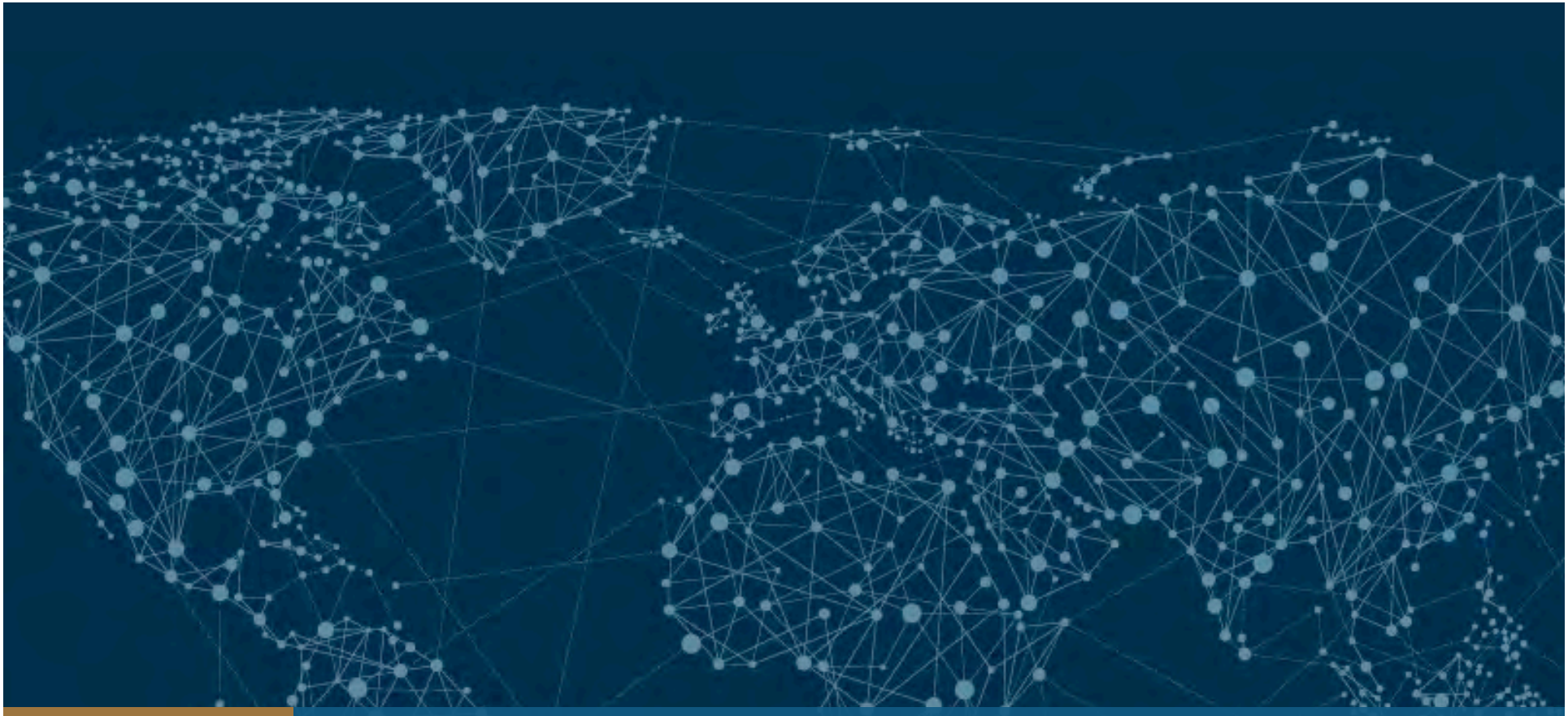


Supporting a Healthy and Resilient Internet

Save Vocea| Pacific ICT Officials Meeting, Tonga | 18 June 2015

Internet Corporation for Assigned Names and Numbers (ICANN)

1. **Dedicated to keeping Internet Secure, Stable and Interoperable**
2. **Formed in 1998 as a not-for-profit public-benefit cooperation**
3. **Follows multistakeholder model**

Functions that ICANN Coordinates

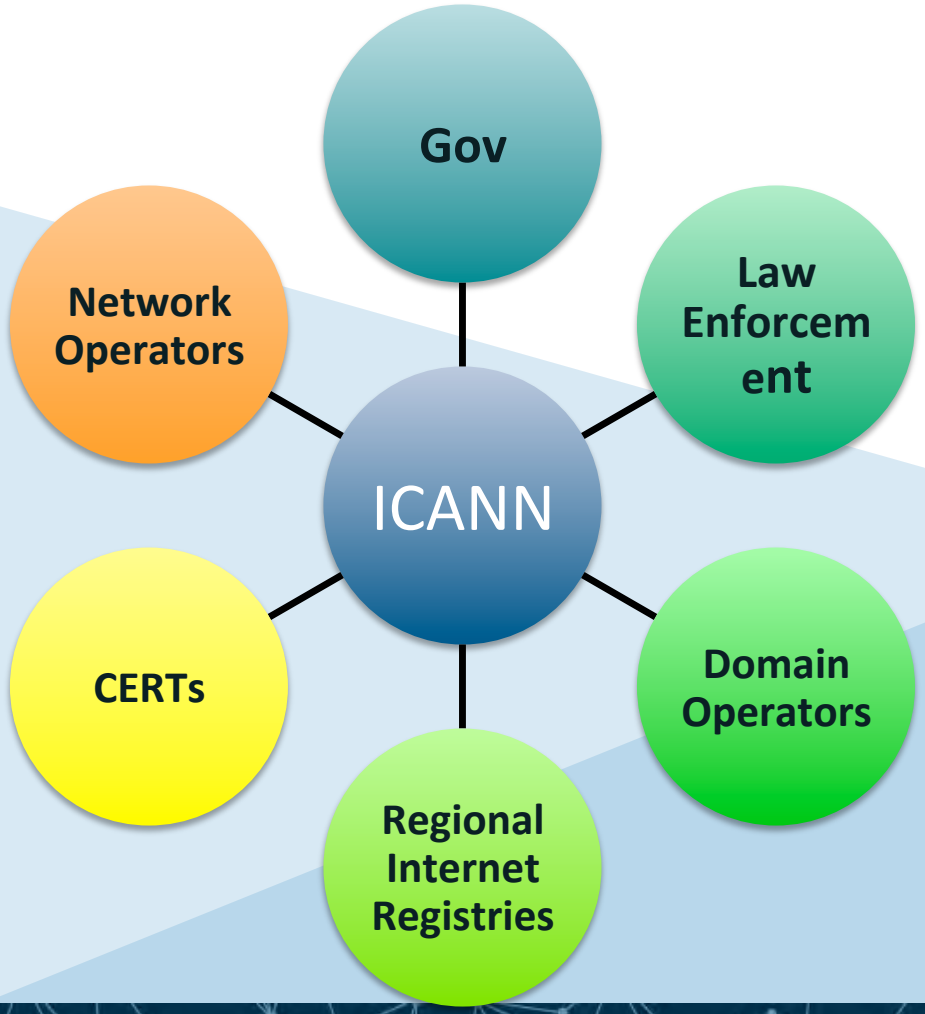
- Domain Name System (DNS)
- Internet Protocol (IP) Address and Autonomous System Number (AS) Allocation
- Protocol-Parameter Registry
- Root Server Systems
- Generic Top-Level Domain Names (gTLD) system management
- Country-code Top-Level Domain Name (ccTLD)
- Time Zone Database Management

Unique Identifiers and SSR Need

- SSR – Security, Stability and Resiliency
- Misuse of and attacks against the DNS and global networks challenge overall unique identifier security
  - Affect the broad range of users, individuals, businesses, civil society, governments etc.
- Security in the context of the Internet's unique identifiers should be addressed through a healthy Internet ecosystem.
  - an Internet that is sustainable or healthy, stable and resilient

Security, Stability, & Resiliency (SSR) A key pillar of ICANN

The Internet – our "Network of Networks"

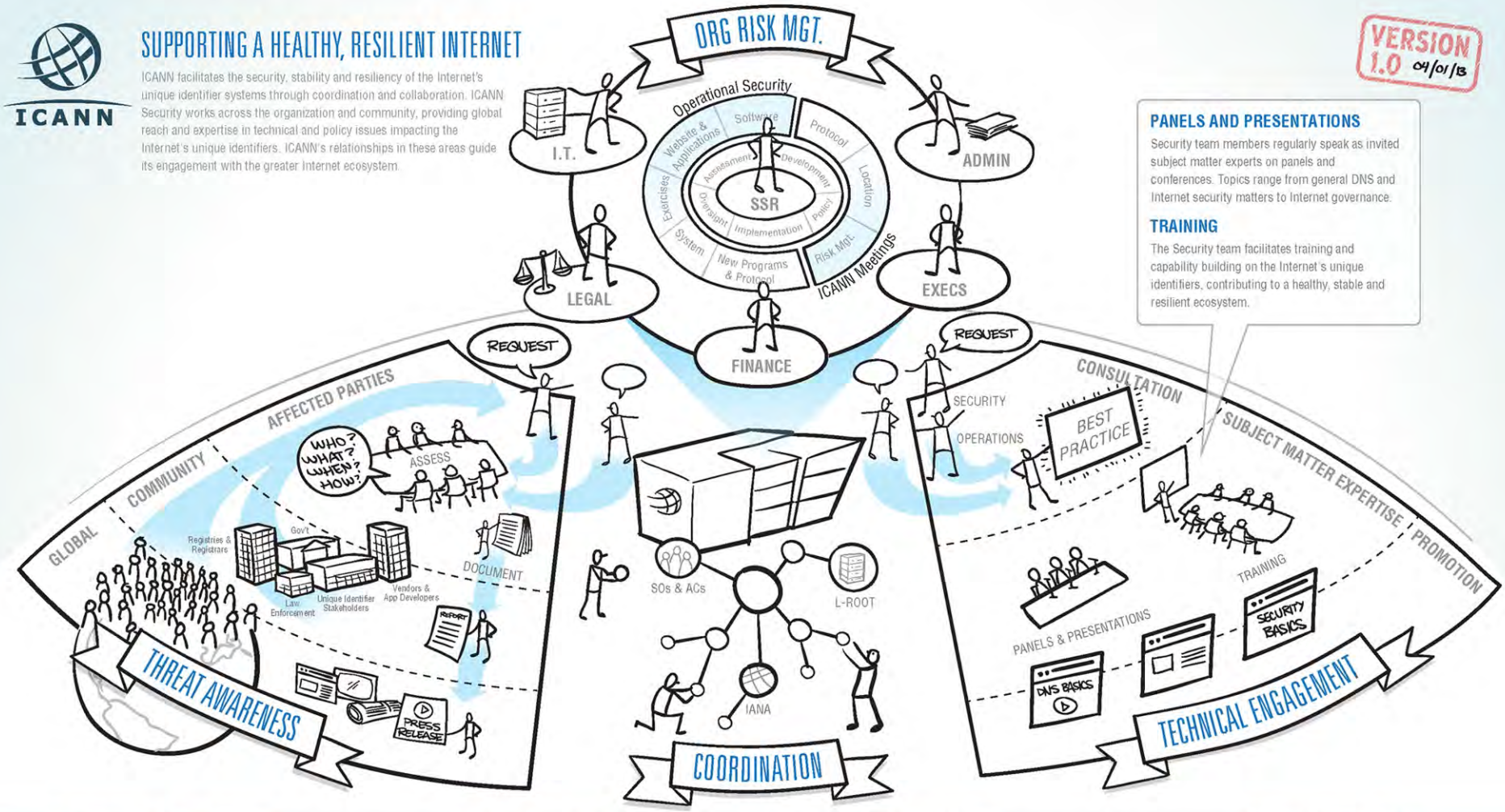


- Threat Awareness and Response
- Trust-based Collaboration
- Capability Building
- Identifier SSR Analytics

SUPPORTING A HEALTHY, RESILIENT INTERNET

ICANN facilitates the security, stability and resiliency of the Internet's unique identifier systems through coordination and collaboration. ICANN Security works across the organization and community, providing global reach and expertise in technical and policy issues impacting the Internet's unique identifiers. ICANN's relationships in these areas guide its engagement with the greater Internet ecosystem.

VERSION 1.0 04/01/13



PANELS AND PRESENTATIONS

Security team members regularly speak as invited subject matter experts on panels and conferences. Topics range from general DNS and Internet security matters to Internet governance.

TRAINING

The Security team facilitates training and capability building on the Internet's unique identifiers, contributing to a healthy, stable and resilient ecosystem.

COORDINATE & COLLABORATE

The Security team is regularly invited to speak with community stakeholder groups, and facilitates activity with ICANN's Supporting Organizations and Advisory Committees.

PUBLICIZE & PROMOTE

The Security team provides thought leadership in the form of white papers, blog posts and the annual Security, Stability & Resiliency Framework for ICANN.

Team members represent ICANN at various conferences and events worldwide, speaking on cybersecurity and governance, the Internet's unique identifiers and ICANN.

CONSULT & ADVISE

The team contributes to scenarios for global cyber exercises, provides advice on operational practices such as with the root server community and DNS technical community.

REVIEW & COMMENT

The team regularly provides input into policy development processes, comments on protocols and open standards managed by others in the Internet ecosystem.

Root Servers to benefit Internet Stability and Resiliency

- Root server nodes keep Internet traffic local and resolve queries faster
- Make it easier to isolate attacks
- Reduce congestion on international bandwidth
- Redundancy and load balancing with multiple instances
- ICANN is the L-Root Operator

L-Root presence

- Geographical diversity via Anycast
  - Around 160 dedicated servers
  - Presence on every continent
- On normal basis 15 ~ 25 kbps
  - Approx. 2 billion DNS queries a day
- We are supporting root server deployment in countries
  - Contact ICANN staff in the region

L-Root anycast server locations

Making the DNS Secure

- A computer sends a question to a DNS server, like “where is www.example.org?”
- It receives an answer and assumes that it is correct.
- There are multiple ways that traffic on the Internet can be intercepted and modified to give a false answer.

How can bad guys attack the DNS?

Attack	Description
Cache Poisoning	Dupe a resolver into adding false DNS records to its cache (example: basic cache poisoning)
Indirection attack	Malware can also poison a client computer's /etc/hosts file (example: DNSChanger)
Distributed Denial of service (DDoS) attack	A resource depletion attack where 1000s of bots send DNS queries to a target NS
DDoS amplification (reflection) attack	1000s of bots issue queries that evoke a very large response message, they all "spoof" the address of a targeted name server,and the targeted NS is flooded with very large DNS response messages requested by the compromised computers
Exploitation attacks	A bad guy discovers a software flaw that causes DNS server software to fail or behave in an unintended way
Redirection (wildcarding, DNS response rewriting)	Instead of a *Name Error* (NXDOMAIN), a name server or resolver returns a response it chooses

ICANN strongly supports DNSSEC

- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).
- DNSSEC infrastructure deployment has been brisk but requires expertise. Call for ccTLD registry and industry to implement DNSSEC

How about Registrations?

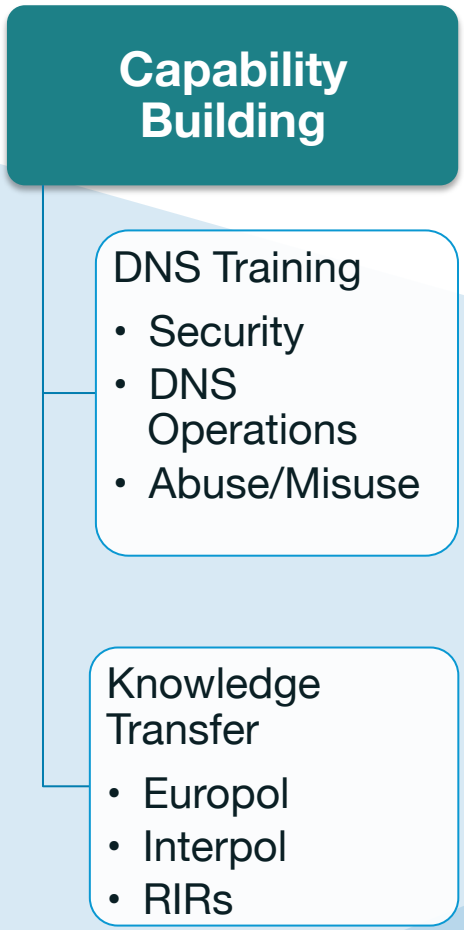
Importance of WHOIS from a Security point of view

+ whois.icann.org
+ Registration Data Directory Service
  - Database containing records of information
+ Verification of records
  - Sponsoring Registrar
  - Domain Name Servers
  - Domain Status
  - Creation/Expiry Dates
  - Point of Contacts
  - DNSSEC Data

IPv6 and Security

- ICANN supports IPv6
  - Mobile Internet, IoT, Smart Nations etc.
  - Partner to promote awareness
  - Capacity building with community
- Be aware
  - When you are running IPv6 the device is accessible via IPv6
  - Interface, Routing filters and firewall rules already present in IPv4 **must** be replicated for IPv6
  - Failure to protect the device after enabling IPv6 means that it is wide open to abuse through IPv6 transport (Even though the IPv4 security is in place)

SSR Capability Building



- Training and Outreach
  - Security, operations, and DNS/DNSSEC deployment training
    - for TLD registry operators
    - Network Operators / ISPs
    - Enterprises, Corporates etc.
  - Information gathering to identify Internet Identifier Systems abuse/misuse and Investigation Techniques
    - Law Enforcement Agencies
    - CERTs
    - Internet Investigators etc.

Engage with ICANN

Thank You and Questions

Email: <save.vocea@icann.org>
ICANN Website: icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations