Comments of the Registries Stakeholder Group

Expedited Registry Security Requests (ERSR)

November 16, 2009

The Registries Stakeholder Group of the GNSO (RySG) appreciates the opportunity to provide these comments in the proceeding, Expedited Registry Security Requests (ERSR) process. The comments that follow represent a consensus position of the RySG as further detailed at the end of the document.

In the current version of the ERSR process, a security incident is defined as follows:

- Malicious activity involving the DNS of scale and severity that threatens systematic security, stability and resiliency of a TLD or the DNS;
- Unauthorized disclosure, alteration, insertion or destruction of registry data, or the unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards;
- An occurrence with the potential to cause a temporary or long-term failure of one or more of the critical functions of a gTLD registry as defined in ICANN's gTLD Registry Continuity Plan

The RySG believes that the phrase within the second bullet point "…unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with all applicable standards" is too broad. That language potentially takes in a wide variety of small and large security incidents on the Internet, such as malware that has infected individual user systems, phishing on compromised Web sites, unauthorized access or data breaches on third-party networks, etc. These do not usually involve registries beyond the fact that services operating on a domain name may be involved. Registries do not have any technical ability to mitigate many of those kinds of problems, and the ERSR itself is designated for serious incidents that threaten the systematic security, stability and resiliency of a TLD or the DNS itself.

The RySG proposes that the second bullet point be changed to read:

> "Unauthorized disclosure, alteration, insertion or destruction of registry data, or the unauthorized access to or disclosure of **registry** information or resources on the Internet by **registry** systems operating in accordance with all applicable standards;" [emphasis added]

The current language appears to come from the Registry Services Evaluation Policy (RSEP) definition of an "effect on security" that is found in all Registry Agreements. The RSEP is intended to ensure that new registry services will not negatively impact security, and that they will be compliant with applicable relevant standards. That context is missing from the ERSR. When pasted into the ERSR without that context, the language has become more expansive; it could be interpreted so broadly as to cover incidents that are not contemplated as within the scope of the ERSR.

The RySG also proposes the following in the third bullet:

replace "…ICANN's gTLD Registry Continuity Plan"
with "…critical operations of the registry, as defined in the gTLD registry agreements".

The definition in the current Registry Continuity plan is not aligned with the definition of critical functions in the registry agreements. It does not seem wise to depend on a definition that differs from what is in the registry agreements. It also does not seem like a good idea to depend on a definition of a document that is still in draft form.

Both ICANN and the RySG desire that registries function within standards, and that current or future registry services are not the genesis of security problems. We believe that the proposed change in language will help achieve those goals.

RySG Information with regard to these Comments

A supermajority of 12 RySG members supported this statement:

- Total # of eligible RySG Members[1]: 14
- Total # of RySG Members: 14
- Total # of Active RySG Members[2]: 14
- Minimum requirement for supermajority of Active Members: 10
- Minimum requirement for majority of Active Members: 8
- # of Members that participated in this process: 14
- Names of Members that participated in this process:

1. Afilias (.info)
2. DotAsia Organisation (.asia)
3. Dot Cooperation LLC (.coop)
4. Employ Media (.jobs)
5. Fundació puntCAT (.cat)
6. mTLD Top Level Domain (.mobi)
7. Museum Domain Management Association – MuseDoma (.museum)
8. NeuStar (.biz)
9. Public Interest Registry - PIR (.org)
10. RegistryPro (.pro)

[1] All Registries are eligible for membership in the RySG upon the "effective date" set forth in the Registry's agreement with ICANN. (Article III, Membership, ¶ 1). The RySG Articles of Operations can be found at: <http://gnso.icann.org/files/gnso/improvements/registries-sg-proposed-charter-30jul09-en.pdf>

[2] Per the RySG Articles of Operations, Article III, Membership, ¶ 6: Members shall be classified as "Active" or "Inactive". A member shall be classified as "Active" unless it is classified as "Inactive" pursuant to the provisions of this paragraph. Members become Inactive by failing to participate in a RySG meeting or voting process for a total of three consecutive meetings or voting processes or both. An Inactive member shall have all rights and duties of membership other than being counted as present or absent in the determination of a quorum. An Inactive member may resume Active status at any time by participating in a RySG meeting or by voting.

11. Societe Internationale de Telecommunication Aeronautiques – SITA (.aero)
12. Telnic, Limited (.tel)
13. Tralliance Corporation (.travel)
14. VeriSign (.com,.name & .net)

Regarding the issue noted above, the level of support in the RySG for the statement is summarized below.

1. Level of Support of Active Members:

   1.1. # of Members in Favor: 13

   1.2. # of Members Opposed: 0

   1.3. # of Members that Abstained: 0

   1.4. # of Members that did not vote: 1