NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

High Assurance Domain Project

DNSSEC Deployment in the .gov TLD

Scott Rose, NIST

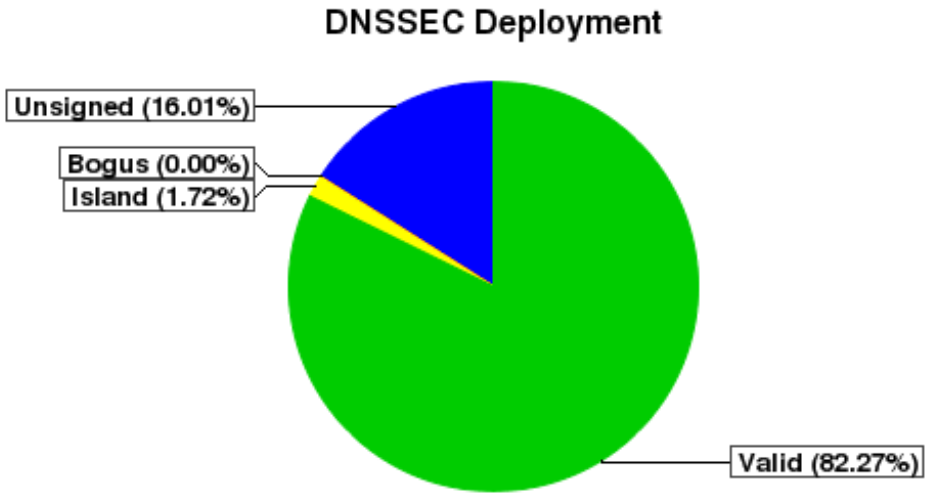
scott.rose@nist.gov

ICANN , Los Angeles CA

Oct 15th, 2014

DNSSEC Deployment Today

- Steady at ~82%
- Far fewer errors seen than four years ago
- Number of Federal .gov delegations shrunk from over 1700 to (currently) 1393.



Lessons Learned

- Set up a monitoring regime to report errors and progress.
- Insure each organization provides up to date POC for zone and/or security operations.
  - Who to contact when things go wrong.
- Encourage automation for applicable DNSSEC operations (e.g. resigning).
- Foster an internal community for admins to discuss issues, ask questions, etc.
  - Closed membership, if necessary

New Issues

- USG IT security policy now requiring DNSSEC validation (Spring 2014)
  - Dept Homeland Security still doing compliance checks.
- Seeing errors due to administrator turnover
  - Admins who did initial deployment leaving, new admins do not know procedures.
- Some agencies battling compliance checks when “moving to the cloud” if provider does not do DNSSEC.