Project Overview for the PTI SOC2 & SOC3 Audits RFP

Request for Proposal

8 August 2022

1. Introduction

1.1 About this Document

This document provides an overview of the RFP. It aims to provide background and pertinent information regarding the requirements for responding to the RFP. The RFP itself comprises this overview as well as other documents that are hosted in the ICANN Sourcing (SciQuest) tool. Indications of interest are to be received by emailing PTI.SOC2.SOC3.Audits-RFP@icann.org by 23:59 UTC on 26 August 2022.

Complete proposals must be electronically submitted by 23:59 UTC on 20 September 2022 using the ICANN sourcing tool (SciQuest), access to which will be granted after receipt of an indication of interest to the email address above.

1.2 About the Internet Corporation for Assigned Names and Numbers (ICANN)

The ICANN organization is a non-profit public benefit corporation dedicated to preserving the operational security and stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. More specifically, the ICANN org:

1. Coordinates the allocation and assignment of the four sets of unique identifiers for the Internet, which are
    a. Domain names (forming a system referred to as the Domain Name System, or “DNS”)
    b. Internet Protocol (“IP”) addresses
    c. Autonomous System (“AS”) numbers
    d. Protocol port and parameter numbers.
2. Coordinates the operation and evolution of the DNS root name server system.
3. Coordinates policy development reasonably and appropriately related to these technical functions.

See www.icann.org for more information.

1.3 Objective

The Internet Corporation for Assigned Names and Numbers (“ICANN”) is seeking a provider to conduct service organization control audits. These audits represent an important component of the accountability ICANN has to Internet stakeholders for the

proper performance of the Internet Assigned Numbers Authority ("IANA") functions, and are mandated by the various contracts between ICANN and the Internet Engineering Task Force (IETF), the Regional Internet Registries (RIR) and Public Technical Identifiers (PTI).

The objective of this RFP is to select an independent audit firm to examine the security, process integrity and availability of: (1) The controls created as part of the Trust Services Principles and Criteria for the Service Organization Control (SOC) 2 covering ICANN's Registry Assignment and Maintenance Systems (RAMS) and (2) The controls created as part of the Trust Services Principles and Criteria for the Service Organization Control (SOC) 3 covering ICANN's Root Zone DNSSEC Key Signing Key (RZ DNSSEC KSK) System.

In seeking a comprehensive proposal for these services, ICANN is placing maximum emphasis on several key components of value including expertise with similar processes, demonstrated practices, and the ability to work within the guidelines established in this RFP.

1.4 Overview of the IANA functions and the Public Technical Identifiers (PTI), an affiliate of ICANN

The IANA functions are the services by which the top-most level of globally unique identifiers used on the Internet are allocated and managed. These functions, first performed by Dr. Jon Postel in the 1970s, are critical to the Internet today. The efficient, secure, and stable performance of the IANA functions ensures that the Internet's Domain Name System (DNS), Internet numbering, and protocol parameter assignments continue to be globally unique and can support the continued operation and evolution of the global Internet.

Public Technical Identifiers (PTI) is an affiliate of ICANN, and, through contracts and subcontracts with ICANN, began performing the IANA functions on behalf of ICANN in October 2016. PTI is responsible 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.

For more information on the IANA functions, please visit www.iana.org. For more information on PTI please visit https://pti.icann.org/

2. SOC2 and SOC3 Background and Scope

2.1 Period of this Audit

The defined audit periods are October 1, 2022 through September 30, 2023 for the SOC2 and December 1, 2022 through November 30, 2023 for the SOC3. The final report as well as any attachments should be delivered no later than 15 February 2024 for the SOC2 and 30 March 2024 for the SOC3.

2.2 Background

In June of 2010, ICANN held its first Root Zone DNSSEC Key Signing Key (KSK) ceremony to secure the root zone of the DNS. The contract that governed the services at the time called for ICANN to engage a third party to ensure the appropriate internal controls were in place to meet the availability, processing integrity and security objectives for the Root Zone DNSSEC KSK System. For this system, the SOC3 framework was chosen (formerly known as SysTrust) and PricewaterhouseCoopers was selected to conduct the annual audit. The SOC3 reports are public and available on the iana.org website.

In 2013, ICANN expanded its audit of the IANA functions to cover additional systems. ICANN selected the SOC2 audit framework and included key systems used to support the IANA function's transaction processing in its scope. The SOC2 audit framework helps PTI ensure that it has the appropriate internal controls to meet the availability, processing integrity and security objectives for the key systems. These systems are collectively referred to as our Registry Assignment and Maintenance Systems (RAMS), and include the Root Zone Management System and the system used to manage protocol parameter and number allocation requests.

As a result of the IANA stewardship transition in September of 2016, PTI was established as the entity responsible for performing the IANA functions on behalf of ICANN. While new contractual relationships were established, these contracts maintained the need for third-party audits to be conducted. PTI conducted a second Request for Proposal in 2017 and selected RSM US, LLP to perform the SOC2 and SOC3 audits. To follow industry best practices as well as comply with ICANN org's internal policies, the organization is now inviting globally recognized firms to participate in this year's process.

2.3 Scope of Work

Although the AICPA Trust Services Principles and Criteria (TSP) consist of Security, Availability, Processing Integrity, Confidentiality, and Privacy, the last two are not a

necessary part of the PTI SOC2 or SOC3 audits due to the fact that IANA services are public.

The SOC2 focuses on the availability, processing integrity and security of the systems used to perform the IANA functions. These systems are referred to as the Registry Assignment and Maintenance Systems (RAMS) and include the Root Zone Management System (RZMS) and Request Tracker (RT).

These systems allow PTI to manage the DNS root zone by assigning the operators of top-level domains and maintaining their technical and administrative details. They also allow for global coordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic and for maintaining many of the codes and numbers contained in a variety of Internet protocols and registries. The platforms that host the RAMS are managed by ICANN's Engineering & IT department.

The SOC3 audit focuses on the availability, processing integrity and security objectives for the PTI-operated Root Zone DNSSEC Key Signing Key (RZ DNSSEC KSK) System which is used to manage the root zone DNSSEC key life cycle. This includes generating, storing, publishing, and backing up of the Key Signing Key (KSK). The RZ DNSSEC KSK System's operations occur at secure facilities using FIPS 140-2 Level 4 cryptographic hardware security modules (HSMs).

RZ DNSSEC KSK System operations are performed in formal key ceremonies. These key ceremonies usually occur four times per year. In between key ceremonies, components are stored in secure containers within secure facilities in a powered off state. The KSK is generated during key ceremonies, and is used to sign the Zone Signing Key (ZSK) from the Root Zone Maintainer (RZM). Ceremony activities are scripted and filmed for observation and access by the public. Access to the components is limited by physical access controls; there are no logical access controls. Access to key management facilities and activities for key management operations are formally logged.

Trusted Persons, an integral element of the key ceremony, are comprised of respected community members and authorized ICANN staff. Trusted Persons include all employees, contractors, and consultants that control or have access to operations that may materially affect generation and protection of the private component of the RZ DNSSEC KSK, secure export or import of any public components, and zone file data. Trusted roles include, but are not limited to designated system administration personnel, crypto officers, recovery key shareholders, safe security controllers, internal witnesses, and the ceremony administrators.

The work methods are expected to include the following:

- One-on-one interviews with control owners and others relevant to the processes.
- Examination and evaluation of systems, policies, and processes.
- Observation of processes as needed.

- Collaboration with ICANN's internal Audit Manager
- Structured Project Management
- Automation of evidence and sample requests, submission and evaluation

ICANN will supply the controls to be used in conducting the audits, which were developed in collaboration with the control owners and/or subject matter experts. There are currently a total of 78 controls for the SOC2 and 37 controls for the SOC3. These controls include but are not limited to the following areas:

- Human Resource Operations
- Computer Operations
- Change Management
- Process Operations
- Access to Programs and Data
- Project Development
- Information Technology

The final reports will be submitted in the English language. The reports will be submitted to ICANN as an electronic document (PDF).

2.4 Contract Period

The contract term is expected to align with the audit period mentioned above, with the ability to renew for subsequent audit periods.

3. High Level Business Requirements

In order to be considered, the providers must be able to demonstrate ability to meet the following business requirements:

- Must be an Internationally recognized audit firm
- Ability to provide a complete response based on ICANN specifications by the designated due date
- Availability to participate in finalist presentations via conference call/remote participation
- Ability to execute a professional services agreement substantially in accordance with the terms and conditions of ICANN's Contractor Consulting Agreement (Copy attached to RFP)
- Ability to demonstrate well organized work methods and strong project management capabilities through collaborative and automated tools
- Ability to conduct work using remote tools
- Ability to travel to Key Signing Ceremony sites, currently in El Segundo, CA and Culpeper, VA

- Ability to meet the specified timeline for the project
- Ability to provide the deliverables according to the following project timeline (note that deliverables and dates may change due to community work schedules):

	High Level Timeline for SOC2	**Estimated Due Date**
a)	Engagement planning phase (Kick off)	15 April 2023
b)	Engagement execution (Fieldwork)	15 October 2023
c)	Engagement execution (Draft Report)	15 January 2024
d)	Report issued	15 February 2024

	High Level Timeline for SOC3	**Estimated Due Date**
a)	Attend Key Signing Key (KSK) Ceremony 1	February 2023
b)	Review of audit evidence	April 2023
c)	Attend Key Signing Key (KSK) Ceremony 2	May 2023
d)	Review of audit evidence	July 2023
e)	Attend Key Signing Key (KSK) Ceremony 3	August 2023
f)	Review of audit evidence	October 2023
g)	Attend Key Signing Key (KSK) Ceremony 4	November 2023
h)	Review of audit evidence	January 2024
i)	Draft Report	February 2024
j)	Report issued	March 2024

4. High Level Selection Criteria

The decision to select a provider as an outcome of this RFP will be based on, but not limited to, the following selection criteria:

1. Must be an Internationally recognized audit firm
2. Overall capabilities & experience of the firm
    a. Demonstrated experience issuing SOC2 and SOC3 audit reports for non-profit organizations, particularly those with subsidiaries/affiliates
    b. Commitment to assign project team members who meet the qualifications below
3. Professional team assigned
    a. Technical competence and understanding of Internet Protocols, DNSSEC and Cryptographic Key generation and protection methodologies

    b. Demonstrated expertise with the Service Organization Control (SOC) framework
    c. Ability to work productively and effectively with highly technical experts
4. Proposed methodology
    a. Effective communication methods
    b. Structured project management capabilities
    c. Collaborative tools and systems that fit a hybrid working environment
5. Flexibility, including but not limited to:
    a. Ability to adjust to circumstances that could impact the audit period, the engagement timelines and ICANN's control environment
    b. Ability to adapt to different time zones
    c. Responsiveness and flexibility to work with ICANN-specific requirements, agreement terms, etc.
6. Value added services
    a. Team's knowledge of the IANA functions
    b. Experience working with ICANN in an audit or consulting capacity
    c. Proven commitment to Diversity & Inclusion
7. Financial value / pricing
8. Office of Foreign Assets Control clearance
9. Mitigation of any conflicts of interest
10. Reference checks

5. RFP Timeline

The following dates have been established as milestones for this RFP. ICANN reserves the right to modify or change this timeline at any time as necessary.

Activity	Estimated Dates
RFP published	8 August 2022
Participants to indicate interest in submitting RFP proposal	26 August 2022 by 23:59 UTC
Participants submit any questions to ICANN	**2 September 2022 by 23:59 UTC**
ICANN responds to participant questions	12 September 2022
Participant proposals due by	**20 September 2022 by 23:59 UTC**
Preliminary evaluation of responses	21 September - 30 September 2022
Target for participant presentations (finalists)	Week of 10 October 2022
Target for final evaluations	21 October 2022
Contracting and award	Early December 2022

6. Terms and Conditions

General Terms and Conditions

1. Submission of a proposal shall constitute each respondent's acknowledgment and acceptance of all the specifications, requirements and terms and conditions in this RFP.

2. All costs of preparing and submitting its proposal, responding to or providing any other assistance to ICANN in connection with this RFP will be borne by the respondent.

3. All submitted proposals including any supporting materials or documentation will become the property of ICANN. If the respondent's proposal contains any proprietary information that should not be disclosed or used by ICANN other than for the purposes of evaluating the proposal, that information should be marked with appropriate confidentiality markings.

Discrepancies, Omissions and Additional Information

1. Respondent is responsible for examining this RFP and all addenda. Failure to do so will be at the sole risk of the respondent. Should respondent find discrepancies, omissions, unclear or ambiguous intent or meaning, or should any question arise concerning this RFP, respondent must notify ICANN of such findings immediately in writing via e-mail no later than ten (10) days prior to the deadline for bid submissions. Should such matters remain unresolved by ICANN, in writing, prior to respondent's preparation of its proposal, such matters must be addressed in respondent's proposal.

2. ICANN is not responsible for oral statements made by its employees, agents, or representatives concerning this RFP. If respondent requires additional information, respondent must request that the issuer of this RFP furnish such information in writing.

3. A respondent's proposal is presumed to represent its best efforts to respond to the RFP. Any significant inconsistency, if unexplained, raises a fundamental issue of the respondent's understanding of the nature and scope of the work required and of its ability to perform the contract as proposed and may be cause for rejection of the proposal. The burden of proof as to cost credibility rests with the respondent.

4. If necessary, supplemental information to this RFP will be provided to all prospective respondents receiving this RFP. All supplemental information issued by ICANN will form part of this RFP. ICANN is not responsible for any failure by prospective respondents to receive supplemental information.

Assessment and Award

1. ICANN reserves the right, without penalty and at its discretion, to accept or reject any proposal, withdraw this RFP, make no award, to waive or permit the correction of any informality or irregularity and to disregard any non-conforming or conditional proposal.

2. ICANN may request a respondent to provide further information or documentation to support respondent's proposal and its ability to provide the products and/or services contemplated by this RFP.

3. ICANN is not obliged to accept the lowest priced proposal. Price is only one of the determining factors for the successful award.

4. ICANN will assess proposals based on compliant responses to the requirements set out in this RFP, responses to questions related to those requirements, any further issued clarifications (if any) and consideration of any other issues or evidence relevant to the respondent's ability to successfully provide and implement the products and/or services contemplated by this RFP and in the best interests of ICANN.

5. ICANN reserves the right to enter into contractual negotiations and if necessary, modify any terms and conditions of a final contract with the respondent whose proposal offers the best value to ICANN.