The Messaging, Malware, and Mobile Anti Abuse Working Group (M3AAWG) welcomes the opportunity to review and submit comments on the final report from ICANN's Second Security Stability and Resiliency Review Team (SSR2 RT) to the ICANN Board.

As we previously noted in our comments on March 17, 2020, to the draft report (https://www.m3aawg.org/documents/en/m3aawg-response-for-icann-security-stability-and-resiliency-review-team-two), the SSR2 RT has done an admirable job of incorporating prior review and consultation into its report. We also note the considerable effort that went into addressing the public comments on the draft report.

Consideration:

We congratulate the team for taking on the difficult and contentious task of identifying persistent or systemic issues that expose the domain name registration and name resolution services to misuse or criminal abuse. We concur with the SSR2 RT assertion that systemic DNS abuse needs to be tackled.

We continue to encourage the ICANN organization and community to take seriously the recommendations from the SSR2 report, and support the RT's position that implementing these recommendations is urgent, particularly when it comes to the issue of DNS abuse.

M3AAWG Recommendation:

M3AAWG recommends that the ICANN Board direct the organization and engages with the community to address the continuing harm created by DNS abuse. Due to its public interest commitments, ICANN should provide a plan to adopt clear indicators, measurements or other transparency and accountability mechanisms as quickly as possible.

Specific Comments

SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures

SSR2 Recommendation Text:

7.1 ICANN org should establish a Business Continuity Plan for all the systems owned by or under the ICANN org purview, based on ISO 22301 "Business Continuity Management," identifying acceptable BC and DR timelines.

7.2 ICANN org should ensure that the DR plan for Public Technical Identifiers (PTI) operations (i.e., IANA functions) includes all relevant systems that contribute to the security and stability of the DNS and also includes Root Zone Management and is in line with ISO 27031. ICANN org should develop this plan in close cooperation with the Root Server System Advisory Committee (RSSAC) and the Root Server Operators (RSO).

7.3 ICANN org should also establish a DR plan for all the systems owned by or under the ICANN org purview, again in line with ISO 27031.

7.4 ICANN org should establish a new site for DR for all the systems owned by or under the ICANN org purview with the goal of replacing either the Los Angeles or Culpeper sites or adding a permanent third site. ICANN org should locate this site outside of the North American region and any United States territories. If ICANN org chooses to replace one of the existing sites, whichever site ICANN org replaces should not be closed until the organization has verified that the new site is fully operational and capable of handling DR of these systems for ICANN org.

7.5 ICANN org should publish a summary of their overall BC and DR plans and procedures. Doing so would improve transparency and trustworthiness beyond addressing ICANN org's strategic goals and objectives. ICANN org should engage an external auditor to verify compliance with these BC and DR plans.

Consideration:

ICANN's current lack of a Business Continuity and Disaster Recovery Plan is alarming and creating one should be a priority.

M3AAWG Recommendation:

We concur with the SSR2 RT that the creation of a strategic, executive security position within the ICANN organization is useful, and agree with the RT that ICANN should pursue best-practice approaches for risk management, information security management, business continuity and disaster recovery.

SSR2 Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties

SSR2 Recommendation Text:

8.1 ICANN org should commission a negotiating team that includes abuse and security experts not affiliated with or paid by contracted parties to represent the interests of non-contracted entities and work with ICANN org to renegotiate contracted party contracts in good faith, with public transparency, and with the objective of improving the SSR of the DNS for end-users, businesses, and governments.

Consideration:

ICANN has not fostered a contract negotiations process that is transparent, or open to participation from all affected ICANN constituencies.

M3AAWG Recommendation:

We fully support the commissioning of a negotiating team to renegotiate contracted party contracts as described in SSR2 Recommendation 8 with the objective of improving the SSR of the DNS for end-users, businesses, and governments.

SSR2 Recommendation 9: Monitor and Enforce Compliance

SSR2 Recommendation Text:

9.1 The ICANN Board should direct the compliance team to monitor and strictly enforce the compliance of contracted parties to current and future SSR and abuse-related obligations in contracts, baseline agreements, temporary specifications, and community policies.

9.2 ICANN org should proactively monitor and enforce registry and registrar contractual obligations to improve the accuracy of registration data. This monitoring and enforcement should include the validation of address fields and conducting periodic audits of the accuracy of registration data. ICANN org should focus their enforcement efforts on those registrars and registries that have been the subject of over 50 complaints or reports per year regarding their inclusion of inaccurate data to ICANN org.

9.3 ICANN org should have compliance activities audited externally at least annually and publish the audit reports and ICANN org response to audit recommendations, including implementation plans.

9.4 ICANN org should task the compliance function with publishing regular reports that enumerate tools they are missing that would help them support ICANN org as a whole to effectively use contractual levers to address security threats in the DNS, including measures that would require changes to the contracts.

Consideration:

As noted last year, M3AAWG member experience when dealing with ICANN Compliance continues to be unproductive. This is in part because ICANN's contracts provide few enforceable clauses related to mitigating abuse.

M3AAWG Recommendation:

We continue to concur with the SSR2 RT regarding ICANN's failure to request, enumerate, or to negotiate for enforcement tools, and therefore support all aspects of SSR2 Recommendation 9.

SSR2 Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms

SSR2 Recommendation Text:

10.1 ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology—e.g., security threat, malicious conduct— ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication.

10.2 Establish a staff-supported, cross-community working group (CCWG) to establish a process for evolving the definitions of prohibited DNS abuse, at least once every two years, on a predictable schedule (e.g., every other January), that will not

take more than 30 business days to complete. This group should involve stakeholders from consumer protection, operational cybersecurity, academic or independent cybersecurity research, law enforcement, and e-commerce.

10.3 Both the ICANN Board and ICANN org should use the consensus definitions consistently in public documents, contracts, review team implementation plans, and other activities, and have such uses reference this web page.

M3AAWG Recommendation:

We would welcome clarification of key terms and definitions around the issue of DNS abuse as used at and by ICANN, and therefore support all aspects of SSR2 Recommendation 10.

SR2 Recommendation 11: Resolve CZDS Data Access Problems

SSR2 Recommendation Text:

11.1 The ICANN community and ICANN org should take steps to ensure that access to Centralized Zone Data Service (CZDS) data is available, in a timely manner and without unnecessary hurdles to requesters, e.g., lack of auto-renewal of access credentials.

Consideration:

We concur that access to the CZDS remains problematic, particularly for researchers who use CZDS data longitudinally. This is evidenced by a large number of complaints and anecdotal evidence of issues with renewing credentials/access.

M3AAWG Recommendation:

We concur with the SSR2 RT and support measures are taken to ensure access to-Centralized Zone Data Service (CZDS) data is available, in a timely manner and without unnecessary hurdles to requesters.

SSR2 Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review

SSR2 Recommendation Text:

12.3 ICANN org should publish reports that identify registries and registrars whose domains most contribute to abuse. ICANN org should include machine-readable formats of the data, in addition to the graphical data in current reports.

12.4 ICANN org should collate and publish reports of the actions that registries and registrars have taken, both voluntary and in response to legal obligations, to respond to complaints of illegal and/or malicious conduct based on applicable laws in connection with the use of the DNS.

Consideration:

A small number of registrars is responsible for an outsized percentage of abusive registrations. In the interests of transparency, ICANN should publish data on this important aspect.

M3AAWG Recommendation:

M3AAWG concurs with the SSR2 RT and recommends the publication of registry and registrar abuse statistics in DAAR reports.

SSR2 Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting

SSR2 Recommendation Text:

13.1 ICANN org should establish and maintain a central DNS abuse complaint portal that automatically directs all abuse reports to relevant parties. The system would purely act as an inflow, with ICANN org collecting and processing only summary and metadata, including timestamps and types of complaint (categorical). Use of the system should become mandatory for all generic top-level domains (gTLDs); the participation of each country code top-level domain (ccTLD) would be voluntary. In addition, ICANN org should share abuse reports (e.g., via email) with all ccTLDs.

13.2 ICANN org should publish the number of complaints made in a form that allows independent third parties to analyze the types of complaints on the DNS.

Consideration:

Our members on either end of the process are affected by issues with the current abuse reporting approach. Contracted parties receive large volumes of misdirected abuse reports, while complainants report that reactions, time lines, and responses are inconsistent. By providing a centralized system, the former can be reduced, while the latter could be made more transparent.

M3AAWG Recommendation:

M3AAWG welcomes the proposed streamlining of abuse complaint processes as outlined in SSR2 Recommendation 13.

SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements

SSR2 Recommendation Text:

14.1 ICANN org should create a Temporary Specification that requires all contracted parties to keep the percentage of domains identified by the revised DNS Abuse Reporting (see SSR2 Recommendation 13.1) activity as abusive below a reasonable and published threshold.

14.2 To enable anti-abuse action, ICANN org should provide contracted parties with lists of domains in their portfolios identified as abusive, in accordance with SSR2 Recommendation 12.2 regarding independent review of data and methods for blocklisting domains.

14.3 Should the number of domains linked to abusive activity reach the published threshold described in SSR2 Recommendation 14.1, ICANN org should investigate

to confirm the veracity of the data and analysis, and then issue a notice to the relevant party.

14.4 ICANN org should provide contracted parties 30 days to reduce the fraction of abusive domains below the threshold or to demonstrate that ICANN org's conclusions or data are flawed. Should a contracted party fail to rectify for 60 days, ICANN Contractual Compliance should move to the de-accreditation process.

14.5 ICANN org should consider offering financial incentives: contracted parties with portfolios with less than a specific percentage of abusive domain names should receive a fee reduction on chargeable transactions up to an appropriate threshold.

Consideration:

ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. As noted previously, a small number of actors is associated with the majority of security-related registrations. Defining clear policies would lead to a clearer playing field where all relevant actors are aware of, and can pursue the same objectives. While a temporary specification is not ideal, it is an appropriate stop-gap measure.

M3AAWG Recommendation:

M3AAWG concurs that ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes.

SSR2 Recommendation 15: Launch an EPDP for Evidence-based Security Improvements

SSR2 Recommendation Text:

15.1 After creating the Temporary Specification (see SSR2 Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements), ICANN org should establish a staff-supported Expedited Policy Development Process (EPDP) to create an anti-abuse policy. The EPDP volunteers should represent the ICANN community, using the numbers and distribution from the Temporary Specification for gTLD Registration Data EPDP team charter as a template.

15.2 The EPDP should draw from the definition groundwork of the CCWG proposed in SSR2 Recommendation 10.2. This policy framework should define appropriate countermeasures and remediation actions for different types of abuse, time-frames for contracted party actions like abuse report/response report timelines, and ICANN Contractual Compliance enforcement actions in case of policy violations. ICANN org should insist on the power to terminate contracts in the case of a pattern and practice of harboring abuse by any contracted party. The outcome should include a mechanism to update benchmarks and contractual obligations related to abuse every two years, using a process that will not take more than 45 business days.

Consideration:

ICANN policy needs to be created around the issue of DNS abuse, clarifying expectations, requirements, and processes. As noted previously, a small number of actors are associated with the majority of security-related registrations. Defining clear policies would lead to a clearer playing field where all relevant actors are aware of, and can pursue the same objectives. An established consensus policy would be most useful for achieving this end.

M3AAWG Recommendation:

M3AAWG concurs with the SSR2 RT and recommends launching an Expedited Policy Development Process to create an anti-abuse policy.

SSR2 Recommendation 18: Informing Policy Debates

SSR2 Recommendation Text:

18.1 ICANN org should track developments in the peer-reviewed research community, focusing on networking and security research conferences, including at least ACM CCS, ACM Internet Measurement Conference, Usenix Security, CCR, SIGCOMM, IEEE Symposium on Security and Privacy, as well as the operational security conferences and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior.

18.2 ICANN org should ensure that these reports include relevant observations that may pertain to recommendations for actions, including changes to contracts with registries and registrars, that could mitigate, prevent, or remedy SSR harms to consumers and infrastructure identified in the peer-reviewed literature.

18.3 ICANN org should ensure that these reports also include recommendations for additional studies to confirm peer-reviewed findings, a description of what data would be required by the community to execute additional studies, and how ICANN org can offer to help broker access to such data, e.g., via the CZDS.

Consideration:

M3AAWG notes that SSR2 Recommendation 10, SSR2 Recommendation 11, SSR2 Recommendation 13 and SSR2 Recommendation 18 are closely connected and should be treated as such. A compliance function which cannot act against DNS Abuse because of staffing issues or unenforceable contracts (existing and future) is a missed opportunity. New definitions and reporting on DNS Abuse which are decoupled from DAAR reporting and/or Compliance action are also missed opportunities.

Conclusion

M3AAWG looks forward to working with our counterparts at ICANN to further the fight against abuse of the Internet. Our members include registrars with a depth and breadth of experience in the detection, mitigation and prevention of DNS and related abuse. M3AAWG anticipates working closely with ICANN to develop and implement working solutions to help address the issues that SSR2 brings forward.