EN

AL-ALAC-ST-0421-01-00-EN
ORIGINAL: English
DATE: 12 April 2021
STATUS: Ratified

AT-LARGE ADVISORY COMMITTEE

ALAC Statement on the Second Security, Stability and Resiliency (SSR2) Review Team Final Report

Introduction

On 10 February 2021, Public Comment opened for the Second Security, Stability and Resiliency (SSR2) Review Team Final Report. On the same day, an At-Large workspace was created for the statement. The At-Large Consolidated Policy Working Group (CPWG), decided it would be in the interest of end users to develop an ALAC statement on the Public Comment. Greg Shatan, ALAC Member of the North American Regional At-Large Organization (NARALO), and Alejandro Pisanty, former member of the SSR1, volunteered to draft the ALAC statement.

On 02 March 2021, Alejandro Pisanty drafted an initial ALAC statement, which was posted to its workspace by ICANN Policy staff in support of the At-Large community. Greg Shatan and Alejandro Pisanty further developed the ALAC statement before presenting to the CPWG.

On 31 March 2021, Greg Shatan presented to the CPWG the draft ALAC statement, generally in support of the SSR2 Final Report. The CPWG provided input on the At-Large points of consensus, and ICANN Policy staff in support of the At-Large community circulated the statement on the CPWG mailing list and posted it to its workspace. A final call for comments was issued to the CPWG and ALAC mailing lists after the CPWG meeting.

On 8 April 2021, the drafting team members finalized the ALAC statement. The ALAC Chair, Maureen Hilyard, requested that the statement be ratified by the ALAC before submission to ICANN Public Comment. ICANN Policy staff in support of the At-Large community requested an extension for submission of the ALAC statement.

On 12 April 2021, staff confirmed the online vote resulted in the ALAC endorsing the statement with 14 votes in favor, 0 votes against, and 0 abstentions. Please note 93.33% (14) of the 15 ALAC Members participated in the poll. The ALAC Members who participated in the poll are (alphabetical order by first name): Abdulkarim Oloyede, Carlos Raul Gutierrez, Dave Kissoondoyal, Gregory Shatan, Holly Raiche, Joanna Kulesza, Jonathan Zuck, Justine Chew, Marita Moll, Matthias Hudobnik, Maureen Hilyard, Sarah Kiden, Sindy Obed, and Sylvia Herlein Leite. One ALAC Member, Pari Esfandiari, did not participate in the poll. You may view the result independently under: https://www.bigpulse.com/pollresults?code=1341856SVrV7XeKwUkym2sDngbT

AT-LARGE ADVISORY COMMITTEE

ALAC Statement on the Second Security, Stability and Resiliency (SSR2) Review Team Final Report

The At-Large Advisory Committee (ALAC), on behalf of the At-Large Community, thanks the Second Security, Stability and Resiliency (SSR2) Review Team for its significant efforts resulting in the SSR2 Review Team Final Report. The Final Report consists of a series of well-considered recommendations that would improve ICANN's fidelity to the core principles of security, stability and resiliency that lie at the heart of ICANN's mission. SSR2 builds on the work of the first SSR-RT (SSR1) and the ALAC is pleased to observe that the SSR2 has ratified most of the work of the SSR1. Please note that one of the drafting team members of this ALAC statement, Alejandro Pisanty, was also a member of the SSR1.

The ALAC takes specific note that the SSR2 reached full consensus on each recommendation. This underscores both the importance and broad support for these recommendations. We are pleased to state our support for or lack of objects to each of the recommendations in the SSR2 Final Report. Our comments below are intended to highlight recommendations and other elements of particular importance or relevance, to help guide ICANN in adopting and implementing the Final Report.

The ALAC agrees with the adoption of SMART (Specific, Measurable, Assignable, Relevant and Trackable) criteria and objectives, and with the SSR2's observation that SMART criteria should be used by both the SSR1 implementation team and by future SSR Review Teams. We observe with interest that the SSR2 team met the same difficulty as SSR1 in prioritizing recommendations. We attribute this to the multiple views both reports provide. The SSR2 team invested great effort and time in finding the right level of aggregation for their analysis and report, which (as the SSR1 team found) could neither be a narrowly focused but in-depth security audit, nor an overbroad and superficial collection of observations.

Some significant developments impacting ICANN in the time between SSR1 and SSR2 have been:

- DNS abuse
- The introduction of GDPR
- Evolution of ICANN after changes in its contractual relationships with the United States government (IANA transition)
- Significant mood changes in the Internet environment
- Additional geopolitical shifts
- A global health crisis

While this has been an extremely eventful period, there is no reason to believe the next 5+ years will be significantly less eventful. ICANN must always prepare for new events, or else it risks being overtaken by them. The SSR2 Final Report shows the way for ICANN to continuously improve its position with regard to internal and external factors that impact Internet security, stability and resiliency.

It is useful to divide the focus, and ultimately the implementation, of the report into three areas. The tools required for each area are different:

- ICANN: What ICANN does or manages (primarily,ICANN as an operating entity (ICANN org) and, to a lesser extent, the SO/ACs and the Board)
- The ICANN "Ecosystem": What ICANN influences or oversees (contracted parties and participants in ICANN policy processes, especially PDPs)
- The Rest of the World: Everything beyond the first two areas.

In the first area (ICANN itself), the ALAC notes an important theme that runs through most, if not all, recommendations: ICANN must strive to adopt industry standard and state-of-the-art practices for technical and technology-driven organizations. While ICANN is relatively small in size, it is a critical actor in global Internet security and thus in information security (InfoSec) more broadly. We recognize that ICANN has significantly professionalized its operations over the years, but more needs to be done to keep pace in a relentlessly evolving world.

In particular, the ALAC applauds **Recommendation 2** for the creation of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) position, recommending that it take into account the best people, work, practices, and experience, including those who have already demonstrated foresight and are proactive in their work. This is, if anything, long overdue.

In addition, the ALAC wishes to highlight its strong support for following recommendations:

- **Recommendation 4**, improving risk management. Risk Management has become a core concern and core organizational goal for organizations of all sizes. Creating a centralized risk management function and adopting a recognized risk management standard (ISO 31000) would bring ICANN into alignment with best practices, both in technology-centric organizations and beyond. However, ICANN needs to recognize the unique risks and risk management challenges that ICANN faces due to its unique mandate and structure, in particular its policy development processes. ICANN's risk management structure must ensure that all risks are considered, including community participation that is balanced in order to avoid risks of capture, disproportionate influence by parties with less at stake and/or the ability to stagnate processes. This is intertwined with **Recommendation 5**, recommending adoption of industry security and security auditing standards such as ISO 27000 and SSAE-18, and concomitant training and employee standards for relevant positions.

- **Recommendation 6**, on vulnerability disclosures, recommending the highest possible level of interaction with the broader ecosystem. Vulnerability disclosures are sensitive and subject to different norms of practice in different communities, among which are software, service providers, specialists, bounty hunters, and many others. Establishing trust takes time and effort which should be expended constantly. In the end, the goal is the same - to promote the implementation of and (voluntary) adherence to standards for vulnerability reporting, by the contracted parties and by ICANN itself.

- **Recommendation 7**, the adoption of business continuity and disaster recovery policies, plans and procedures, should be read in conjunction with Recommendations 2 and 5, discussed above. All of these recommendations (and others) support the overarching theme of bringing ICANN into alignment with InfoSec and operational security standards prevalent in technology-centric organizations worldwide. Practices such as these have moved from "nice to have" to "must have" over the last several years; over the next several years, they will move to "negligent to do without."

- **Recommendation 8**, representation of the "public interest" in negotiations with contracted parties, is a recommendation of particular importance to the ALAC and the At-Large Community, which in many ways represents the public interest in the broadest sense within the ICANN structure. Independent abuse and security experts must have a voice in how these issues are represented in ICANN's contracts. In addition, end users, who are often most affected (even if not always first affected) by abuse and security incidents need a voice as well. In each case, these

additional “seats at the table” must not be construed in ways that reduce efficiency, either in contract negotiations and adoption, or in performance..

- **Recommendation 9**, monitoring and enforcing contractual compliance, is critical, particularly in connection with Recommendation 8. A contract without compliance is only words on a page, with little or no value except as “contractual theatre.” This must be seen as a core SSR concern and not merely a legal one.

- **Recommendation 10** echoes one of the ALAC’s current major topics -- the proper definition of DNS abuse. ICANN needs to take the lead in this area, rather than ceding this critical standard-setting activity to the contracted parties, no matter how well meaning they may be. If ICANN is to support the full implementation of the multistakeholder model, it must ensure that the full panoply of stakeholders are engaged and it must facilitate such engagement. However, **Recommendation 10.2** should include a voice for end-users directly and not merely indirectly via consumer protection stakeholders. While end-users are in many cases consumers, they are much more than that. **Recommendation 13** is a necessary companion to this Recommendation 10.

- **Recommendation 12** on DNS abuse transparency, cautioning against implications which arise from the ongoing, complex relationship between GDPR and WHOIS/RDS; avoiding the paradoxical effect of “personal data” being protected while users and their assets are not.

- **Recommendations 14 and 15** are aligned with another oft-stated concern of the ALAC -- that ICANN must actively define and promote metrics for actions and inactions in the DNS, including those of contracted parties. ALAC also notes that this is another necessary element of the suite of recommendations dealing with DNS abuse. **Recommendation 22** is aligned with this concern as well.

- **Recommendation 16** on privacy and RDS, with the above caveat related to Recommendation 12 in mind.

The ALAC agrees emphatically with:

- **Recommendation 17**, on the avoidance of name collisions, which is particularly important for a diverse, global user base. During the 2012 New gTLD round, ICANN was somewhat taken by surprise with regard to name collisions and cannot afford for that to happen again.

- **Recommendation 18**, informing policy debate, for which increased engagement, attendance to meetings, and mutual participation are recommended, with organizations such as the IETF, IEEE, ACM, ISOC, and many other national and regional bodies, including universities and research centers. ICANN needs to take an active role in bringing information into the policy debates from the I* and other organizations relevant to the work of ICANN

Finally, we support **Recommendation 20** on the key rollover, recommending further that the experience gained from the COVID-19 pandemic be carefully considered.

The ALAC recommends that geopolitical and similar risks, including consumer and citizen sentiment in different jurisdictions, be given a stronger consideration with the implication of maintaining a constant, high level of short, medium and long term situational awareness with as many relevant parties as possible.

As noted before, regarding the recommendations not specifically mentioned here, the ALAC supports them “as is”, with no further comment.

In closing, the ALAC once again thanks the SSR2 Review Team for an important and highly relevant report, while noting with caution that *implementation* of the report is the most critical element of all, and one that is outside the remit of SSR2. The ALAC looks to ICANN org to make this Final Report (and the SSR1 Report) a reality with regard to each recommendation.