Strawman

ICANN SSR

This work stream relates to Bylaw 4.6(c) (ii) A, 4.6(c) (ii) B as well as 4.6(c) (iii) and focused on three key areas: 1. security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers; 2. conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers.; and 3. completeness and effectiveness of ICANNs internal security processes and the effectiveness of the ICANN security framework.

Methodology Statement

For reviewing the completeness and effectiveness of ICANNs internal security processes and the effectiveness of the ICANN security framework related to the Internet's system of unique identifiers, the Review Team considered ICANN's organizational security management, risk management and business continuity management process implementations.

The Review Team identified the following key areas of focus and investigated these areas specifically:

- ICANN's Security Framework and emerging threats
- ICANN's Risk Management Framework
- ICANN's Business Continuity strategies, objectives, plans and procedures
- ICANN's operational planning and controls, and prioritized activity recovery strategy
- ICANN's Incident Response Structure
- ICANN's root server operations
- ICANN's Global Domains Division activities that relate to SSR objectives, including:
- New gTLD program SSR-related safeguards
    - Emergency Back-End Registry Operator (EBERO), and related processes, and testing
    - Registry Data Escrow (RyDE) program and Data Escrow Agents (DEA)
    - Centralized Zone Data Service (CZDS) compliance, failures, plans
    - Vetting of registrar and registry operators as relates to SSR, and measurement & impact of malicious conduct by contracted parties, databreaches, etc.
    - SLA Monitoring System (SLAM)
    - Abuse reports, including SADAG and DAAR (Statistical Analysis of DNS Abuse & Domain Abuse Activity Reporting)
    - SSR objectives in ICANN'S standard operating procedures (SOP).

The Review Team recognized that this work stream was dependent on themes from the other dependent areas. More specifically, in addition to the key areas listed above, other challenges under the work stream as related to DNS SSR and Future Threats may be identified.

The steps undertaken to affirm the findings and develop recommendations for consideration of ICANN included:

- Review, analyze and summarize relevant documentation and consult with other work streams to track progress and identification of similar topics

- Conduct relevant interviews and especially with ICANN staff subject matter experts to discuss a range of issues relating to the completeness and effectiveness of ICANN's security processes and the effectiveness of the ICANN security framework.
- Draft summary of key findings.

Chronology for the topics of focus

In May 2017, the sub teams and topics were identified and went through several rounds of review and validation. In September 2017, the work stream ICANN SSR was restructured and categorized in seven different sub-topics. In October 2017, the sub team had a very productive two-day, fact-finding meeting with a number of ICANN staff subject matter experts at ICANN's headquarter in Los Angeles where the team member reviewed, submitted questions & information requests about, and discussed early observations about the referenced topics above. Post-pause, the summary of the work to date and next steps were identified and included in the subgroup work summaries in August 2018.