ICANN Specific Reviews - Second Security, Stability and Resiliency of the DNS Review (SSR2) Recommendation 5.3 - Implementation Documentation

Published on 2 February 2024

SSR2 Final Report
https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

Board resolution on SSR2 Final Report
https://www.icann.org/resources/board-material/resolutions-2021-07-22-en#2.a

- Recommendation submitted: January 2021
- Recommendation approved: July 2021
- Implementation completed: January 2024

See https://community.icann.org/display/SSR/Implementation for more information on SSR2 implementation.

Recommendation 5.3

ICANN org should require external parties that provide services to ICANN org to be compliant with relevant security standards and document their due diligence regarding vendors and service providers.

Board Action on 5.3

The Board notes that to complete this recommendation, ICANN org, when renegotiating its one-year based contracts with external service-provider parties, would need to include a clause on compliance with relevant security standards. The Board notes that ICANN org's Engineering & Information Technology (E&IT) function already requires all appropriate vendors and service providers to have a risk assessment performed and documented by E&IT's Security and Network Engineering Department which meets ICANN' orgs needs as instructed by industry standard practices.

Final Implementation Report

As noted by the Board, ICANN org's Engineering & Information Technology (E&IT) function already requires all appropriate vendors and service providers to have a risk assessment performed and documented by E&IT's Security and Network Engineering Department which meets ICANN org's needs as instructed by industry standard practices.

In addition, in Q3 2023, ICANN org completed the identification of relevant security standards following National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) standards, and reached agreement on language that, starting in 2024, will be included within relevant and applicable contracts with external service-provider parties. The contract term will be reviewed regularly and updated as needed.

The contract term that ICANN will incorporate is:

> *Contractor shall implement, maintain, and abide by, and shall ensure that its employees and subcontractors abide by: (1) any and all relevant laws, industry best practices and standards for information security; (2) all technical, organizational, and physical security policies and measures described in this Agreement or any mutually executed Exhibit hereunder; and (3) ICANN's reasonable request to receive the written results of any relevant self- or third-party audit or certification program that verifies such measures and policies comply with clause (1) and (2) above. The foregoing security practices and standards are material obligations of this Agreement and shall, at a minimum, protect all ICANN data, including confidential and/or sensitive information and Personal Data, from unauthorized access, destruction, use, modification, or disclosure.*
>
> *For purposes of this Agreement, "Personal Data" means any information that relates to an identified or identifiable living individual. The parties agree and warrant that any processing of Personal Data in connection with the Services has been and will be carried out in accordance with Data Protection Laws applicable to their respective processing of personal data. "Data Protection Laws" means any applicable law or regulation from time to time concerning data protection and cybersecurity that governs the processing of Personal Data under this Agreement. Furthermore, each party will provide such cooperation as reasonably required by the other party, upon request, in relation to: a) any request, complaint or query from any data subject in relation to Personal Data; and/or; b) any inquiry, investigation or request made by, or reporting obligations to, a supervisory authority, or any other authority in relation to Personal Data processed in connection with the Services. In the event the parties enter into a Data Processing Agreement ("DPA"), this clause shall not affect the validity or enforceability of this DPA. In the event of a conflict between the DPA and this clause, the DPA shall prevail, but only to the extent of such conflict.*

The development and integration of this contract term completes the implementation of the recommendation, including the relevant contracts that will be renegotiated to include this obligation.

Rationale

Per industry standard practices and ICANN Engineering and IT Security and Network Engineering department, inclusion of a contract term in all relevant and applicable contracts between ICANN and external service-provider parties is required. Recommendation 5.3 has been implemented with the inclusion of the new language which will be incorporated in all relevant contracts, where applicable.

Timeline

Expected implementation date: Q1 2024
Final implementation date: Q1 2024

Milestones

July - September 2023 - Identification of list of security standards following NIST CSF standards.
October - December 2023 - Agreement on draft contractual language to be included in contract renewals.
January 2024 - Integration of contract term to all new contracts and renewals (where applicable).