Key Issues for ICANN on Security, Stability and Resiliency

ICANN Bylaws – Article 1

"To coordinate, overall, the global Internet's system of unique identifiers, and **to ensure stable and secure operation of the Internet's unique identifier systems**"

An Emergent Construct: Security, Stability and Resiliency

– Security: System ability to limit or protect against malicious <u>activity</u> (e.g. unauthorized system access, fraudulent representation of identity, and interception of communications). Security provides increased user confidence in the DNS

– Stability: System functions in a reliable fashion day-to-day. Stability limits the need for constant adjustment and facilitates Internet usage

– Resiliency: the DNS's ability to effectively respond and recover to a known, desired, and safe state when disrupted (e.g. distributed denial of service). Resiliency is viewed by users as availability, viewed by providers as a combination of detection, response, and recovery processes, and increases consumer confidence in relying on and investing in the Internet over the long-term

Key Decision regarding ICANN's role:
Relative Focus on Stability & Resiliency vis-a-vis Security

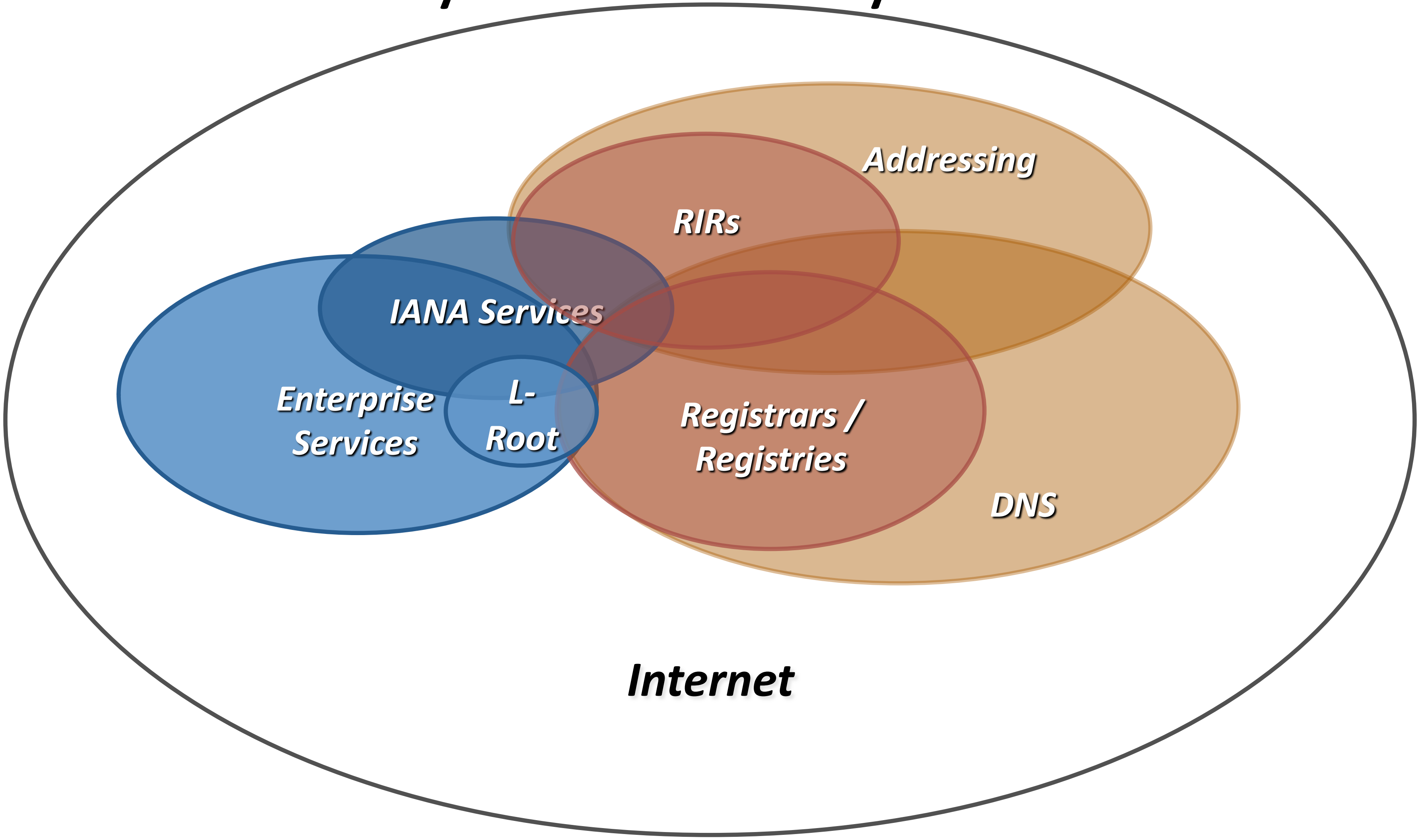
ICANN '09 Operating Plan

- Security Specific Initiatives
  - Establish & engage on ICANN's role in security, stability and resiliency
  - Engage community on DNS risks and mitigation
    - Conduct DNS Security Symposium
  - TLD disaster & attack planning/mitigation
  - Establish ICANN internal security plan

- Security, Stability, Resiliency Related Initiatives
  - Communications to community on ICANN's role
  - IDNs and new gTLDs
  - Strengthen IANA
    - RZM; DNSSec
  - Contract Compliance
    - WhoIs & Data escrow
  - Registry/Registrar Support
    - Failover plan/events

Responsibilities Distributed Across ICANN staff/community

Conceptual Map for ICANN Security, Stability & Resiliency Activities



Key Strategic Issues

- **ICANN Operations**
  - Establish risk management process and determine risk tolerance to disruptions and flaws
  - Ensure progress on initiatives to improve security and stability for RZM, DNSSec, L-root, rPKI and other IANA/ICANN responsibilities
  - Ensure ICANN's internal security programs are sound
- **ICANN and Partners with Contracts/Agreements**
  - How can we optimize addressing security/stability/resiliency concerns through contracts and agreements?

Key Strategic Issues (cont.)

- **Externally with Community**
  - Effectively partnering on Security, Stability and Resiliency
    - With multi-stakeholder organizations to include ISOC, IETF, others
    - With governments related to critical infrastructure protection
  - Establish ICANN Security, Stability and Resiliency role vis-à-vis Internet
    - How to delineate ICANN's specific roles/responsibilities and lead/participate in communities engaging on key issues?
      - In DNS? Role in DNSSec signing of root?
      - In Addressing system? Role in development of rPKI?
    - How to build partnerships with others? Who to partner with?
      - Enhance capacity in the DNS and addressing communities
    - Help delineate Internet-wide challenges and responsibilities

Focus on Stability/Resiliency (eg. DNS not disrupted)
vis-a-vis Security (eg. DNS not misused)?