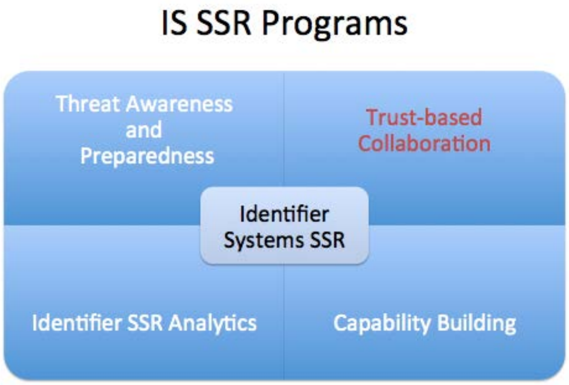
Identifier Systems Security, Stability, and Resiliency Programs

Dave Piscitello, VP Security and ICT Coordination

This program note describes one of four IS SSR programs, **Trust-based Collaboration**.

Projects in this program area fall into two categories:



1. *Global Cybersecurity cooperation*. The initiative will coordinate closely with GSE to contribute cybersecurity subject matter expertise in ICANN's engagements with private sector, civil society, or governments.

2. *Global Security & Operations*. SMEs in the department participate in the daily interaction with the global infosec, DNS operations and law enforcement communities. This form of interaction serves as an information feed for all participants in these trusted communities, keeping them constantly appraised of emerging threats, responses, trends, and new tools or methods of analyzing malicious or criminal misuses of the DNS.

The purpose of lending competencies to the community and engaging in trust-based collaboration is to grow trust for ICANN among organizations that are not part of the ICANN community and from this trust, encourage them to participate in ICANN's multi-stakeholder consensus policy development. Team members accept invitations to engage from ICANN Global Stakeholder Engagements, ICANN Speaker Bureau or directly from inviting organizations.

Many invitations come from governments or agencies, including European Commission, Global Cybersecurity Capacity Centre, Organization of American States, and the Inter-American Telecommunications Commission, OECD, and the Commonwealth Secretariat. We also visit global and national law enforcement agencies (Europol, Interpol, UK National Crime agency), and US federal agencies (DoJ, FBI, DHS, DEA, FDA).

Staff are also active in information security research and collaboration communities such as the APWG, MAAWG, ISOI, DNS-OARC, national and regional CERTS, regional operations groups (SG.NIC, MENOG, NANOG, LACNIC, CR.NIC, TR.NIC) or other similar communities where ICANN's participation is sought or valued.

Examples of activities that fall within trust-based collaboration include:

Assistance with suspending malicious DNS or domain registrations. The Security Team assists law enforcement or private sector OPSEC actors in corroborating or complementing data associated with malicious domain registrations or name resolution investigations. Certain of these fall under contractual compliance and we collaborate with ICANN compliance for these. For global security risks, we facilitate communications between LEA/OPSEC and domain registrars or registries.

Improving global DNS and domain registration abuse analysis. Security team members lend DNS and cybersecurity expertise to the LEA/OPSEC communities to help improve the kinds, quality and accuracy of threat intelligence associated with DNS and domain registrations.

DNSSEC status and public root key rollover testing. A security team member supports a DNSSEC Status Page and a resource page that supports public root key rollover testing. The Status page has helped to provide early notifications of signing issues since 2010. The ad hoc testing program sends email alerts to key ICANN staff and the technical contact of the affected TLD as listed in the IANA database when DNSSEC signatures are about to expire.