Policy and contractual requirements govern the practices of gTLD domain name registries and registrars. ICANN org enforces its own agreements and consensus policies that are developed by the ICANN community. In late 2022 ICANN's registrars and gTLD registries came to ICANN to request a negotiation to enhance the obligations related to DNS Abuse in both the Registrar Accreditation Agreement and the Base gTLD Registry Agreement. They sought to level the playing field and ensure ICANN has the right to terminate registrars and registries that don't adequately mitigate DNS Abuse in their platforms. In 2023, ICANN and the contracted parties agreed to new terms and followed the procedures to update the agreements. On 5 April 2024, the terms became legally binding. ICANN began publishing monthly reports on its enforcement of the new DNS abuse obligations shortly after they became effective.[2]

The role of governments at ICANN

Governments influence global policy development at ICANN through the Governmental Advisory Committee (GAC). The GAC constitutes the voice of Governments and Intergovernmental Organizations (IGOs) in ICANN's multistakeholder structure. Created under the ICANN Bylaws, the GAC is an advisory committee to the ICANN Board. The GAC's key role is to provide advice to ICANN on issues of public policy, and especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements. Currently, there are 183 Member governments and 39 Observer organizations in the GAC.

As an active member of the GAC, the U.S. Government (USG) has helped shape ICANN's global policies in multiple areas, including by providing input on the introduction of new gTLDs and International Domain Names (IDNs), registration data policy (governing the collection, use, storage, and sharing of domain name registrants' data) and DNS abuse. ICANN's multistakeholder system enables the USG, working through the GAC, to help shape global cyber incident reporting for ICANN, PTI, RIRs, RSOs, registries and registrars.

[2] *See* https://compliance-reports.icann.org/dnsabuse.html and https://compliance-reports.icann.org/dnsabuse/dashboard/trends-list.html; explanatory blog at https://www.icann.org/en/blogs/details/icann-launches-reports-on-the-enforcement-of-dns-abuse-requirements-28-06-2024-en.

The historical role of the U.S. Government within ICANN

The USG supported the creation of ICANN and the private sector-led approach to Internet governance. Democratic and Republican Administrations have pushed back against efforts by governments and intergovernmental organizations to take over ICANN's role in coordinating the Internet's unique identifier systems.

The USG was the original overseer of ICANN's performance of the IANA functions. In the 1990s, the USG recognized that as the Internet expanded globally, its governance should expand and adapt along with it. It therefore set in motion a process to transition the coordination and management of the Internet's unique identifier systems from USG oversight to the multistakeholder community.

In 2014, the USG asked the global Internet community to develop a framework to transition oversight of IANA. For the transition to be successful, ICANN would need to evolve its multistakeholder system and strengthen its mechanisms to ensure accountability and transparency. Public and private sector organizations, technical experts, and civil society representatives from around the world organized themselves into groups to work on the plan. For more than two years, through more than 600 meetings and conference calls these groups collaborated to create a new, fully global, multistakeholder oversight system.

In March 2016, the proposal was endorsed by all stakeholders, including ICANN's GAC, and taken into consideration by the USG. The plan was designed to prove the multistakeholder approach was a stable, secure, accountable, and transparent mechanism for managing a critical Internet resource.

A key part of the IANA transition to the multistakeholder system was establishing a new non-profit organization, the Public Technical Identifiers (PTI), to be the home of the performance of the IANA functions. PTI is a wholly owned affiliate of ICANN on whose behalf it manages these functions. PTI also provides a mechanism to implement important safeguards for the IANA functions.

Because ICANN and its community were able to enhance their multistakeholder system of governance to meet the transition criteria set by the USG, the oversight role was officially passed on to the global Internet community on 30 September 2016. These enhancements ensured that the USG's previous role will never be replaced with another government-led or intergovernmental organization solution, and that the Internet will remain a platform for innovation, economic growth, and free speech. Without such safeguards in the new governance system, the transition would not have happened.

In January 2017, the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) ended its joint Affirmation of Commitments with ICANN. Seven years later, ICANN remains an independent organization in which policies are developed

through a private-sector led multistakeholder system, implemented by the ICANN organization, and incorporated into ICANN's agreements with gTLD registries and registrars.

The DNS exception

ICANN limits its comments to the Notice's discussion of CIRCIA's DNS exception. Under that exception, CIRCIA's reporting obligations:

> "shall not apply to a covered entity or the functions of a covered entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority."[3]

In the Notice, CISA proposes to interpret the exception to apply to ICANN, ARIN, and affiliates of those entities. CISA additionally proposes to create a limited exception from CIRCIA reporting requirements for Root Server Operators' (RSOs) DNS Root Server function.[4]

ICANN appreciates CISA's recognition of "the long-standing U.S. Government policy goal of support of the multi-stakeholder approach to internet governance" and that it specifically seeks comment as to, "How should the U.S. government's support for the multi-stakeholder system of internet governance inform the DNS Exception?"[5]

ICANN does not take a position on CISA's determination that under U.S. law, these entities meet the criteria for a "covered entity" that, absent the exception, would be subject to CIRCIA's reporting requirements. ICANN appreciates and agrees with CISA's determination that "ICANN, ARIN, any affiliates of ICANN or ARIN (such as PTI), and the RSO function of covered entities" meet the statutory requirements for the DNS Exception.[6]

Conclusion

Congress and the U.S. Administration demonstrated their continued support for ICANN's multistakeholder system of Internet governance by incorporating the DNS exception into CIRCIA. CISA's proposal to codify the exception and apply it to ICANN, PTI, ARIN, and the root server operators' root service function, is consistent with the USG's longstanding support for the multistakeholder system of Internet governance. The successful effort to develop and enforce binding obligations to combat DNS abuse is a model of how ICANN and its stakeholders

---

[3] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), as amended, 6 U.S.C. 681b(a)(5)(C).
[4] Notice, p. 231 (https://public-inspection.federalregister.gov/2024-06526.pdf?source=email; note this is not FR version at https://www.govinfo.gov/content/pkg/FR-2024-04-04/pdf/2024-06526.pdf).
[5] Notice, pp. 236-237, question 48.
[6] Notice, p. 235 and proposed CHAPTER II--DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY PART 226—COVERED CYBER INCIDENT AND RANSOM PAYMENT REPORTING, § 226.4 Exceptions to required reporting on covered cyber incidents and ransom payments, pp. 421-422).

can address other emerging and challenging issues with a globally unified solution that is not bound by any specific jurisdiction. Global policies enable the Internet to remain a single, unified and interoperable platform. CIRCIA's DNS exception, and ICANN's multistakeholder system, implement the vision of the USG and the many other governments which signed the "Declaration for the Future of the Internet": An "open, free, global, interoperable, reliable, and secure Internet."[7]

Respectfully submitted,

Sally Costerton, Interim President and CEO
Internet Corporation For Assigned Names And Numbers (ICANN)

[7] "*A Declaration for the Future of the Internet*," available at https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf.