1. **SSAC MEETINGS.** Attended SSAC Meeting on 14Mar13.

2. **SSAC WORK PARTIES.** I am currently participating in two SSAC Work Parties:
   - Identifier Abuse Metrics Work Party – apology for meeting on 13Mar13
   - DNS Abuse Work Party – attended meetings on 28Feb13 and 21Mar13

3. **RELEASE OF SAC057 - SSAC ADVISORY ON INTERNAL NAME CERTIFICATES.** SAC057 was publicly released on 15Mar13. Some brief notes in which I attempted to encapsulate the 18 pages into a very brief summary were prepared for the ALAC ExCom and these are appended below.

4. **RELEASE OF FY14 SECURITY, STABILITY AND RESILIENCY FRAMEWORK.** The ICANN Security Team released the FY14 SSR Framework for public comment on 6Mar13. I have drafted a suggested ALAC Statement on this document and it is posted on the At-Large Workspace.

5. **DSSA WORKING GROUP.** In hibernation until the ICANN Meeting in Beijing. In a related issue, the contractors engaged by ICANN to develop a DNS Risk Management Framework, Westlake Governance, have posted their presentation on the ICANN Beijing schedule.

### NOTES FOR ALAC EXCOM ON SAC057 – SSAC ADVISORY ON INTERNAL NAME CERTIFICATES

**Background**

During its annual workshop on 14 – 16 November 2012, a SSAC member highlighted a Certificate Authority (CA) practice that, if widely exploited, could pose a significant risk to the privacy and integrity of secure Internet communications and impact the new gTLD program. Recognizing the seriousness of this issue, a SSAC work party developed advice that was formally delivered to the ICANN security team on 31 January 2013.

Due to the sensitive nature of this issue, the SSAC did not follow its customary publication procedures; instead, the SSAC delivered a briefing and an interim advisory to the ICANN security team during January. The ICANN security team took immediate action to prepare mitigation options. Public release of the SSAC advisory was withheld until these mitigation actions had been successful.

**Findings**

The vulnerability identified relates to the issuing of digital certificates by a Certificate Authority (CA) for an internal name i.e. a domain or IP address that is part of a private network. These are certificates that contain names “that are not currently resolvable using the public DNS” and are assumed to be for private use only. These internal names are not allocated to any specific organization and CAs cannot verify them because it is not possible to look up who owns them. When determining whether a certificate application is for internal use or not, CAs often rely on the list of currently delegated TLDs and not, for instance, against the list of the TLDs applied for in ICANN’s new gTLD program. The exact number of internal name certificates that end in an applied for new gTLD is not known.

The practice for issuing internal name certificates allows a person, not related to an applied for TLD, to obtain a certificate for the TLD with little or no validation, and launch a man-in-the-middle attack more effectively. If an attacker obtains a certificate before the new TLD is delegated, he/she could surreptitiously redirect a user from the original site to the attacker site, present his certificate and the victim would get the TLS/SSL “lock icon”.

The Certificate Authority (CA)/Browser forum was aware of this issue and had requested its members to stop this practice by October 2016. The vulnerability window to new gTLDs was therefore at least 3 years.

**Outcome**

On 23 January 2013, the ICANN security team scheduled a preliminary teleconference with the Certificate Authority and Browser Forum Chairperson to alert him to this issue. Recognizing its seriousness, the Chairperson invited ICANN to brief the CA/Browser Forum members in its upcoming annual meeting on 5 February 2013. As a result of this meeting, the CA/Browser Forum advanced Ballot 96 on new gTLDs. The ballot called for CAs to stop issuing certificates that end in an applied-for-gTLD string within 30 days of ICANN signing the contract with the registry operator, and revoke any existing certificates within 120 days of ICANN signing the contract with the registry operator [NOTE: the original CA timeline for not issuing internal name certificates was 1 July 2015, with revocation starting on 1 October 2016]. On 20 February 2013, the CA browser forum passed Ballot 96.

**Comment by SSAC Liaison**

The outcome of these efforts is a significant success and will mitigate a security vulnerability for all internet users. It reflects excellent cooperation between the SSAC work party members, the ICANN security team, and the CA/Browser Forum.