ISPCP Comments on:

Draft Statement of ICANN's Role and Remit in Security, Stability and Resiliency of the Internet's Unique Identifier Systems

1. Purpose

The ISPCP is responding to ICANN's request for community feedback on a draft statement of ICANN's Role and Remit in Security, Stability & Resiliency of the Internet's Unique Identifier Systems. That statement is intended to provide a clear and enduring explanation of ICANN's role and remit in this area, and also inform ICANN's consideration of the Security, Stability & Resiliency of the DNS Review Team's draft Recommendations #1 and #3.

2. Overall Comments

The ISPCP welcomes the launch of this discussion. Our position can be summarized as follows: we support a broader, more structured, conversation amongst ecosystem participants in order to arrive at a mutually agreeable statement of ICANN's remit.

One source of confusion throughout this conversation is the ambiguous meaning of "ICANN." In some cases contributors may be referring to "ICANN the corporation, headed by its CEO," in others "ICANN the community" and in many cases it may not be clear. It may be useful to start stating that distinction more overtly as we think and write about this Role and Remit topic, since the conclusions may differ depending on which definition of ICANN we're referring to.

A final broad comment: participants in this conversation need to know "what's in it for me?" It will be much easier to conduct this conversation, and make the changes that may result, if there are clearly understood benefits for all stakeholders at the end. These benefits will likely fall in four broad categories:

- Become more nimble, reduce response/reaction time
- Increase revenue/activity/impact
- Improve quality
- Reduce costs

We commend the ICANN security team for stepping forward to get the conversation under way and hope to contribute to it throughout.

3. Comments in response to SSR-RT Recommendation 1

ICANN (the corporation?) is requesting community feedback on three questions arising from Recommendation 1 of the draft SSR-RT report, which states that ICANN

(the corporation, or the community?) should "publish a single, clear and consistent statement of its SSR remit and limited technical mission."

3.1. What does it mean "to coordinate at the overall level, the global Internet's system of unique identifiers"?

The answer proposed in the Draft Statement is:

> "To coordinate means to actively engage with stakeholders in the global Internet ecosystem to ensure
>
> - allocation of the Internet's unique identifiers,
> - security, stability and resiliency of the Internet's unique identifiers, and
> - operational and policy development functions of the Internet's unique identifiers is conducted in an open, accountable and transparent manner and inclusive of the diversity of stakeholders in the ecosystem.
>
> This is a shared responsibility among the community of multi-stakeholder participants in the Internet ecosystem and not one borne alone by ICANN as a singular entity."

The ISPCP suggests that this answer falls short of the hope expressed by the SSR-RT. The proposal addresses vague language with different vague language and does not really clarify the situation.

The ISPCP would answer this question with another – what does it mean, "to actively engage with stakeholders"?

In essence, the SSR-RT seems to be asking for a better definition of the roles and responsibilities of ICANN (the corporation and the community) in this context. It is our view that the proposed language could go further in clarifying that understanding. A much more useful definition would include statements describing the role, responsibility, accountability and authority of all the participants in the process: ICANN the corporation, members of the ICANN community and others.

The proposed statement could be further improved by replacing the phrase "shared responsibility among the community" with some underpinnings as to what that shared set of responsibilities are, and who is accountable for them.

The ISPCP understands that ICANN (corporation or community) cannot arrive at the final definitions of these things alone and commends the sensitivity to the feelings of all the other participants. But this sensitivity is bordering on hesitancy and the ISPCP suggests a bolder and more collaborative approach. The current confusion about "who is responsible for what" in the SSR arena may not just be a boundary

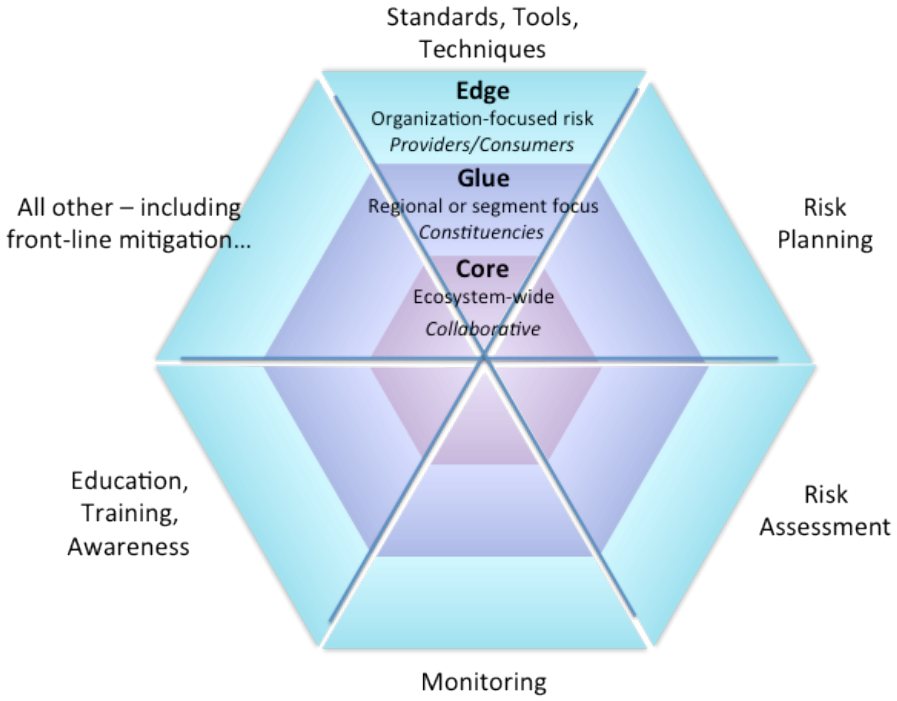
dispute between participants and providers of identifier services, it may be opening up vulnerabilities in the name and number systems themselves.

The ISPCP would like to encourage the leaders of this effort to make another attempt, preferably in collaboration with other members of the ecosystem, at writing this statement – with the goal of producing one that does a better job of describing who does what and lays out the benefits of that approach.

Here is a partial list of organizations that probably need to be a part of that conversation:

- Backend registry providers
- ccTLD registries
- CERTs
- DNRMF
- DNS-OARC
- DSSA
- ENISA
- FIRST
- gTLD registries
- IANA
- ICANN Security Team
- ICANN SOs and ACs
- IETF
- ISOC
- Network Operator Groups
- NRO
- RSAC
- SSR-RT
- SSAC

Here is a diagram that appears in the recently released DSSA phase-1 report that highlights the number of different roles that exist in the DNS SSR ecosystem. It is likely that a similar model applies to the numbering-system community.



Perhaps by building models like this, finding agreement as to who is responsible and accountable for what part of it, identifying the benefits of doing these things well,

and then rewriting this statement of Role and Remit based on that agreement, we can do a better job of leveraging the collective talent, resources and will of the community and clarify what roles ICANN (the corporation and the community) should play.

3.2. What are the limits of that coordination role?

The answer proposed in the Draft Statement is:

> "Responsibilities that lie outside ICANN's role in SSR include:
>
> - ICANN does not play a role in policing the Internet or operationally combatting criminal behaviour;
> - ICANN does not have a role in the use of the Internet related to cyber-espionage and cyber-war;
> - ICANN does not have a role in determining what constitutes illicit conduct on the Internet."

ICANN the corporation **does** have an operational role in all three of these areas if, for example, the infrastructure it manages were to come under attack during cyber-warfare or a criminal assault. ICANN the corporation **does** have a role in policing the behavior of its contracted parties. ICANN the community **does** have a role in developing and disseminating knowledge and techniques that may help front-line providers (such as ISPs) understand current best practices and respond to similar SSR issues.

ICANN, the corporation and the community, tends to self-limit its roles – sometimes consciously, sometimes not. This often results in a "best efforts" posture rather than one that actually addresses and fulfills a mission. Here are two recent examples:

- **The GNSO Council's treatment of the RAP-WG recommendation to build more uniform reporting into the policy process (Uniformity of Reporting)**

  Here is an example of self-limiting behavior by the community that produces best-efforts results rather than optimal ones. A GNSO working group recommended a community-wide effort be launched to explore how to provide data collection and reporting for all ICANN policies, rather than the much narrower information collected by ICANN Compliance. Data-collection is a crucial part of the "plan, do, check, act" security cycle and needs to be addressed in any complete statement of ICANN's remit.

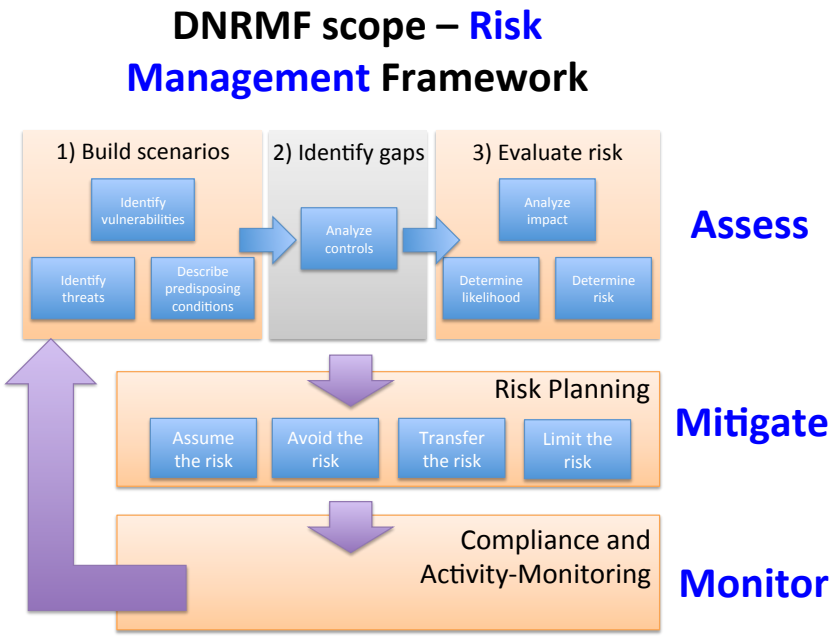
  However, the GNSO Council is having a very hard time figuring out how to act on this recommendation because it falls outside their policy development process (PDP). This may well result in the recommendation being dropped

off the agenda, even though it received unanimous consensus from the members of the working group.

- **The recent staff assessment for the Board DNS Risk Management Framework Working Group (DNRMF)**

  This is a good example of self-limiting behavior by ICANN the corporation. In this case the working group is chartered by the Board (18-March, 2011) to "oversee the development of a risk management framework and system for the DNS as it pertains to ICANN's role as defining in the ICANN Bylaws."

  Here is another diagram from the recently released DSSA report, which lays out a textbook view of the components found in a typical "risk management framework."



  Yet the Staff Assessment for the DNRMF working group focuses it's List of Tasks on the first of these broad areas, risk assessment, and makes no mention at all of the risk planning, monitoring, mitigation and compliance activities that are crucially important for effective risk management. Here then is another way in which ICANN self-limits its role and remit.

What is clear is that while this proposed language is useful in defining sharp boundaries between what is inside and outside ICANN's corporate and policy purview it, like the preceding proposal, needs refinement. The process of arriving at that more-nuanced scope boundary would again benefit from benefits-driven collaboration with other participants in the ecosystem.

In the final analysis, the current proposal is too sharp in its statement of what is outside ICANN's remit. Its crisp definition again leaves questions of role, responsibility, authority and accountability unanswered – which creates tension among the participants in the ecosystem, and ultimately may expose vulnerabilities for participants and end-users of the naming and numbering systems.

3.3. What does it mean to ensure the security and stability of the global Internet's unique identifier systems?

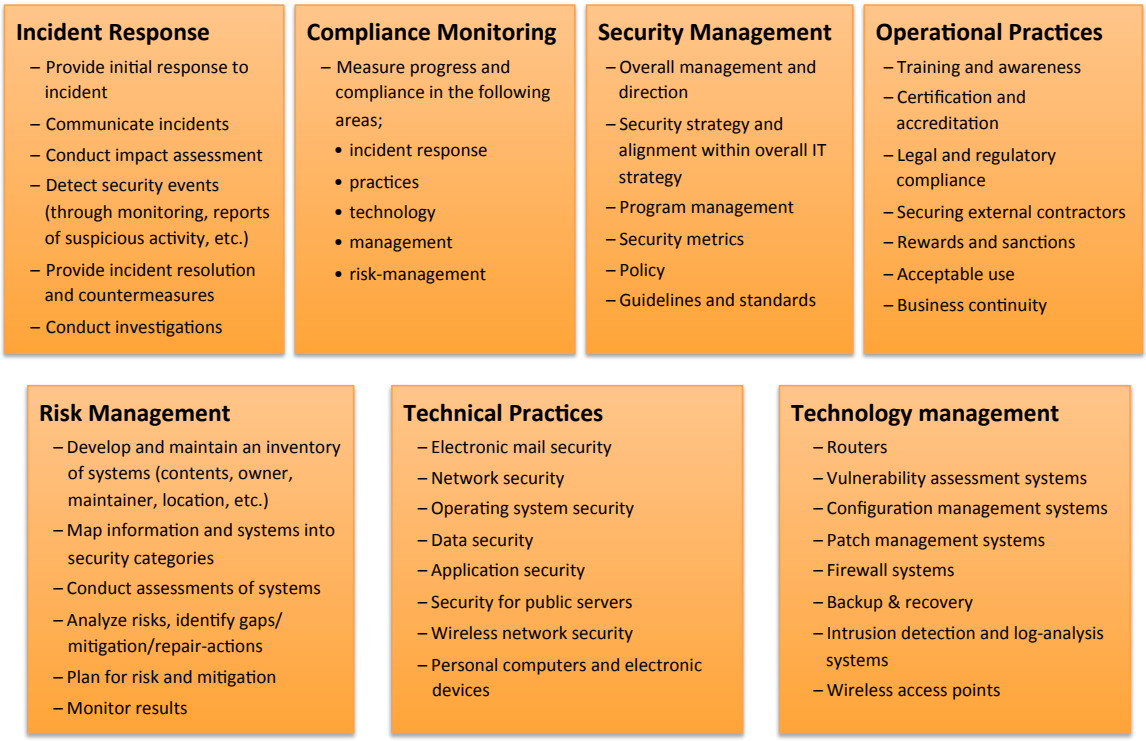
The use of the word "ensure" in ICANNs mission has undoubtedly provided the opportunity for a number of difficult discussions over the years. The fragment of the mission statement in which that word appears reads as follows:

> "ICANN acts within its Bylaws to support a multi-stakeholder model collaborating to ensure the security, stability and resiliency of the Internet's unique identifiers."

If we use a strong definition of the word ("guarantee" or "vouch" for example), this is a very good illustration of a classic management mistake – assigning responsibility without corresponding authority. Neither ICANN the corporation nor some amorphously defined "multi-stakeholder model" currently has the authority needed to **guarantee** the security and stability of the naming and numbering systems. The remedy to this management mistake is simple in theory, although much harder in practice. Either grant the authority or remove the responsibility.

An alternate definition of "ensure" (words such as "ascertain" "verify" "check"), describes a role that is somewhat more consistent with the current posture of ICANN (the corporation). However this verification role may fall short of the assurance that the framers of the mission statement had in mind when they wrote it. And ICANN (the corporation and the community) may need to step up its efforts even to meet this lower standard.

The following diagram (again from the recently released DSSA report) illustrates the typical array of security management functions found in information technology delivery organizations as they maintain the SSR of their systems. This is only provided as an example of a toolset that ICANN the community could describe, promote and verify if it chose to.



Once again the distinction needs to be drawn between the corporation and the community. At a minimum, the corporation should be able to deliver all of these functions as a part of its direct infrastructure-delivery responsibility. And an internal audit function ought to be able to verify that they are deployed effectively within that narrow responsibility. But this is only the operational subset of responsibilities carried by ICANN the corporation.

ICANN also has contracts with a various parties and those contracts provide the basis, indeed the requirement, for ICANN the corporation to play a strong role in defining and enforcing the policy questions that arise from this list of responsibilities.

The ICANN community, on the other hand, may be uniquely positioned to collaborate in improving these SSR among its members. Indeed it is this unique role may be part of the remit that the original framers of ICANN's mission statement had in mind when they drafted it.

The language proposed in this Role and Remit uses words like "coordinate," "collaborate," "facilitate" and "engage" rather than words like "assure" or

"guarantee," or even the softer words like "ascertain" or "verify" as discussed above. The concern is that this makes collaboration the end rather than the means. ICANN is not charged with being a collaboration platform – its mission is to help ensure the security and stability of the naming system. Collaboration is a powerful tool to meet that responsibility, but it is only one of many – including audit and compliance.

There also needs to be data in order for ICANN (corporation and community) to be able to fulfill a narrow "verification" mission, and data would also be extremely helpful to the broader community as they collaborate towards a broader "guarantee" goal. In order to have that data there needs to be an agreement as to which data is needed, who will provide it, what benefits would accrue, and good mechanisms for collecting and sharing that data in a secure way. This presents yet another "role, responsibility, accountability, authority" puzzler to sort out.

The ISPCP hopes to see stronger and clearer language in the future – language that weaves together both the "guarantee" and "verify" definitions of the word "ensure" in ways that are useful and agreeable to all the parties who must collaborate effectively to deliver stable, secure and reliable identifier systems.

4. Comments in response to SSR-RT Recommendation 3

Recommendation 3 of the SSR-RT report states "ICANN should document and clearly define the natures of the SSR relationships it has within the ICANN community in order to provide a single focal point for understanding the interdependencies within the organizations." Here are the specific questions being posed for public comment on this topic.

4.1. What is ICANN's coordination role with root server operators?

4.2. Should ICANN develop a process for transitioning a root server should a root server operator cease that role?

4.3. What is ICANN's scope of responsibility for addressing an attack against root servers, or "against the DNS" in general?

The ISPCP is reluctant to answer these questions. It is our view that there is higher-level work to be done first, and that proposing answers prior to that work being completed is at best likely to ill-informed and may border on irresponsible. The SSR-RT report illustrates how complex these questions are, and proposes a process to start answering them. Here is a relevant quote from that report:

> "The IETF and the root server operators came into existence long before ICANN existed.
>
> "When analyzing the Supporting Organization, Advisory Committees and relationships as part of a review, it quickly becomes clear that there are

interwoven dependencies. These are often complex to analyze and sometimes difficult to understand as to the exact nature of each agreement or relationship. Often the agreements span back over many years and are documented across multiple documents and versions.

"It would be helpful for ICANN to bring together all relevant agreements, whether formally contracts, or an agreed understanding, in order to clarify for the wide community what the relationship is between ICANN and the other party. This would facilitate understanding as well as allowing a closer look at the effectiveness and applicability of each relationship to the overall SSR mission."

The ISPCP supports this approach as a very useful first step. Once this preliminary fact-finding and analysis is completed, the ISPCP would also support a collaborative effort to decompose the jobs that need doing and then agree to a mutually acceptable division of labor between the parties involved. It would be very helpful if this collaboration could clearly spell out specific roles, responsibilities, authority and accountability as described in section 3 above.

Only then is it likely to be appropriate for the community to weigh in on questions such as the ones posed in this part of the Request for Comment, as they are basically operational questions that may indeed have obvious answers once all the parties know, and agree on, who was broadly responsible for what.