Workstream #2 - ICANN SSR

Mandate: The group will be responsible for reviewing the completeness and effectiveness of ICANNs internal security processes and the effectiveness of the ICANN security framework.

Workplan: The work plan for this workstream is incorporated into the SSR2 Review Team work plan. View the SSR2 Review Team work plan to see the key areas for research and discussion and related milestones to be achieved during the review process.

Workstream task management (Trello): https://trello.com/b/5Eu1ppuv/ssr2-subtopic-2-icann-ssr

Workstream Documents - available here.

The information below is archived:

Members:

- **Boban Krsic - Rapporteur**
- Denise Michel
- Eric Osterweil
- Kerry-Ann Barrett
- Noorul Ameen
- Norm Ritchie
- Žarko Keci

Mandate: The group will be responsible for reviewing the completeness and effectiveness of ICANNs internal security processes and the effectiveness of the ICANN security framework.

Email Archives - HERE

Conference calls: https://community.icann.org/display/SSR/Subgroup+Conference+Calls

Background Materials:

- SAC097: SSAC Advisory Regarding the Centralized Zone Data Service (CZDS) and Registry Operator Monthly Activity Reports (12 June 2017)
- ICANN SSR Implementation Briefing Materials

Subgroup Documents

Date	Document *(Versions in Red are latest)*	File
19 Jan 2019	ICANN SSR Questions & Answers	Excel
12 Dec 2018	Preamble for team review	Google Doc
10 Oct 2017	Draft Report - ICANN SSR Subgroup - Meeting in LA	Google Doc
10 Aug 2017	LA Meeting - Day 2 notes	Google Doc
27 Aug 2017	ICANN SSR Subtopic activities	Google doc
22 Aug 2017	Draft Audit Plan: ICANN SSR Workshop 9-10 October	Google doc
14 Aug 2017	SS2 Work Plan (including Subgroup Work Plans)	Wiki page
04 Jun 2017	ICANN Security Subtopic: Work Plan Draft	Google doc

Meeting Summary (9-10 October 2017)

The ICANN SSR Subgroup had a very productive two-day, fact-finding meeting at ICANN headquarters in Los Angeles. The subgroup met with a number of ICANN staff subject matter experts and discussed a range of issues relating to the completeness and effectiveness of ICANN's security processes and the effectiveness of the ICANN security framework (including activities connected to the SSR2 Terms of Reference and implementation of SSR1 recommendations). Topics were covered to varying degrees of detail as warranted; some topics were covered sufficiently and some will require follow-on discussions.

The subgroup reviewed, submitted questions & information requests about, and discussed early observations about:

- 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).

Decisions

This section is under maintenance

Date	Decision
26 Jun 2017	Rapporteur: Boban Krsic