ICANN SSR Subgroup Meeting - Follow-up Questions
9-10 October 2017
Los Angeles

ICANN security relating to the security and stability of the DNS

1. Recommendation 9 of the SSR1 report: Can you elaborate on the certification options that were then pursued and whether a roadmap was laid out for what ICANN staff assumed was the appropriate certification and standards to be followed for its operational responsibilities?
2. Deployment of new instances, change management: It sounds like there is a lot of custom process around how you're managing a lot of this. Is the reason why you haven't looked at a more industry-standard process, which is ITIL or something less unique in line with the SSR1 recommendations to move to a more industry-standard, certifiable and auditable method around founding controls, vulnerability management?
3. Given the relative importance of IANA.org, because if you have to reach out to it to do any automated changes to a TLD zone, you have to be able to reach it. I'm wondering how the DNS, what the resiliency is for IANA.org to maintain? Is it given any special attention?
4. Please provide an answer on who administrates IANA-servers.net as well, and any process behind that.
5. Follow-up in the same area: Expanding away from just IANA.org, there is a lot of "critical operations stuff", the GDD portal and some of the other supporting infrastructure. Is that managed just as a general ICANN service or is actual attention given to the supporting infrastructure that sits around the root zone maintenance? And how is that handled or is that just handled as a general ICANN IT service?
6. Dependencies involved to maintain L-Root dependence: Do you track what the secondary dependency is like when there is a domain name that needs to be looked up because GitHub.com or your internal naming infrastructure, does it reach outside whereby at some point, if there was something going on with the root and one of your dependent systems, have you done even just a [packet] trace level or any kind of audit to see what sort of expected or unexpected external dependencies might keep in the case of an event, disaster, or whatever else, keep you from being able to maintain your deployment? Do you know what I'm saying? When you do the tabletops? I can give, probably a specific example. For example, I know ICANN uses OPTA a lot, across a lot of your systems. Do you have where you're logging in to your GitHub instances through OPTA and you have backup procedures to be able to fall back to local user, these type of things where you're not mapping necessarily the direct infrastructure, but the supporting infrastructure that is around it?
7. I see [inaudible] enabled and in the world of protocol abuse, in future I think may be abused to launch any kind of cyber attack, so what's the stand on ICMP enabled? Do each of the servers allow ICMP packets in?

8. Several months ago, some DNS attacks and defense occupied a lot of attention with attacks taking out some of the major root zone servers. How do you feel the state of things are and can you elaborate about steps that were taken, both by ICANN and by the community in response to that? I’m referring specifically to the attacks that jeopardized some of the root servers and the community response to that and ICANN as well.
9. Is there any meta data surveillance part in the DNS traffic?