ICANN Strategic Initiatives for Security, Stability and Resiliency

See postings at http://www.icann.org/en/public-comment/
Background

- Growing risks to DNS security and resiliency
  - Emergence of Conficker; growing domain hijacking
- Community calls for systemic DNS security planning and response
- ICANN commitments under Affirmation of Commitments
- Initiatives called for in ICANN 2010-2013 Strategic Plan

Organizational/resource approaches not predetermined
Initiative #1 – System-wide DNS Risk Analysis; Contingency Planning; Exercises

• Envisaged as a Community-based effort; supported by ICANN
• Risk framework and regular risk assessment
• Root sever information sharing system
  – Based on concerns raised in root scaling study
• Contingency planning based on key scenarios
• Initiate a system-wide DNS exercise program
  – Build on existing efforts
Initiative #2 – DNS CERT
(Computer Emergency Response Team)

• Validated need for standing collaborative response capability to address systemic threats/risks
  – Full-time/global; coordinate existing capabilities; serve all stakeholders especially less resourced operators
• Operational focus determined in engagement with stakeholders and leveraging existing efforts
  – Fostering situational awareness; incident response assistance/coordination; support efforts under Initiative #1

More fully developed DNS CERT Business Case posted along with Strategic Initiatives paper
Way Forward on Security Initiatives

• Seek community feedback
  – Consultation occurred Monday at Nairobi meeting

• Address organizational and funding approaches
On-Going ICANN SSR Activities

• Working closely with FIRST and national CERT community
  – Joint session; 35 students; help set up East African CERT
  – Plan survey on ccTLD – national CERT collaboration
• Continue ccTLD training program in association with regional TLD regional associations
  – Technical training here involved 25 people; 8 cc TLDs
• Still engaged in containing spread of Conficker worm
• Revising *ICANN Plan for Enhancing Internet Security, Stability and Resiliency*; basis for upcoming Affirmation of Commitments review