IPC COMMENTS ON SECOND SECURITY, STABILITY, AND RESILIENCY (SSR2) REVIEW TEAM DRAFT 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 (RT) Draft Report."

EXECUTIVE SUMMARY

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). Echoing the RT, the IPC reiterates the importance of ICANN's "commitment 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 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.

The IPC notes that in some cases the numbering in the Recommendations summary table does not match the body of the report. For example, the sub-recommendations under Recommendation 10 are numbered 10.5-10.8 in the main body of the report. For the avoidance of doubt we are using the numbering in the summary table.

SPECIFIC IPC COMMENTS

#	Recommendation	IPC Comments
1	**Complete the implementation of all relevant SSR1 recommendations**	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.

2	**SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications** 2.1 ICANN org should establish a road map of its industry-standard security audits and certification activities that are being undertaken, including milestone dates for obtaining each certification and noting areas of continuous improvement. 2.2 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. 2.3 ICANN org should also provide reasoning for their choices, demonstrating how they fit into its security and risk management strategies 2.4 ICANN org should implement an Information Security Management System and undergo a third-party audit. 2.5 In order to reap the benefits of a certification and audit regimen, ICANN org should be audited and certified by a third party along the lines of industry security standards and should assess certification options with commonly accepted international standards (e.g., ITIL, ISO 27001, SSAE-18) for its operational responsibilities.	The IPC is supportive of this recommendation.
3	**SSR1 Recommendations 12,15, and 16 - SSR Strategy and Framework, Metrics, and Vulnerability Disclosures** 3.1. ICANN org should address security issues clearly, publicly (with consideration for operational security, e.g., after an established moratorium and anonymization of the information, if required), and promote security best practices across all contracted parties. 3.2. ICANN org should also capture SSR-related best practices in a consensus document, establish clear, measurable, and trackable objectives, and then implement the practices in contracts, agreements, and MOUs. 3.3. ICANN org should implement coordinated vulnerability disclosure reporting. Disclosures and information regarding SSR-related issues should be communicated promptly to trusted, relevant parties (e.g., those affected or required to fix the given issue), such as in cases of breaches at any contracted party and in cases of key vulnerabilities discovered and reported to ICANN org.	The IPC is supportive of this recommendation.

	3.4. ICANN org should establish a clear communication plan for reports to the community and produce regular (at least annual) and timely reports containing anonymous metrics of the vulnerability disclosure process. These communiques should contain responsible disclosure as defined by the community- agreed process and include anonymized metrics.	
4	**SSR1 Recommendation 20 and 22 - Budget Transparency and Budgeting SSR in new gTLDs** 4.1 Where possible (contractually) and reasonable in terms of effort (i.e., over 10% of the activity described in the budget line item), ICANN should be more transparent with the budget for parts of ICANN org related to implementing the Identifier Systems Security, Stability, and Resiliency (IS-SSR) Framework and performing SSR-related functions, including those associated with the introduction of new gTLDs.	The IPC is supportive of this recommendation. Budget transparency would be helpful in reflecting ICANN's commitment to SSR recommendations, however the opening language of this recommendation (e.g., "Where possible" and "reasonable in terms of effort") leaves open the possibility that ICANN could circumvent the transparency intended by this recommendation.
5	**SSR1 Recommendation 27 - Risk Management** 5.1. ICANN's Risk Management Framework should be centralized and strategically coordinated. 5.2. ICANN org should clearly articulate their risk framework and strategically align the framework against the requirements and objectives of the organization, describing relevant measures of success and how ICANN org will assess these measures. 5.3. ICANN should make information pertaining to risk management centrally available to the community. This information should be regularly updated to reflect the current threat landscape (at least annually).	The IPC is supportive of this recommendation.

6	**Create a Position Responsible for Both Strategic and Tactical Security and Risk Management** 6.1. ICANN org should create a position responsible for both strategic and tactical security and risk management across the internal security domain of the organization, as well as the external global identifier system. 6.2. ICANN org should hire an appropriately qualified individual for that position and allocate a specific budget sufficient to execute this role's functions. 6.3. This position should manage ICANN org's Security Function and oversee the interactions of staff in all relevant areas that impact security. 6.4. The position should also provide regular reports to ICANN's Board and community. 6.5. This position would act as a pathfinder and problem-solver who would strategize and execute multi-faceted programs to achieve substantial improvements. 6.6. Additionally, this role should take part in all security-relevant contractual negotiations (e.g., 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.
7	**Further Develop a Security Risk Management Framework** 7.1. ICANN org should clearly articulate their Security Risk Management Framework and ensure that it aligns strategically against the requirements and objectives of the organization. 7.2. ICANN org should describe relevant measures of success and how these measures are to be assessed. The SSR2 RT described the foundation of this in detail in the additional feedback regarding SSR1's Recommendation 9 (see 'SSR1 Recommendation 9 - Information Security Management Systems and Security Certifications'	The IPC is supportive of this recommendation.

	earlier in this report). 7.3. ICANN org should: 7.3.1. Adopt and implement ISO 31000 "Risk Management" and validate and certify their implementation with appropriate independent audits. Risk management efforts should feed into Business Continuity and Disaster Recovery Plans and Provisions. 7.3.2. Regularly update a register of security risks and use that register to prioritize and guide the activities of the ICANN org. ICANN org should report on updates of their methodology and updates to the register of security risks. Findings should feed into BC/DR and the Information Security Management System (ISMS). 7.3.3. Name or appoint a dedicated, responsible person in charge of security risk management that will report to the C-Suite Security role as described in the recommendation "C-Suite Security Position."	
8	**Establish a Business Continuity Plan Based on ISO 22301** 8.1. ICANN org should establish a Business Continuity Plan for all the systems owned by, or under the purview of ICANN org, based on ISO 22301 "Business Continuity Management."5 8.2. ICANN should identify the importance of functional, acceptable timelines for BC and DR based on the urgency of restoring full functionality. 8.3. For Public Technical Identifiers (PTI) operations (IANA functions, including all relevant systems that contribute to the Security and Stability of the DNS and also Root Zone Management), ICANN org should develop a shared approach to service continuity in close cooperation with the Root Server System Advisory Committee (RSSAC) and the root server operators. 8.4. ICANN org should publish evidence (e.g., a summary) of their Business Continuity Plans and Provisions. An external auditor should be engaged to verify compliance aspects of the implementation of the resulting business continuity plans.	The IPC is supportive of this recommendation.

9	**Ensure the Disaster Recovery Plan is Appropriate, Functional, and Well Documented** 9.1. ICANN org should ensure that the DR plan for PTI operations (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 *Guidelines for information and communication technology readiness for business continuity.* ICANN org should develop this plan in close cooperation with RSSAC and the root server operators. 9.2. ICANN org should also establish a DR Plan for all the systems owned by or under the purview of ICANN org, again in line with ISO 27031 *Guidelines for information and communication technology readiness for business continuity.* 9.3. ICANN org should have a disaster recovery plan developed within twelve months of the ICANN Board's adoption of these recommendations around establishing at least a third site for disaster recovery (in addition to Los Angeles and Culpepper), specifically outside of the United States and its territories and the North American region, including a plan for implementation. 9.4. ICANN org should publish a summary of their overall disaster recovery plans and provisions. ICANN org should engage an external auditor engaged to verify compliance aspects of the implementation of these DR plans.	The IPC is supportive of this recommendation.

10	**Improve the Framework to Define and Measure Registrar & Registry Compliance** 10.1. Establish a performance metrics framework to guide the level of compliance by Registrars and Registries for WHOIS obligations (including inaccuracy), as well as other elements that affect abuse, security, and resilience, as outlined in the RDS/WHOIS2 Review and the CCT Review. 10.2. Allocate a specific budget line item for a team of compliance officers tasked with actively undertaking or commissioning the work of performance management tests/assessments of agreed SLA metrics. 10.3. Amend the SLA renewal clause from 'automatically renewed' to a cyclical four-year renewal that includes a review clause included (this review period would consider the level of compliance to the performance metrics by the Registrar and Registry and recommend the inclusion of requirements to strengthen the security and resilience where non-compliance was evident). 10.4. Further, the ICANN Board should take responsibility for bringing the EPDP to closure and passing and implementing a WHOIS policy in the year after this report is published.	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. 10.4: While the IPC is supportive of the intent behind recommendation 10.4, it notes that it is not the role of the Board to direct the outcome or timing of a community-led PDP. The RT may wish to revise this language, for example to refer to the Board itself, and via Org, offering all necessary support to achieve the desired outcome
11	**Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions** 11.1 ICANN Board should drive efforts that minimize ambiguous language and reach a universally acceptable agreement on abuse, SSR, and security threats in its contracts with contracted parties and implementation plans. 11.2 ICANN org and Board should implement the SSR-relevant commitments (along with CCT and RDS/WHOIS2 Review recommendations) based on current, community vetted abuse definitions, without delay. 11.3 ICANN Board, in parallel, should encourage community attention to evolving the DNS abuse definition (and application), and adopt the additional term and evolving external definition of "security threat"—a term used by the ICANN Domain Abuse Activity Reporting (DAAR) project, and the GAC (in its Beijing Communique[10] and for Specification 11[11]), and addressed in international conventions such as the Convention on Cybercrime and its related "Explanatory Notes" 12 —to use in conjunction with ICANN org's DNS Abuse definition. 11.4 The ICANN Board should entrust SSAC and PSWG to	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.

	work with e-crime and abuse experts to evolve the definition of DNS Abuse, taking into account the processes and definitions outlined in the Convention on Cybercrime.	
12	**Create Legal and Appropriate Access Mechanisms to WHOIS Data** 12.1. The ICANN Board should create a legal and appropriate access mechanisms to WHOIS data by vetted parties such as law enforcement. 12.2. The ICANN Board should take responsibility for, and ensure ICANN org comes to immediate closure on, implementation of the Temporary Specification for gTLD Registration Data.	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.

13	**Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program** 13.1 The ICANN Board and ICANN org should work with the entities inside and outside the ICANN community that are mitigating abuse to improve the completeness and utility of DAAR, in order to improve both measurement and reporting of domain abuse. 13.1.1. ICANN org should publish DAAR reports that identify registries and registrars whose domains most contribute to abuse according to the DAAR methodology. 13.1.2. ICANN org should make the source data for DAAR available through the ICANN Open Data Initiative and prioritize items *"daar"* and "*daar-summarized*" of the ODI Data Asset Inventory[14] for immediate community access. 13.1.3. ICANN org should publish reports that include machine- readable formats of the data, in addition to the graphical data in current reports. 13.1.4. ICANN org should provide assistance to the Board and all constituencies, stakeholder groups and advisory committees in DAAR Interpretation, including assistance in the identification of policy and advisory activities that would enhance domain name abuse prevention and mitigation.	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.
14	**Enable Rigorous Quantitative Analysis of the Relationship Between Payments for Domain Registrations and Evidence of Security Threats and Abuse** 14.1 ICANN org should collect, analyze, and publish pricing data to enable further independent studies and tracking of the relationship between pricing and abuse.	The IPC is supportive of this recommendation. 14.1 While the IPC is strongly supportive of the intent behind recommendation 14.1, it notes that new gTLD registries are not under a contractual obligation to disclose their wholesale pricing and that efforts to gather this information from registries voluntarily during previous reviews (such as CCT) and PDPs (such as RPMs) have been unsuccessful. The RT is encouraged to revisit and refine this recommendation, for example to encourage Org to seek to include obligations during contract renewal/contract negotiations to disclose pricing information on a confidential basis for the use by RTs and PDPs and/or for Org to consider whether registrar retail pricing can meaningfully inform this issue.

15	**Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse** 15.1. ICANN org should, make SSR requirements mandatory on contract or baseline agreement renewal in agreements with contracted parties, including Registry Agreements (base and individual) and the RAA, These contract requirements should include provisions that establish thresholds of abuse (e.g., 3% of all registrations) that would automatically trigger compliance inquiries, with a higher threshold (e.g., 10% of all registrations) at which ICANN org considers registrars and registries to be in default of their agreements. The CCT Review also recommended this approach.[15] 15.2. ICANN org should introduce a contract clause that would support contract termination in the case of "a pattern and practice" of abuse (as in section 5.5.2.4 "TERM, TERMINATION AND DISPUTE RESOLUTION" of the 2013 Registrar Accreditation Agreement)[16]. 15.3. In order to support the review of these contract changes, ICANN org should: 15.3.1. Ensure access to registration data for parties with legitimate purposes via contractual obligations and with rigorous compliance mechanisms. 15.3.2. Establish and enforce uniform Centralized Zone Data Service requirements to ensure continuous access for SSR research purposes. 15.3.3. Attract and collaborate with ccTLDs and the ccNSO to help address DNS abuse and security threats in ccTLDs. 15.3.4. The ICANN Board, community, and org should work with the ccNSO to advance data tracking and reporting, assess DNS abuse and security threats in ccTLDs, and develop a ccNSO plan to support ccTLDs in further mitigating DNS abuse and security threats. 15.3.5. Immediately instantiate a requirement for the RDAP services of contracted parties to white-list ICANN org address space and establish a process for vetting other entities that RDAP services of contracted parties will whitelist for non-rate-limited access. 15.4 In the longer term, ICANN Board should request that the GNSO initiate the process to adopt new policies and agreements with Contracted Parties that measurably improve mitigation of DNS abuse and security threats, including changes to RDAP and registrant information, incentives for	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. 15.3.2 The IPC would point out that many brand owners who operate Brand TLDs under Spec 13 are reluctant to have their future branding decisions telegraphed by means of the public access to the CZDS. The Brand TLDs would encourage a more nuanced treatment of CZDS access which recognizes the particular nature of a TLD. 15.3.3 – 4 The IPC is supportive of the intent behind these recommendations but notes that ICANN has no control over ccTLDs and the ccNSO. The RT is encouraged to revisit and refine this to acknowledge this lack of control. We seek clarification as to the changes to registrant information proposed by 15.4: what changes specifically are proposed?

	contracted parties for abuse/security threat mitigation, establishment of a performance metrics framework, and institutionalize training and certifications for contracted parties and key stakeholders.	

16	**Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats** 16.1. ICANN org should incentivize the mitigation of abuse and security threats making the following changes to contracts: 16.1.1. Contracted parties with portfolios with less than a specific percentage (e.g., 1%) of abusive domain names (as identified by commercial providers or DAAR) should receive a fee reduction (e.g., a reduction from current fees, or an increase of the current per domain name transaction fee and provide a Registrar with a discount). 16.1.2. Registrars should receive a fee reduction for each domain name registered to a verified registrant up to an appropriate threshold. 16.1.3. Waive RSEP fees when the RSEP filings clearly indicate how the contracted party intends to mitigate DNS abuse, and that any Registry RSEP receives pre-approval if it permits an EPP field at the Registry level to designate those domain names as under management of a verified Registrant. 16.1.4. Refund fees collected from registrars and registries on domains that are identified as abuse and security threats and are taken down within an appropriate period after registration (e.g., 30 days after the domain is registered). 16.2. Given all parties (ICANN org, contracted parties, and other critical stakeholders such as Registries, Registrars, Privacy/Proxy Service Providers, Internet Service Providers, and the contracted parties) must understand how to accurately measure, track, detect, and identify DNS abuse, ICANN org should institutionalize training and certifications all parties in areas identified by DAAR and other sources on the common methods of abuse **[citation to be added]** and how to establish appropriate mitigation efforts. Training should include as a starting point: Automatic tracking of complaint numbers and treatment of complaints; Quarterly/Yearly public reports on complaints and actions; and analysis.	The IPC is generally supportive of this recommendation, and discusses its support for this recommendation in greater detail below. 16.1.4 The IPC does not understand what is intended by this recommendation. It would appear to create the possibility of a bad-actor registrar selling such names and then rapidly taking them down, thereby receiving payment both from the registrant and a refund from ICANN. This presumably is not the intent, so the RT may wish to clarify this recommendation.

17	**Establish a Central Abuse Report Portal** 17.1 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 inflow, with only summary and metadata flowing upstream. Use of the system should be mandatory for all gTLDs; ccTLDs should be invited to join. Responses must be publicly searchable and included in yearly reports (in complete form, or by reference). In addition, reports should be made available (e.g., via email) to non-participating ccTLDs.	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below.
18	**Ensure that the ICANN Compliance Activities are Neutral and Effective** 18.1. ICANN org should have compliance activities audited externally and hold them to a high standard. 18.2. The ICANN Board should empower the Compliance Office to react to complaints and require Compliance to initiate investigations and enforce contractual obligations against those aiding and abetting systemic abuse, as defined by the SLA. This additional authority could include support for step by step actions around the escalation of enforcement measures and appropriate implementable actions that ICANN org can use in response to any failures to remedy compliance violations within specified timeframes. 18.3. The ICANN Compliance Office should, as their default, involve SLAs on enforcement and reporting, clear and efficient processes, a fully informed complainant, measurable satisfaction, and maximum public disclosure.	The IPC is supportive of this recommendation.

19	**Update Handling of Abusive Naming** 19.1. ICANN org should build upon the current activities to investigate typical misleading naming, in cooperation with researchers and stakeholders, wherever applicable. 19.2. When misleading naming rises to the level of abusive naming, ICANN org should include this type of abuse in their DAAR reporting and develop policies and mitigation best practices. 19.3. ICANN org should publish the number of abusive naming complaints made at the portal in a form that allows independent third parties to analyze, mitigate, and prevent harm from the use of such domain names. 19.4. ICANN org should update the current "Guidelines for the Implementation of IDNs" **[citation to be added]** to include a section on names containing trademarks, TLD-chaining, and the use of (hard-to-spot) typos. Furthermore, ICANN should contractually enforce "Guidelines for the Implementation of IDNs" for gTLDS and recommend that ccTLDs do the same.	The IPC is supportive of this recommendation, and discusses its support for this recommendation in greater detail below. 19.2 The IPC understand the DAAR to be a collection of existing, publicly available feeds. The IPC suggests that this recommendation might better be expressed as "ICANN Org should seek to identify and incorporate feed(s) tracking this type of abuse in the DAAR. We would also encourage ICANN org to include information covering cybersquatting within the meaning of "abusive naming" for purposes of reporting and other requirements around anti-abuse measures, to the extent this category is not already explicitly covered. 19.4 The IPC encourages the RT to expand on this recommendation, which presently lacks clarity and specificity. The recommendation might include specific reference to cybersquatting and the use of IDN homoglyphs to mimic trademarks as an example of abusive naming through IDNs.
20	**Complete Development of a DNS Regression Testing** 20.1. ICANN org should complete the development of a suite for DNS regression testing. 20.2. ICANN org should ensure that the capability to perform functional testing of different configurations and software versions is implemented and maintained.	The IPC is supportive of this recommendation.

21	**Implement the Recommendations from SAC063 and SAC073 and Establish Formal Procedures for Key Rollovers** 21.1. ICANN org should implement the recommendations from SAC063 and SAC073 in order to ensure the SSR of the KSK rollover process. 21.2. 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, FSM) for public comment, and community feedback should be incorporated. 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 lessons learned can be used to adjust the process. 21.3. 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.
22	**Establish Baseline Security Practices for Root Server Operators and Operations** 22.1 ICANN org, in close cooperation with RSSAC and other relevant stakeholders, should ensure that the RSSgovernance model as proposed by RSSAC037 includes baseline security best practices for root server operators and operations in order to minimize the SSR risks associated with root server operation. These best practices should include change management, verification procedures, and sanity check procedures. 22.2. ICANN org should also develop relevant KPIs to measurethe implementation of these best practices and requirements and ensure yearly public reporting on how Root Server Operators (RSOs) and other relevant parties, including ICANN org, can meet these KPIs. 22.3. ICANN org should document hardening strategies of the ICANN Managed Root Server (IMRS), commonly known as L- Root, and should encourage other RSOs to do the same. 22.4. ICANN org should ensure that the IMRS uses a vulnerability disclosure process (not necessarily	The IPC is supportive of this recommendation.

	public), security reports and intelligence, and communication with researchers and RSSAC advice or recommendations, where applicable.	
23	**Accelerate the Implementation of the New-Generation RZMS** 23.1. ICANN and PTI operations should accelerate the implementation of new RZMS security measures regarding the authentication and authorization of requested changes. 23.2. ICANN org should launch public comment as soon as possible on changes regarding revisions to the RZMS policies.	The IPC is supportive of this recommendation.
24	**Create a List of Statistics and Metrics Around the Operational Status of the Unique Identifier Systems** 24.1. ICANN org should create a list of statistics and metrics that reflect the operational status (such as availability and responsiveness) of each type of unique identifier information, such as root-zone related service, IANA registries, and any gTLD service that ICANN org has authoritative purview over. 24.2. ICANN org should publish a directory of these services, data sets, and metrics on a single page on the ICANN org web site, such as under the Open Data Platform. 24.3. ICANN should publish annual and longitudinal summaries of this data, solicit public feedback on the summaries, and incorporate the feedback to improve future reports.	The IPC is supportive of this recommendation.

	24.4.	For both sets of KPIs, ICANN org should produce summaries over both the previous year and longitudinally, request and publish a summary of community feedback on each report and incorporate this feedback to improve follow-on reports.	

25	**Ensure the Centralized Zone File Data Access is Consistently Available** 25.1 The ICANN community and ICANN org should take steps to ensure that access to CZDS as well as other data is available, in a timely manner, and without unnecessary hurdles to requesters. 25.2 ICANN org should implement the four recommendations in SSAC 97: *"Recommendation 1: The SSAC recommends that the ICANN Board suggest to ICANN Staff to consider revising the CZDS system to address the problem of subscriptions terminating automatically by default, for example by allowing subscriptions to automatically renew by default. This could include an option allowing a registry operator to depart from the default on a per-subscriber basis, thereby forcing the chosen subscriber to reapply at the end of the current term. The CZDS should continue to provide registry operators the ability to explicitly terminate a problematic subscriber's access at any time.* *Recommendation 2: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that in subsequent rounds of new gTLDs, the CZDS subscription agreement conform to the changes executed as a result of implementing Recommendation 1.* *Recommendation 3: The SSAC recommends that the ICANN Board suggest to ICANN Staff to seek ways to reduce the number of zone file access complaints, and seek ways to resolve complaints in a timely fashion.* *Recommendation 4: The SSAC recommends that the ICANN Board suggest to ICANN Staff to ensure that zone file access and Web-based WHOIS query statistics are accurately and publicly reported, according to well-defined standards that can be uniformly complied with by all gTLD registry operators. The Zone File Access (ZFA) metric should be clarified as soon as practicable.*	The IPC is supportive of this recommendation, subject to above-noted concerns about CZDS access, and particularly the treatment of Brand TLDs.

26	**Document, Improve, and Test the EBERO Processes** 26.1. ICANN org should publicly document the EBERO processes, including decision points, actions, and exceptions. The document should describe the dependencies for every decision, action, and exception. 26.2. Where possible, ICANN org should automate these processes and test them annually. 26.3. ICANN org should publicly conduct EBERO smoke-testing at predetermined intervals using a test plan coordinated with the ICANN contracted parties in advance to ensure that all exception legs are exercised and publish the results. 26.4. ICANN org should improve the process by allowing the gTLD Data Escrow Agent to send the data escrow deposit directly to the EBERO provider.	The IPC is supportive of this recommendation.
27	**Update the DPS and Build Consensus Around future DNSKEY Algorithm Rollovers** 27.1. PTI operations should update the DPS to facilitate the transition from one digital signature algorithm to another, including an anticipated transition from the RSA digital signature algorithm to ECDSA or to future post-quantum algorithms, which will create a more resilient DNS while providing the same or greater security. 27.2. As 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.

28	**Develop a Report on the Frequency of Measuring Name Collisions and Propose a Solution** 28.1. ICANN org should produce findings that characterize the nature and frequency of name collisions and resulting concerns. The ICANN community should implement a solution before the next round of gTLDs. 28.2. ICANN org should facilitate this process by initiating an independent study of name collisions through to its eventual completion and adopt or account for the implementation or non-adoption of any resulting recommendations. By "independent," SSR2 RT means that ICANN org should ensure that the SSAC Name Collision Analysis Project (NCAP) work party research and report evaluation team's results need to be vetted by parties that are free of any financial interest in TLD expansion. 28.3. ICANN org should enable community reporting on instances of name collision. These reports should allow appropriate handling of sensitive data and security threats and should be rolled into community reporting metrics.	The IPC is supportive of this recommendation.

29	**Focus on Privacy and SSR Measurements and Improving Policies Based on Those Measurements** 29.1. ICANN org should monitor and regularly report on the privacy impact of technologies like DoT (DNS over TLS) and DoH (DNS over HTTPS). 29.2. ICANN org's consensus policies and agreements with registry operators and registrars should, therefore, have clauses to reflect compliance with these while ensuring that the DNS is not fragmented because of the need to maintain/implement minimum requirements governing the collection, retention, escrow, transfer, and display of registration data, which includes contact information of the registrant, administrative, and technical contacts as well as technical information associated with a domain name. 29.3. ICANN org should: 29.3.1. Create specialized units within the contract compliance function that focus on 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 evolving RDAP framework. 29.3.2. Monitor relevant and evolving privacy legislation (e.g., CCPA and legislation protecting personally identifiable information (PII)) and ensure that ICANN org's policies and procedures are aligned and in compliance with privacy requirements and the protection of personally identifiable information as required by relevant legislation and regulation.20 29.3.3. Develop and keep up to date a policy for the protection of personally identifiable information. The policy should be communicated to all persons involved in the processing of personally identifiable information. Technical and organizational measures to appropriately protect PII should be implemented. 29.3.4. Conduct periodic audits of adherence to privacy policies implemented by registrars to ensure that they, at a minimum, have procedures in place to address privacy breaches. 29.4. ICANN org's DPO should also be responsible for external DNS PII. The DPO should provide guidance to managers and stakeholders regarding responsibilities and procedures and monitor and report on relevant technical developments.	The IPC is supportive of this recommendation, while noting that the following recommendation is unclear and potentially subject to unintended interpretation in implementation: 'ICANN org's DPO should also be responsible for external DNS PII'.

30	**Stay Informed on Academic Research of SSR Issues and Use That Information to Inform Policy Debates** 30.1. 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 S&P, as well as the operational security conferences APWG, M3AAWG, and FIRST, and publish a report for the ICANN community summarizing implications of publications that are relevant to ICANN org or contracted party behavior. 30.1.1. These reports should include 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. 30.1.2. These reports should also include recommendations for additional study to confirm peer-reviewed findings, a description of what data would be required to execute additional recommended studies, and how ICANN can offer to help broker access to such data, e.g., CZDS.	The IPC is supportive of this recommendation.
31	**Clarify the SSR Implications of DNS-over-HTTP** 31.1. ICANN org should commission an independent investigation(s) into the SSR-related implications of DoH deployment trends, as well as implications for the future role of IANA in the Internet ecosystem. The intended outcome is to ensure that all stakeholders have the opportunity to understand the SSR- related implications of these developments, and the range of alternatives (or lack thereof) various stakeholders have to influence the future.	The IPC is supportive of this recommendation.

SSR2 Recommendation 1: Complete the implementation of all relevant SSR1 recommendations.

The IPC is concerned about the SSR2 RT's finding that none of the 28 SSR1 recommendations issued in 2012 have yet to be fully implemented by ICANN. It is ICANN's stated 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." By failing to implement high priority SSR recommendations from 2012, ICANN is not just in neglect of its important SSR duties but also contributes to the rising problem of DNS abuse, detailed below.

It is the IPC's position that these outstanding SSR1 recommendations must be implemented and are

critical to the effective implementation of any new SSR2 recommendations. As the RT finds 27 of the initial 28 recommendations to still be relevant, the IPC strongly supports the recommendation that all relevant SSR1 recommendations be expeditiously implemented.

SSR2 Recommendations Regarding the Creation of a C-Suite Security Position

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. As the RT points out, the current system that decentralizes the roles related to SSR across two separate units within ICANN appears unlikely to be effective. The IPC agrees with this assessment, particularly 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 a designated 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, including SSR2 Recommendation 7: "Further Develop a Security Risk Management Framework."

SSR2 Recommendations Addressing DNS Abuse

The IPC commends the SSR2 RT for correctly highlighting the significant and growing problem of DNS abuse, and recommending several steps for combatting such abuses. DNS abuse has been the subject of great concern and much discussion among members of the ICANN community (see, for example, December 2019 letter from the BC to the ICANN Board). As a preliminary matter, the IPC supports SSR2 Recommendation 11: "Lead Efforts to Evolve Definitions Around Abuse and Enable Reporting Against Those Definitions" and any related efforts to define abuse so that reporting and consequences for abuse can flow more efficiently from an agreed-upon definition.

The RT recommends, and the IPC supports, several methods for ICANN to better utilize its relationships with the Registrars and Registries to combat DNS abuse, including SSR2 Recommendation 10: "Improve the Framework to Define and Measure Registrar & Registry Compliance," SSR2 Recommendation 15: "Enhance Contracts with Registrars and Registries to Incent the Mitigation of DNS Abuse," and SSR2 Recommendation 16: "Create Pricing Incentives for Contracted Parties to Mitigate Abuse and Security Threats." The IPC supports these recommendations and any steps to more effectively combat DNS abuse relating to the Registry Agreement (RA) and Registrar Accreditation Agreement (RAA) contracts. As highlighted in the BC's December 2019 letter, there is existing language within both the RA and RAA contracts that creates obligations to mitigate abuse. However, we learned at ICANN66 that ICANN Compliance narrowly construes this language and does not require meaningful implementation of these terms by registries or registrar. Accordingly, the IPC supports these SSR2 recommendations that would require meaningful enforcement of existing obligations of registries and registrars to prohibit certain security threats and abusive activities, enhance such requirements to further mitigate such activities, include real consequences for registrants who engage in prohibited abusive behavior, and motivate active and consistent investigation and response to reports of abuse by registrars.

The IPC strongly supports the RT's recommendations that address investigating and responding to DNS abuse, including Recommendation 12: "Create Legal and Appropriate Access Mechanisms to WHOIS Data," SSR2 Recommendation 13: "Improve the Completeness and Utility of the Domain Abuse Activity Reporting Program (DAAR)," SSR2 Recommendation 17: "Establish a Central Abuse Report Portal," and SSR2 Recommendation 19: "Update Handling of Abusive Naming." Recommendation 12 addressing

WHOIS data addresses issues raised by many in the community including the Security and Stability Advisory Committee (SSAC), Governmental Advisory Committee (GAC), BC, and IPC. It is important to the issue of addressing abuse that registrant data is correct, and available through the proper channels or to the proper authorities. As for the DAAR, the IPC commends ICANN's intended goal of "develop[ing] a robust, reliable, reproducible, and replicable methodology for analyzing security threat activity that can then be later used by the ICANN community to facilitate informed policy decisions." However, the RT's assessment finds that the DAAR falls far short of this goal in practice because it lacks sufficient information to be able to tell which registrars or registries are harboring significant abuse. The IPC supports the RT's recommendation to include this critical data and turn the DAAR into a powerful tool for accountability and transparency in the domain name registration system. The IPC also strongly supports and commends the RT's Recommendation 19 to target abusive naming in the DNS. Cybercriminals are assisted in their attacks on individuals and companies through use of misleading names, oftentimes channeling a trusted or well-known name (including in many cases a trademark), to gain the trust of their victims. The IPC encourages ICANN to adopt this recommendation and take steps to make it more difficult for a cybercriminal to take advantage of abusively misleading names.
The IPC does however note that a number of brand owners now operate Brand TLDs under Specification 13, in which, due to the nature of these TLDs, the risk of DNS abuse is low. In making recommendations that seek to impose additional obligations for monitoring and reporting, the IPC would urge the RT to acknowledge differing risk profiles and avoid imposing unnecessary and costly burdens on Brand TLDs. In particular, this might include different requirements for access to Brand TLD zone files through the CZDS, different security threat monitoring and reporting requirements, and different audit approaches with respect to maintaining the security of a Brand TLD.

Lastly, the RT is correct in recognizing that cybercriminals and other threat actors identify and take advantage of gaps in DNS security. Therefore, the IPC believes it is critical that ICANN implement the SSR2 recommendations with a sense of urgency and efficiency not previously applied to the SSR1 recommendations.

Input on format and characterization of recommendations as 'high priority'

In closing, the IPC notes that the RT has made 31 recommendations, most of which have multiple sub-recommendations, and most of these are assigned a 'high priority' by the RT. We would simply caution that spirit and intent of the Operating Standards for Specific Reviews1 encourage RTs to categorize each recommendation as 'high priority', 'medium priority', or 'low priority', as a useful guideline for the planning of the implementation work. This prioritization is intended to assist Org and the community and to try to minimize volunteer exhaustion. The RT could greatly assist the community by being more selective in prioritization for their Final Report.

The IPC **also** notes that the recent Operating Standards for Specific Reviews also ask that recommendations "provide specific, measurable, achievable, realistic, and time-bound (SMART) recommendations based on fact-based findings. The review team is strongly encouraged to lay out problems it discovered and explain how its recommendations will address these, leading to substantive improvements. To facilitate the eventual implementation of its recommendations, the review team shall include, wherever possible, relevant metrics and applicable key performance indicators (KPIs) that could be applied to assess the implementation of each of its recommendations." The IPC commends the RT for having produced a report which is well-structured and easy to navigate and read. Based on the IPC's experience with other Reviews, and particularly on the time that it can take to track back through the recommendations of earlier iterations of a specific review, the IPC asks the RT to consider whether it

[1] https://www.icann.org/en/system/files/files/operating-standards-specific-reviews-23jun19-en.pdf

would be feasible for its recommendations to also be presented in a manner where the recommendation, the problem it addresses and how it does so, together with any KPIs, are clearly laid out together in a tabular form, perhaps in an annex. The IPC believes that this would assist both the next SSR RT when they come to assess the implementation and effectiveness of the SSR2 recommendations, and the community during the subsequent public comment process.

Respectfully submitted,

Intellectual Property Constituency