8 April 2021

IPC COMMENTS ON SECOND SECURITY, STABILITY, AND RESILIENCY (SSR2) REVIEW TEAM FINAL REPORT

The Intellectual Property Constituency (IPC) appreciates the opportunity to comment on the important matter of the Second Security, Stability, and Resiliency (SSR2) Review Team Final Report, published 25 January 2021.

GENERAL IPC COMMENTS

As expressed in its comments on the SSR2 Draft Report, the IPC commends the SSR2 RT for its efforts in assessing the current state of, and recommending thoughtful improvements for, the security, stability, and resiliency of the domain name system (DNS). The IPC further commends SSR2 Review Team for achieving full consensus on all 63 Recommendations contained in the 24 Recommendation Groups. Overall, the IPC strongly supports the recommendations outlined in the Final Report, as noted in the comment chart below. There are, however, certain matters of particular importance or concern to the IPC such that the IPC believes it is its responsibility to discuss in greater detail.

First and foremost is the issue of the long-overdue implementation of SSR1 recommendations. The IPC is certainly not alone in the Community in being alarmed that not a single one of the 28 SSR1 recommendations has been implemented as of present—despite the assessment that every one of these recommendations remains relevant today. It is thus essential that the ICANN Board and Org put into place a plan for expeditiously implementing these delinquent recommendations. Both the health of the DNS, as well as faith in the multi-stakeholder model, rely on this important work product of the initial Review Team being implemented.

The IPC also remains very concerned with DNS abuse, and commends the SSR2 RT for correctly highlighting the significant and growing problem of DNS abuse, and recommending several concrete steps, as set forth in Recommendation Groups 8-15 for combatting such abuses. As a threshold matter, the IPC concurs with the recommendations to define abuse so that reporting and consequences for abuse can flow more efficiently from an agreed-upon definition. A definition will also help focus the Community on solutions, to the extent the current lack of a definition acts an excuse for some to deflect the need to address the problems of DNS abuse. The IPC also strongly supports including neutral subject matter experts in abuse and security in the negotiation of contractual DNS Abuse terms as set forth in Recommendation 8 and the establishment of pro-active and improved enforcement, monitoring and auditing of current (and future) contractual compliance with abuse related contract provisions as set forth in Recommendation Group 9.

The IPC also concurs with recommendations geared towards holding contracted parties more accountable for their roles in combatting DNS abuse, such as increased monitoring and enforcement to ensure the accuracy of registration data. While the IPC continues to urge a return to former WHOIS access for legitimate registrant data requestors, a crucial piece is ensuring the registrant data on record is complete and accurate.

SPECIFIC IPC COMMENTS

#	Recommendation	IPC Comments
1	**Recommendation 1: Further Review of SSR1** 1.1 The ICANN Board and ICANN org should perform a further comprehensive review of the SSR1 Recommendations and execute a new plan to complete the implementation of the SSR1 Recommendations (see Appendix D: Findings Related to SSR1 Recommendations).	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.
2	**Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management** 2.1 ICANN org should create a position of a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) at the Executive C-Suite level of ICANN org and hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this 2.2 ICANN org should include as part of this role's description that this position will manage ICANN org's security function and oversee staff interactions in all relevant areas that impact security. This position should be responsible for providing regular reports to the ICANN Board and community on all SSR-related activities within ICANN org. Existing security functions should be restructured and moved organizationally to report to this new position. 2.3 ICANN org should include as part of this role's description that this position will be responsible for both strategic and tactical security and risk management. These areas of responsibility include being in charge of and strategically coordinating a centralized risk assessment function, business continuity (BC), and disaster recovery (DR) planning (see also SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) across the internal security domain of the organization, including the ICANN Managed Root Server (IMRS, commonly known as L-Root), and coordinate with other stakeholders involved in the external global identifier system, as well as publishing a risk assessment methodology and approach. 2.4 ICANN org should include as part of this role's description that this role will be responsible for all security-relevant budget items and responsibilities and take part in all security-relevant contractual negotiations (e.g., registry and registrar agreements, supply chains for hardware and software, and associated service level agreements) undertaken by ICANN org, signing off on all security-related contractual terms.	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.

3	**Recommendation 3: Improve SSR-related Budget Transparency** 3.1 The Executive C-Suite Security Officer (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management) should brief the community on behalf of ICANN org regarding ICANN org's SSR strategy, projects, and budget twice per year and update and publish budget overviews annually. 3.2 The ICANN Board and ICANN org should ensure specific budget items relating to ICANN org's performance of SSR-related functions are linked to specific ICANN strategic plan goals and objectives. ICANN org should implement those mechanisms through a consistent, detailed, annual budgeting and reporting process. 3.3 The ICANN Board and ICANN org should create, publish, and request public comment on detailed reports regarding the costs and SSR-related budgeting as part of the strategic planning cycle.	The IPC is supportive of this recommendation.
4	**Recommendation 4: Improve Risk Management Processes and Procedures** 4.1 ICANN org should continue centralizing its risk management and clearly articulate its Security Risk Management Framework and ensure that it aligns strategically with the organization's requirements and objectives. ICANN org should describe relevant measures of success and how to assess them. 4.2 ICANN org should adopt and implement ISO 31000 "Risk Management" and validate its implementation with appropriate independent audits. ICANN org should make audit reports, potentially in redacted form, available to the community. Risk management efforts should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures). 4.3 ICANN org should name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role (see SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management). This function should regularly update, and report on, a register of security risks and guide ICANN org's activities. Findings should feed into BC and DR plans and procedures (see SSR2 Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures) and the Information Security Management System (ISMS) (see SSR2 Recommendation 6: Comply with Appropriate Information Security Management Systems and Security Certifications).	The IPC is supportive of this recommendation. The IPC concurs with the goals of this recommendation to prevent and address internal risks, and to adopt common industry standards.

5	**Recommendation 5: Comply with Appropriate Information Security Management Systems and Security Certifications** 5.1 ICANN org should implement an ISMS and be audited and certified by a third party along the lines of industry security standards (e.g., ITIL, ISO 27000 family, SSAE-18) for its operational responsibilities. The plan should include a road map and milestone dates for obtaining certifications and noting areas that will be the target of continuous improvement. 5.2 Based on the ISMS, ICANN org should put together a plan for certifications and training requirements for roles in the organization, track completion rates, provide rationale for their choices, and document how the certifications fit into ICANN org's security and risk management strategies. 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. 5.4 ICANN org should reach out to the community and beyond with clear reports demonstrating what ICANN org is doing and achieving in the security space. These reports would be most beneficial if they provided information describing how ICANN org follows best practices and mature, continually-improving processes	The IPC is supportive of this recommendation.
6	**Recommendation 6: SSR Vulnerability Disclosure and Transparency** 6.1 ICANN org should proactively promote the voluntary adoption of SSR best practices and objectives for vulnerability disclosure by the contracted parties. If voluntary measures prove insufficient to achieve the adoption of such best practices and objectives, ICANN org should implement the best practices and objectives in contracts, agreements, and MOUs. 6.2 ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues, such as breaches at any contracted party and in cases of critical vulnerabilities discovered and reported to ICANN org, should be communicated promptly to trusted and relevant parties (e.g., those affected or required to fix the given issue). ICANN org should regularly report on vulnerabilities (at least annually), including anonymized metrics and using responsible disclosure.	The IPC is supportive of this recommendation. However, the IPC believes the current language should not be read tol require dotBrands to disclose all vulnerabilities in their business to ICANN. This goes beyond ICANN's remit. At a minimum, any vulnerabilities should be limited only to those systems directly related to the operation of the TLD. And in the case of a dotBrand or other single registrant TLD where even such vulnerabilities are, effectively, an internal matter,such disclosure may not be warranted.

7	**Recommendation 7: Improve Business Continuity and Disaster Recovery Processes and Procedures** 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.	The IPC is supportive of this recommendation
8	**Recommendation 8: Enable and Demonstrate Representation of Public Interest in Negotiations with Contracted Parties** 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.	The IPC is supportive of this recommendation, particularly as it applies to the base agreements for contracted parties. The IPC would be willing to assist with the negotiation process by supplying subject matter experts in the field of Intellectual Property. A key concern of the IPC is for contractual language in the base agreements with respect to abuse be clear and recognized as effective and enforceable by ICANN org and the Compliance team. In general, the IPC thinks that the participation of these experts is most relevant to the

		negotiation of base agreement contractual terms and not the bi-lateral contracts between ICANN and a contracted party.
9	**Recommendation 9: Monitor and Enforce Compliance** 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.	The IPC is supportive of this recommendation. The IPC finds the current state of contractual compliance is inadequate and strongly recommends that the Board and ICANN org immediately embrace and implement this recommendation.

10	**Recommendation 10: Provide Clarity on Definitions of Abuse-related Terms** 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.	The IPC is supportive of this recommendation. The IPC further notes that the definition of abuse should be expansive and that illegal activity, such as copyright infringement and distribution of child sexual abuse material, not be erroneously conflated with or equated to content regulation. ICANN's mission and responsibility for adequately ensuring "the stable and secure operation of the Internet's unique identifier systems" is dependent upon an expansive concept of DNS Abuse, such as reflected in the Specification 11 Public Interest Commitments of the Registry Agreement.
11	**Recommendation 11: Resolve CZDS Data Access Problems** 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.	The IPC is supportive of this recommendation. However, the IPC also supports retaining checks and balances on access to CZDS data, given that it could be used to interrupt legitimate business operations. The IPC also notes that many dot Brands are opposed to having to disclose their zone file data since it could be time-sensitive commercial information, for example, if there are names registered in the dot Brand for a new product launch.

12	**Recommendation 12: Overhaul DNS Abuse Analysis and Reporting Efforts to Enable Transparency and Independent Review** 12.1 ICANN org should create a DNS Abuse Analysis advisory team composed of independent experts (i.e., experts without financial conflicts of interest) to recommend an overhaul of the DNS Abuse Reporting activity with actionable data, validation, transparency, and independent reproducibility of analyses as its highest priorities. 12.2 ICANN org should structure its agreements with data providers to allow further sharing of the data for non-commercial use, specifically for validation or peer-reviewed scientific research. This special no-fee non-commercial license to use the data may involve a time-delay so as not to interfere with commercial revenue opportunities of the data provider. ICANN org should publish all data-sharing contract terms on the ICANN website. ICANN org should terminate any contracts that do not allow independent verification of methodology behind blocklisting. 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.	The IPC is supportive of this recommendation. The IPC further notes that ICANN org should look to other sources of information relating to DNS abuse such as governments, industry trade groups and individuals.
13	**Recommendation 13: Increase Transparency and Accountability of Abuse Complaint Reporting** 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.	The IPC is supportive of this recommendation

14	**Recommendation 14: Create a Temporary Specification for Evidence-based Security Improvements** 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.	The IPC is supportive of this recommendation

15	**Recommendation 15: Launch an EPDP for Evidence-based Security Improvements** 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.	The IPC is supportive of this recommendation

16	**Recommendation 16: Privacy Requirements and RDS** 16.1 ICANN org should provide consistent cross-references across their website to provide cohesive and easy-to-find information on all actions—past, present, and planned—taken on the topic of privacy and data stewardship, with particular attention to the information around the Registration Directory Service (RDS). 16.2 ICANN org should create specialized groups within the Contractual Compliance function that understand privacy requirements and principles (such as collection limitation, data qualification, purpose specification, and security safeguards for disclosure) and that can facilitate law enforcement needs under the RDS framework as that framework is amended and adopted by the community (see also SSR2 Recommendation 11: Resolve CZDS Data Access Problems). 16.3 ICANN org should conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they have procedures in place to address privacy breaches.	The IPC is supportive of this recommendation

17	**Recommendation 17: Measuring Name Collisions** 17.1 ICANN org should create a framework to characterize the nature and frequency of name collisions and resulting concerns. This framework should include metrics and mechanisms to measure the extent to which controlled interruption is successful in identifying and eliminating name collisions. This could be supported by a mechanism to enable protected disclosure of name collision instances. This framework should allow the appropriate handling of sensitive data and security threats. 17.2 The ICANN community should develop a clear policy for avoiding and handling new gTLD-related name collisions and implement this policy before the next round of gTLDs. ICANN org should ensure that the evaluation of this policy is undertaken by parties that have no financial interest in gTLD expansion.	The IPC notes that this recommendation appears to overlap with both the outputs from SubPro on Name Collision, and the Board's recent resolution requesting the second NCAP study. The IPC has diverse opinions on Name Collision. The IPC supports a gating mechanism for high risk strings. Some in the IPC support maintaining the existing Controlled Interruption. Others in the IPC support the NCAP and SubPro IRT working in tandem to develop a new mechanism to prevent name collisions.
18	**Recommendation 18: Informing Policy Debates** 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.	The IPC is supportive of this recommendation

19	**Recommendation 19: Complete Development of the DNS Regression Test Suite** 19.1 ICANN org should complete the development of a suite for DNS resolver behavior testing. 19.2 ICANN org should ensure that the capability to continue to perform functional testing of different configurations and software versions is implemented and maintained.	The IPC is supportive of this recommendation..
20	**Recommendation 20: Formal Procedures for Key Rollovers** 20.1 ICANN org should establish a formal procedure, supported by a formal process modeling tool and language to specify the details of future key rollovers, including decision points, exception legs, the full control-flow, etc. Verification of the key rollover process should include posting the programmatic procedure (e.g., program, finite-state machine (FSM)) for Public Comment, and ICANN org should incorporate community feedback. The process should have empirically verifiable acceptance criteria at each stage, which should be fulfilled for the process to continue. This process should be reassessed at least as often as the rollover itself (i.e., the same periodicity) so that ICANN org can use the lessons learned to adjust the process. 20.2 ICANN org should create a group of stakeholders involving relevant personnel (from ICANN org or the community) to periodically run table-top exercises that follow the root KSK rollover process.	.The IPC is supportive of this recommendation.

21	**Recommendation 21: Improve the Security of Communications with TLD Operators** 21.1 ICANN org and PTI operations should accelerate the implementation of new Root Zone Management System (RZMS) security measures regarding the authentication and authorization of requested changes and offer TLD operators the opportunity to take advantage of those security measures, particularly MFA and encrypted email.	The IPC is supportive of this recommendation.
22	**Recommendation 22: Service Measurements** 22.1 For each service that ICANN org has authoritative purview over, including root zone and gTLD-related services as well as IANA registries, ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of that service, and publish a directory of these services, data sets, and metrics on a single page on the icann.org website, such as under the Open Data Platform. ICANN org should produce measurements for each of these services as summaries over both the previous year and longitudinally (to illustrate baseline behavior). 22.2 ICANN org should request community feedback annually on the measurements. That feedback should be considered, publicly summarized after each report, and incorporated into follow-on reports. The data and associated methodologies used to measure these reports' results should be archived and made publicly available to foster reproducibility.	The IPC is supportive of this recommendation.

23	**Recommendation 23: Algorithm Rollover** 23.1 PTI operations should update the DNSSEC Practice Statement (DPS) to allow the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to other algorithms or to future post-quantum algorithms, which provide the same or greater security and preserve or improve the resilience of the DNS. 23.2 As a root DNSKEY algorithm rollover is a very complex and sensitive process, PTI operations should work with other root zone partners and the global community to develop a consensus plan for future root DNSKEY algorithm rollovers, taking into consideration the lessons learned from the first root KSK rollover in 2018.	The IPC is supportive of this recommendation.
24	**Recommendation 24: Improve Transparency and End-to-end Testing for the EBERO Process** 24.1 ICANN org should coordinate end-to-end testing of the full EBERO process at predetermined intervals (at least annually) using a test plan that includes datasets used for testing, progression states, and deadlines, and is coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results. 24.2 ICANN org should make the Common Transition Process Manual easier to find by providing links on the EBERO website.	The IPC is supportive of this recommendation.

SSR2 Recommendation 1: Further Review of SSR1

ICANN's delinquency in implementing the SSR1 recommendations is deeply concerning to the IPC and other members of the Community. It is ICANN's duty to "enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates." ICANN must therefore fulfill its commitments, including completing the implementation of all relevant SSR1 recommendations which have been left outstanding since 2012.

These commitments are particularly important today as we witness a rise in DNS abuse, which ICANN has not just the opportunity, but responsibility, to address head-on through its SSR commitments. Yet as the chart below illustrates, not a single one of the 28 SSR1 recommendations has been implemented as of

present. The Final Report App'x D also concludes that every one of the original SSR1 recommendations remains relevant today.

Table 2: SSR1 Recommendation Overview

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Relevant	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Implemented	P	P	P	P	P	N	P	P	-	P	P	P	N	N	P	P	-	N	-	P	P	P	P	P	P	P	P	P
Effective	N	N	N	Y	-	N	N	N	-	N	-	N	N	N	-	N	-	-	N	N	N	N	-	N	N	-	N	N

Key: Y = Yes N = No P = Partial - = Unable to Determine

Such unexplained delays in implementing otherwise important and consensus-backed recommendations have the additional negative affect of shaking the Community's faith in the effectiveness of the multi-stakeholder model. Thus, for the health of the DNS as well as the health of the overall Internet Community, ICANN must fulfill its outstanding obligations as relates to the SSR1 recommendations. Accordingly, the IPC strongly supports the recommendation that the ICANN Board and ICANN Org review all SSR1 recommendations to put in place a plan for the recommendations to be expeditiously implemented.

SSR2 Recommendation 2: Create a C-Suite Position Responsible for Both Strategic and Tactical Security and Risk Management

The IPC supports the SSR2 RT's recommendation that a C-Suite level executive officer position be created to coordinate and strategically manage ICANN's security and risk management objectives. This new role should effectively centralize previously decentralized roles related to SSR in a manner geared toward greater efficiency and responsibility. The need for this new position is particularly clear to the IPC in light of ICANN's failure to efficiently implement the SSR1 objectives that have been outstanding since 2012. It is the hope of the IPC that an experienced security executive designated as this officer, supported by a sufficient budget and staff, will be able to more efficiently prioritize and implement these critical security and risk management activities for which ICANN is responsible. Accordingly, the IPC is strongly supportive of the RT's recommendations related to this new position.

The SSR2 Final Report clearly sets forth what it will take for each of the recommendations to be considered "implemented." This provides very helpful guidance and the IPC urges that the Board and ICANN Org not only adopt these SSR2 recommendations but also specifically direct ICANN Org to implement the recommendations in accordance with the specific guidance set forth in the SSR2 Final Report.

Respectfully submitted,

Intellectual Property Constituency