Internet Corporation for Assigned Names and Numbers (ICANN)

PTI Registry Assignment and Maintenance System

System and Organization Controls Report

Report on ICANN's Assertion on the PTI Registry Assignment and Maintenance System and on the Suitability of the Design and Operating Effectiveness of Controls to Meet the Criteria for Security, Availability and Processing Integrity

Throughout the Period October 1, 2023, to November 30, 2024

I. Independent Service Auditor's Report

Internet Corporation for Assigned Names and Numbers

Scope
We have examined Internet Corporation for Assigned Names and Numbers' (ICANN's) accompanying assertion titled "Assertion of Internet Corporation for Assigned Names and Numbers' Management," (assertion) that the controls within ICANN's Public Technical Identifiers (PTI) Registry Assignment and Maintenance system (system) were effective throughout the period October 1, 2023, to November 30, 2024 to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and processing integrity (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA Trust Services Criteria.

ICANN uses subservice organizations identified in the assertion to provide co-location hosting services and managed services for the production and disaster recovery environments. The assertion indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ICANN, to achieve ICANN's service commitments and system requirements based on the applicable trust services criteria. The assertion presents the types of complementary subservice organization controls assumed in the design of ICANN's controls. The assertion does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities
ICANN is responsible for its service commitments and system requirements and for designing, implementing and operating effective controls within the system to provide reasonable assurance that ICANN's service commitments and system requirements were achieved. ICANN has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ICANN is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities
Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve ICANN's service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ICANN's service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion
In our opinion, management's assertion that the controls within ICANN's PTI Registry Assignment and Maintenance system were effective throughout the period October 1, 2023, to November 30, 2024, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

RSM US LLP

Los Angeles, California
April 30, 2025

I. Assertion of Internet Corporation for Assigned Names and Numbers' Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Internet Corporation for Assigned Names and Numbers' (ICANN) PTI Registry Assignment and Maintenance system (system) throughout the period October 1, 2023, to November 30, 2024, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*, in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2023, to November 30, 2024, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria. ICANN's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

ICANN uses subservice organizations identified in Attachment A. Attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ICANN, to achieve ICANN's service commitments and system requirements based on the applicable trust services criteria.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2023, to November 30, 2024, to provide reasonable assurance that ICANN's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A

Internet Corporation for Assigned Names and Numbers' Description of its PTI Registry Assignment and Maintenance System

Overview of Operations

Background

The Internet is renowned for being worldwide and free from centralized control; however, there is a technical need for some key parts of the Internet to be globally coordinated. This coordination includes the operational aspects of the Internet's unique identifiers. In performing the coordination role, responsibilities include allocating and maintaining unique codes and numbering systems that are used in the technical standards (protocols) that drive the Domain Name System (DNS). These activities can be broadly grouped into three categories, collectively the Internet Assigned Numbers Authority (IANA) Services (IANA Services): domain names, number resources and protocol parameters.

Overview of Services Provided

Public Technical Identifiers Process and Controls Overview

Public Technical Identifiers (PTI) is the ICANN affiliate responsible for performing the IANA Services defined above, which are key functions that keep the Internet interoperable and the DNS running smoothly. PTI's mission statement describes the role of PTI, which includes responsibility for the operational aspects of coordinating the Internet's unique identifiers and maintaining the trust of the community to provide these services in an unbiased, responsible and effective manner. Mainly, PTI is responsible for the operation of the IANA Services, partitioned into these three categories:

- Domain names
- Number resources
- Protocol parameter assignments

PTI does not set policy by which it performs IANA Services. Instead, the various stakeholder communities develop the agreed policies and principles and PTI is then responsible for the implementation of those policies and principles in a neutral and responsible manner. ICANN supports the development of policies for domain name operations and IP addressing with input from the various stakeholders. ICANN has a structure of supporting organizations that contribute to developing the policies ICANN implements, including those related to the IANA Services. The development of Internet protocols that often dictate how protocol parameters should be handled are arrived at within the Internet Engineering Task Force (IETF), the Internet Engineering Steering Group (IESG) and the Internet Architecture Board.

Scope of Report and Boundaries of the System

The scope of this report includes ICANN's PTI Registry Assignment and Maintenance System (RAMS), leveraging the Root Zone Management System (RZMS), Request Tracker (RT) and Git as tools used to perform the IANA Services as they relate to the security, availability and processing integrity trust services criteria.

The boundaries of the RAMS begin as DNS root, IP addresses and IP resources are requested by customers to be registered for use on the Internet. For protocol parameters, names, and numbers, the customer request is logged within the RT or RZMS system, which captures request information and status and sends the customer an automated acknowledgement. Once data enters the RAMS it is processed by IANA staff to meet customer requirements and business rules for specified public registry changes.

The boundaries of the system end when the records or updates requested by the customer are made on the publicly available registries based on the approved requests.

ICANN utilizes CoreSite and Equinix (subservice organizations) for co-location hosting services and managed services. This appendix does not include any of the controls expected to be implemented at the subservice organizations.

ICANN has provided the IANA Services since 1999 and continues to do so today through a series of contracts and subcontracts with its affiliate PTI in existence since 2016. Key control activities identified to meet the Trust Services Criteria include control activities performed by both ICANN and PTI. Activities performed by ICANN include management of IT, support staff and the following activities:

- HR and training
- Risk management
- Policy and procedure establishment and maintenance
- Logical access/security maintenance
- System development and change management
- Computer operations

This description includes the processes and control activities of both ICANN and PTI that are relevant to the RAMS. References in this report to ICANN are inclusive of staff and management including those who work for its affiliate PTI.

Infrastructure and Software

Infrastructure

The following table describes the system software and infrastructure used to support the PTI RAMS:

Application/System	Process/Transactions	Purchased or Developed	Platform and Operating System	Data Environment
RAMS Root Zone Management System (RZMS)	Maintains the contents of the DNS root zone and facilitates customer change requests	Developed	Linux and Kubernetes (MicroK8s)	MariaDB
RAMS Request Tracker (RT)	Ticketing system for email-based customer interactions	Developed	Linux and Kubernetes (OKD)	MariaDB

The physical and hardware components of the RAMS (facilities, equipment and computers) include:

- Web application servers
- Database servers

Physical and hardware components are hosted within third-party data centers.

Software

There are two in-scope applications within the RAMS, including RZMS and RT. ICANN considers any individual user with access to RZMS or RT to be an in-scope user. These systems are used to support the IANA Services related to domain names, number resources and protocol parameters.

- RZMS is a custom-built workflow management system utilized to manage the DNS Root Zone. RZMS also has an external web interface that customers log into with their own username and password to check status and request changes. Although this web interface enables customer tracking of change requests and provides a communication tool to request changes, customers still retain the ability to communicate the same information by other means.

- RT is a general-purpose ticketing system used to track requests for all three categories of the IANA Services. For DNS Root Zone management, RZMS is the workflow system that customers primarily interact with to lodge and authorize root zone change requests. RZMS is closely integrated with RT, and RZMS uses RT to log request history in addition to providing a system to manage correspondence with the requestor and approvals from business owners.

RZMS and RT are hosted on CentOS Linux servers running on VMWare virtual machines and Kubernetes clusters. Web applications are hosted on a mixture of Apache HTTP server and Apache Tomcat servers. These are open-source platforms that are developed in a transparent and participatory manner and released under open-source licenses that allow for the inspection of the source code. The RZMS and RT applications use MariaDB as a relational database backend. The database and application servers are housed in ICANN's secured third-party data centers.

People

ICANN has 449 staff located in 34 countries, has four regional offices, four engagement centers and its headquarters in Los Angeles. Its leadership is composed of 11 executives reporting to ICANN's President and Chief Executive Officer (CEO). Each executive has a senior management team to manage the departments reporting to them. An organization chart is published monthly based on data sourced from Oracle Fusion, the HR system, and is made accessible to staff electronically. The organization chart defines the reporting structure for IANA in-scope users. The staff responsible for the performance of the IANA Services are employed by PTI.

On a semiannual basis, a performance review is performed for staff to evaluate performance of responsibilities, delivery of goals, and behavioral expectations. The evaluations are used to determine at-risk compensation and annual merit compensation increases. Goals relating to organizational and departmental objectives are established prior to each evaluation period. Staff are expected to complete a self-evaluation based on the predefined goals and behaviors. The managers submit the evaluations to the HR department. HR facilitates performance alignment reviews with each function's management team to ensure consistent scoring and to enable broad-based feedback on each individual's performance. Following this, managers have a discussion with each staff member to review their performance and to agree upon goals and expectations for the next evaluation period.

The anonymous hotline is an additional available resource provided to staff to report any work-related concerns regarding ethical, moral or legal conduct. The hotline committee reviews complaint reports after receipt of notice from the hotline service provider and determines an appropriate course of action.

PTI, along with ICANN's E&IT function, is involved in the governance, operation and use of the in-scope systems. The ICANN executive responsible for E&IT is also a member of the organization's information technology steering committee (ITSC), whose role includes the annual review and approval of ICANN's IT-related policies. ICANN has established an organization chart, which identifies, defines and documents the roles, responsibilities and reporting structure within PTI and ICANN E&IT.

Procedures

In an effort to provide an overall direction regarding corporate security, ICANN has developed, documented and implemented a wide array of policies that cover the security, availability and processing integrity of its in-scope systems. These policies address issues such as access management, acceptable use, data classification and infosec guidelines: passphrases. Management maintains a data classification policy that assigns and defines responsibilities for data ownership and users. Relevant policies include:

- Engineering & IT IANA Information Security Policy
- Engineering & IT Acceptable Use Policy
- Engineering & IT Access Management Policy
- Engineering & IT Data Classification Policy
- Engineering & IT Infosec Guidelines: Passphrases
- Engineering & IT Incident Response plan

These policies are reviewed and formally approved by the ITSC on an annual basis and are readily available on ICANN's intranet.

Data

ICANN maintains data classification guidelines that reflect the minimum level of care necessary for ICANN organization data. ICANN classifies its information assets into high, moderate and low risk categories to determine which levels of controls must be utilized to protect data from unauthorized access. The classification levels are defined below:

- Low risk—Data and systems are classified as low risk if the data is intended for public disclosure. or the loss of confidentiality, integrity or availability of the data or system would have no adverse impact on any third party's information or ICANN's mission, finances or reputation.
- Moderate risk—Data and systems are classified as moderate risk if the data is not generally available to the public, or the loss of confidentiality, integrity or availability of the data or system could have an adverse impact on a third party or on ICANN's mission, finances or reputation.
- High risk—Data and systems are classified as high risk if ICANN would be required to report to the community and/or provide notice to individuals if the data is inappropriately accessed, the loss of confidentiality, integrity or availability of the data or system could have a significant adverse impact on third parties or on ICANN's mission, finances or reputation, or protection of the data is required by law/regulation.

Data, as defined by ICANN, constitutes the domain names, number resources and protocol parameter records that are maintained and updated by ICANN for review by the initiator, and includes the following:

- Domain names
  - Operation and maintenance of a number of key aspects of the DNS, including the root zone, and the .int and .arpa top-level domains
- Number resources
  - Allocation of the global pool of IP addresses and autonomous system numbers (ASNs), including making allocations to Regional Internet Registries (RIRs)
- Protocol parameters
  - Maintenance and administration of the IP parameter registries

User input and transactions are processed on function-specific applications servers.

ICANN's data classification guidelines define the minimum-security standards for the acceptance, handling, storage and disposal of data and systems based on the risk classification as defined above.

Subservice Organizations

ICANN uses CoreSite and Equinix (subservice organizations), for co-location hosting services and managed services. The scope of this report does not include the controls and related trust service criteria at the subservice organizations. The following table presents a description of services the subservice organizations provided:

Subservice Organization	Service Provided
CoreSite	Data center co-location and managed services for the production environment
Equinix	Data center co-location and managed services for the disaster recovery environment

Below are the applicable trust service criteria that are impacted by the subservice organization and the controls expected to be implemented at the subservice organization.

Applicable Criteria	Controls Expected to Be Implemented
Common Criterion 6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	• Logical access to servers, databases and backup data is restricted to authorized personnel., and the access is reviewed. • Access to servers, databases and backup data systems is restricted to authorized users and removed upon termination.
Common Criterion 6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	• Logical access to servers, databases and backup data is restricted to authorized personnel, and that access is reviewed periodically. • Access to servers, databases and backup data systems is restricted to authorized users and removed upon termination.
Common Criterion 6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	• Access to the facility hosting production systems is restricted to personnel or visitors authorized by the tenant and reviewed periodically by management for appropriateness. • The ability to administer the badge access control system is restricted to user accounts accessible by authorized staff. • Visitors are required to be escorted by authorized staff while within the co-location facilities. • Badge access privileges are provisioned or revoked according to ICANN requests.
Common Criterion 6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	• Servers and media storing backup data are erased to remove confidential data and destroyed upon retirement.

Applicable Criteria	Controls Expected to Be Implemented
Common Criterion 7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	• Events are reported to clients as needed to assist with resolving security and availability incidents.
Common Criterion 7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate and communicate security incidents, as appropriate.	• Events are reported to clients as needed to assist with resolving security and availability incidents.
Availability Criterion 1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	• Critical components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services. • Hot sites, warm sites and cold sites are maintained for system failover. • Environmental monitoring software is configured to monitor cooling systems, UPS, smoke detectors, sprinklers and fire suppression systems.
Availability Criterion 1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.	• Disaster recovery procedures are documented, reviewed and tested on a periodic basis.

Attachment B

Principal Service Commitments and System Requirements

ICANN designs its processes and procedures related to the RAMS based on the service commitments that ICANN makes to user entities and the operational and compliance requirements that ICANN has established.

Security, availability and processing integrity commitments to user entities are documented and communicated in the IANA Naming Function Contract, Service-Level Agreement (SLA) for IANA Numbering Services, and the ICANN IETF Memorandum of Understanding (IETF MoU) and the annual supplemental agreement thereto. Security, availability and processing integrity commitments include, but are not limited to, the following:

Security Commitments

- ICANN ensures that individuals performing security functions are provided training of appropriate and relevant security and technical topics.
- ICANN maintains a security controls program to meet industry-accepted practices, such as vulnerability testing, disaster recovery, application of patches and usage of appropriate remote access via VPN.

Security Requirements

- Users are subject to ICANN's security policies posted on the ICANN intranet.
- Physical access to servers is restricted to ICANN staff who have been authorized for server access.
- Administrative and staff security measures are implemented to restrict access to systems, programs, data, facilities and other components of the system to authorized and appropriate users.
- System security measures are implemented to secure the transmission of data through encryption and network security measures.
- Security measures with third parties and vendors with whom ICANN shares information are implemented to document, control and mitigate risk associated with the use of third parties.

Availability Commitments

- ICANN provides a stable and secure environment for functions through the implementation of processes and policies.
- ICANN maintains a Disaster Recovery Plan that is reviewed annually.
- PTI maintains a Contingency and Continuity Operation Plan that is reviewed and approved annually.
- To ensure the continuation of the IANA Services in the event of a disaster, ICANN operates at least two redundant data centers in geographically dispersed sites within the United States and uses multiple network providers.
- Public registry data generated as a result of data processing requests will remain available to user entities in the public domain.

Availability Requirements

- ICANN ensures restoration of systems through the use of policies and procedures, including the Disaster Recovery Plan in the event of an emergency.
- ICANN performs regular backups of in-scope systems. Backups are replicated to an off-site data center on a regular, scheduled basis.

Processing Integrity Commitments

- ICANN ensures the authentication, integrity and reliability of the data in performing the IANA Services.
- ICANN communicates requirements to user entities regarding the information, procedures, data or other specifications necessary to complete processing.
- ICANN processes customer requests according to SLAs in the various contracts with key stakeholders such as:
    - Protocol parameter SLAs in the supplemental agreement to the ICANN-IETF MoU
    - IANA Numbering Function SLAs in the SLA for the IANA Numbering Services
    - IANA Naming Function SLAs in the IANA Naming Services Contract and associated IANA SLA table
- ICANN verifies that top-level domain change requests are consistent with the technical and procedural criteria developed by the community.

Processing Integrity Requirements

- Issues reported to ICANN within the application or application data are corrected.
- Input validation measures are in place to ensure data received conforms to the requirements or specifications described in the SLAs or other written information provided to the user entity about deliverable.
- ICANN follows documented processes and refers to standards documentation, global policies and other authorized sources when relevant for processing requests.
- Quality assurance processes are in place to validate the quality, accuracy and completeness within each IANA Services.
- Output validation steps are in place to ensure that output (registry updates) matches the original request.
- Documentation for the IETF includes creation of new public registries, maintenance of public registries, review of documents that appear on IESG telechats, confirmation that the directions in the draft standards are clear and unambiguous, coordination with the Request for Comments Editor in final steps of document publications, and maintenance of the list of Designated Experts.