Project Overview for the DNSSEC Deployment Metrics Research RFP

Request for Proposal
ICANN Office of the CTO

17 May 2021

1. Introduction

1.1 About this document

The Internet Corporation for Assigned Names and Numbers (ICANN) organization is soliciting proposals to perform a survey of academic and industry literature related to the deployment of the DNS Security Extensions (DNSSEC), to find and document the different techniques and metrics used to measure all aspects of DNSSEC deployment, to make recommendations to ICANN org for which metrics to measure to obtain the most comprehensive view of DNSSEC deployment across the Internet, and to write a comprehensive report detailing the findings.

This document provides an overview of the request for proposal (RFP). It aims to provide background and pertinent information regarding the requirements. The RFP comprises this document as well as others that are hosted in the ICANN sourcing tool (SciQuest/Jaggaer). Indications of interest are to be received by emailing DNSSEC-Deployment-Metrics-Research-RFP@icann.org by 23:56 UTC on 26 May 2021.

Complete proposals must be electronically submitted by 23:59 UTC on 14 June 2021 using the RFP portal. Access will be granted after receipt of an indication of interest to the email address above.

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

The ICANN organization is a non-profit public benefit corporation dedicated to ensuring the stable and secure operation of the Internet's unique identifier systems; 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 organization:

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; and
    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.

2. Background

The Domain Name System (DNS) is a distributed database spanning the entire Internet. Its primary function is mapping domain names used by humans to the IP addresses required by computers and network devices to route Internet traffic to the appropriate destination. For example, if a user enters www.icann.org in a web browser on a phone, the device uses the DNS to learn that the corresponding IP address is 192.0.32.7, allowing the device to send traffic to that destination.

The initial design of the DNS in the 1980s did not include any authentication, so a device looking up DNS information had no way to verify that the answer received was authentic. The DNS protocol engineering community recognized this shortcoming and began efforts to add integrity checking to the DNS, which required significant engineering effort over several years. The result was the DNS Security Extensions, known as DNSSEC. Early versions of the protocol enhancements were not considered operationally viable, but after revisions, the DNSSEC protocol was stable enough by 2008 for widespread deployment to begin.

DNSSEC comes with a cost of administrative complexity and additional processing and network resources. The protocol requires both publishers of DNS data and devices that look up DNS data to make changes. With DNSSEC, DNS data must be cryptographically signed by the owner to generate digital signatures in a process known as signing. DNS clients must be configured to validate the digital signatures over DNS data they retrieve. This process is called validation.

DNSSEC deployment has been slow and this slowness is believed to be the result of the added complexity and resource requirements imposed by DNSSEC compared to the benefits it brings. The DNS root zone and almost all of the top-level domains (TLDs) have been signed, but relatively few zones lower in the DNS hierarchy have been signed. DNSSEC validation, when enabled, almost always occurs on recursive resolvers operated by ISPs and enterprises. At the time of writing, less than a third of DNS responses are being validated.

The ICANN organization supports the deployment of DNSSEC as part of its mission to "ensure the stable and secure operation of the Internet's unique identifier systems".[1] ICANN org has undertaken efforts over the years to promote DNSSEC deployment, such as capacity building for ccTLD operators and training for the community at ICANN meetings and directly via ICANN's Technical Engagement and Global Stakeholder Engagement teams. Determining the effectiveness of these efforts requires tracking metrics representing DNSSEC deployment, but measuring deployment of DNSSEC signing and validation can be difficult. Signed zones can be counted directly when an

[1] https://www.icann.org/resources/pages/governance/bylaws-en/#article1

operator, such as a TLD registry, publishes its zone file, but not all TLDs make their zone data available. Measuring DNSSEC validation directly requires querying individual recursive resolvers, but there are millions of resolvers and not all are publicly accessible. In addition, there may be other metrics beyond signing and validation that would provide valuable insight into DNSSEC deployment.

Based on preliminary research, ICANN believes academic and industry researchers have discovered novel and interesting techniques for measuring DNSSEC deployment both directly and indirectly. ICANN org seeks to discover and document these techniques for the purpose of developing systems to measure and track DNSSEC deployment metrics. These metrics will enable both ICANN org and the community to better understand the pace and scope of DNSSEC deployment.

3. Scope of Work

3.1 Tasks

The work encompasses the following tasks:

1. Perform an extensive survey of academic and industry literature related to the deployment of the DNS Security Extensions (DNSSEC).
2. Find and document the different techniques and metrics used to measure DNSSEC deployment, including signing, validation, and any other relevant activities. Metrics might indicate an absolute value, a rate, or another relevant parameter.
3. Analyze the documented metrics and recommend which metrics ICANN org should measure to gain the most comprehensive insight into the state of DNSSEC deployment.
4. Write a comprehensive report detailing the findings, including a detailed bibliography of all sources consulted.

3.2 Deliverables

The following deliverables are required:

1. A proposed work plan and timeline, to be created first and reviewed by the ICANN org before any other work is performed.
2. A draft report.
3. A final report, resulting from any revisions necessary to the draft report based on feedback from ICANN org.

The expected project duration, from contract award to final report, should not exceed six months.

4. High-Level Selection Criteria

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

1. Capability and experience of key personnel
2. Availability of key personnel
3. Demonstrated understanding of the scope of work, including required deliverables
4. Proposed approach to the work including timeframe for completion
5. Quality of similar prior work
6. Responsiveness and flexibility to work with ICANN-specific requirements, agreement terms, etc.
7. Financial value / pricing
8. Value added services
9. Financial Health
10. Reference checks
11. Mitigation of any conflicts of interest

5. High-Level Business Requirements

A summary of the requirements for a contractor to perform the work is:

1. Provide a complete response based on ICANN specifications by the designated due date.
2. Participate in finalist presentations via conference call/remote participation.
3. Execute a professional services agreement substantially in accordance with the terms and conditions of ICANN's Contractor Consulting Agreement (contact ICANN staff for copy).
4. Possess the subject matter expertise and technical skills required to understand, analyze and write about academic literature related to DNSSEC deployment.
5. Produce all the deliverables listed above in Section 3.2 Deliverables within six months from contract award.
6. Provide monthly status updates via phone/email/meeting, as appropriate. Contractor must be able to accommodate bi-weekly status meetings with key personnel during business hours in Eastern Time Zone.
7. Communicate (verbally and in writing) in English.

6. Project 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 Date
RFP opened	17 May 2021
Participants to indicate interest in submitting RFP proposal	26 May 2021 by 23:59 UTC
Participants submit any questions to ICANN via the Q&A Board	31 May 2021 by 23:59 UTC
ICANN responds to participant questions	8 June 2021
Participant proposals due by	14 June 2021 by 23:59 UTC
Evaluation of responses	Thru July 2021
Vendor contracting and award	Thru August 2021

7. Terms and Conditions

General Terms and Conditions

1. Submission of a proposal shall constitute 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 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 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 email 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.

ICANN.ORG