

DNSSEC Deployment

Steve Crocker

Steve@shinkuro.com

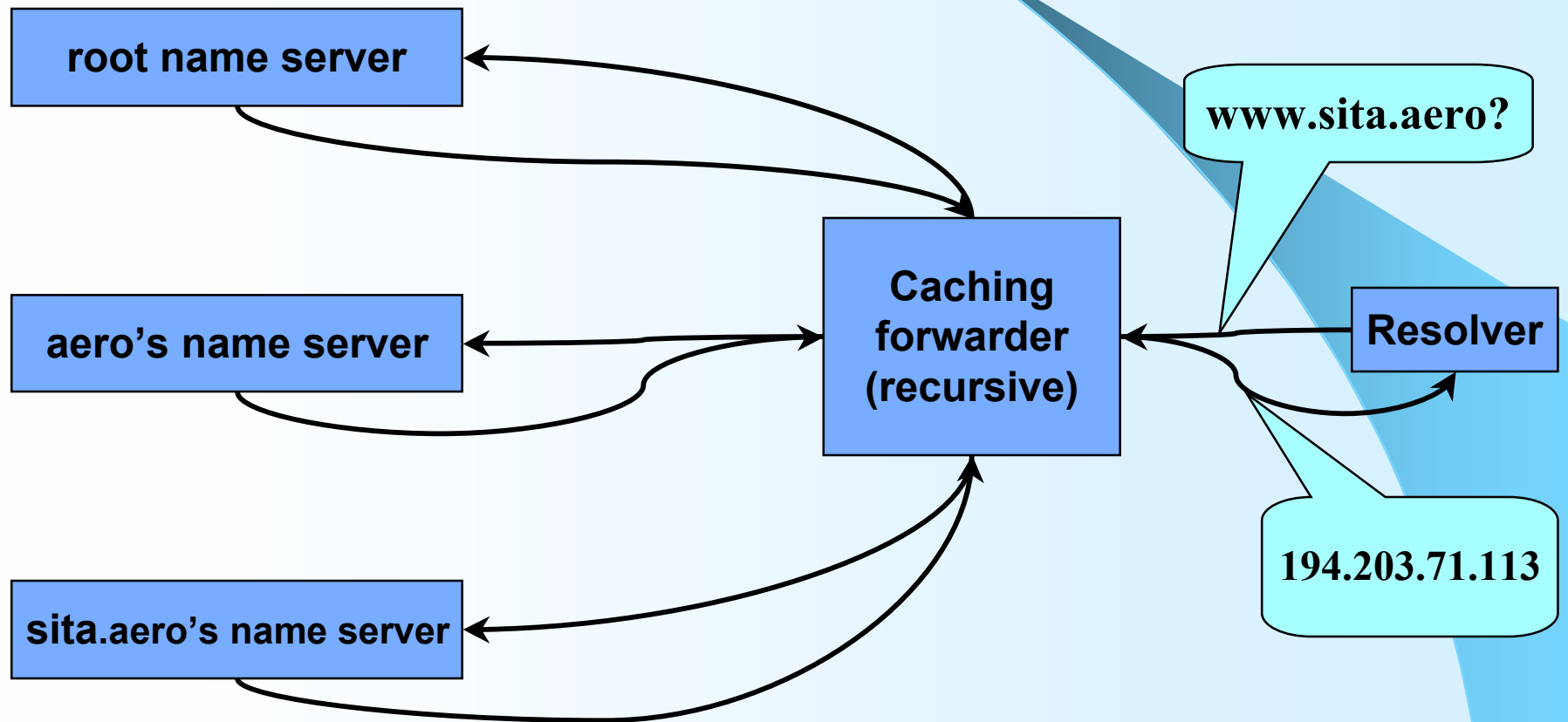
CEO, Shinkuro, Inc.

Chair, ICANN Security and
Stability Advisory Committee

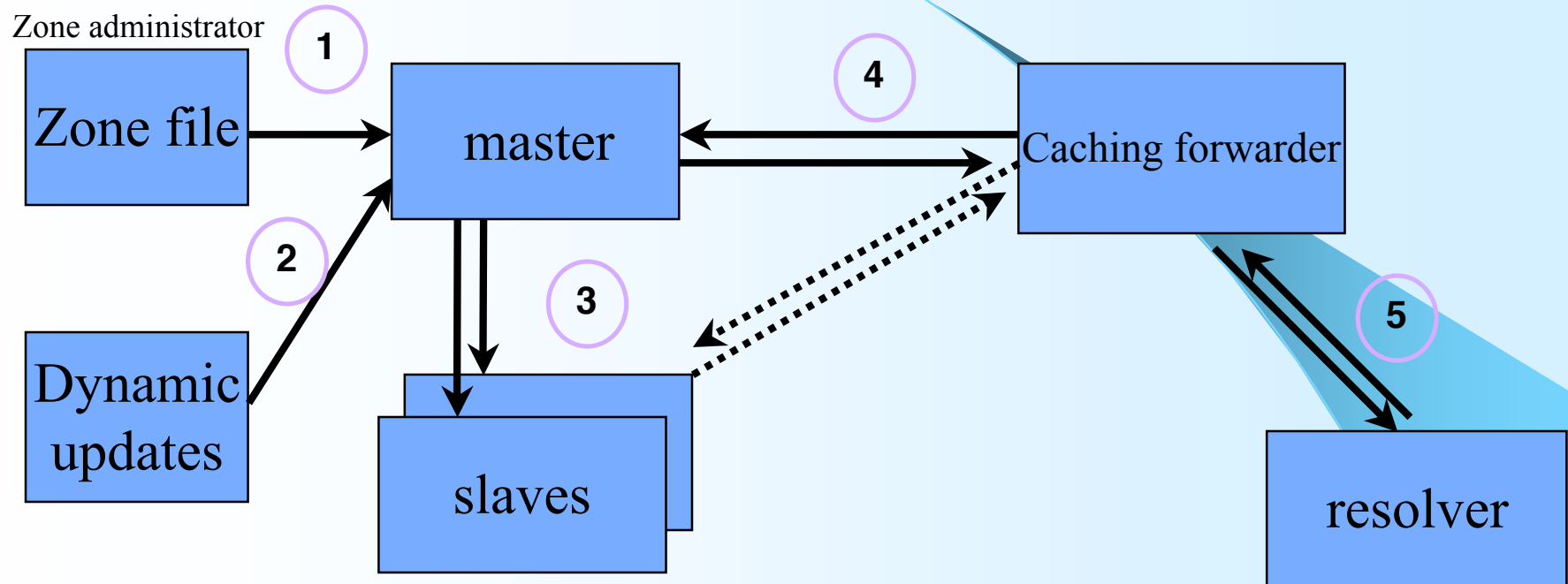
DNS and security

- Quick review of DNS
- Vulnerabilities
- Protection (DNSSEC)
- Deployment Status

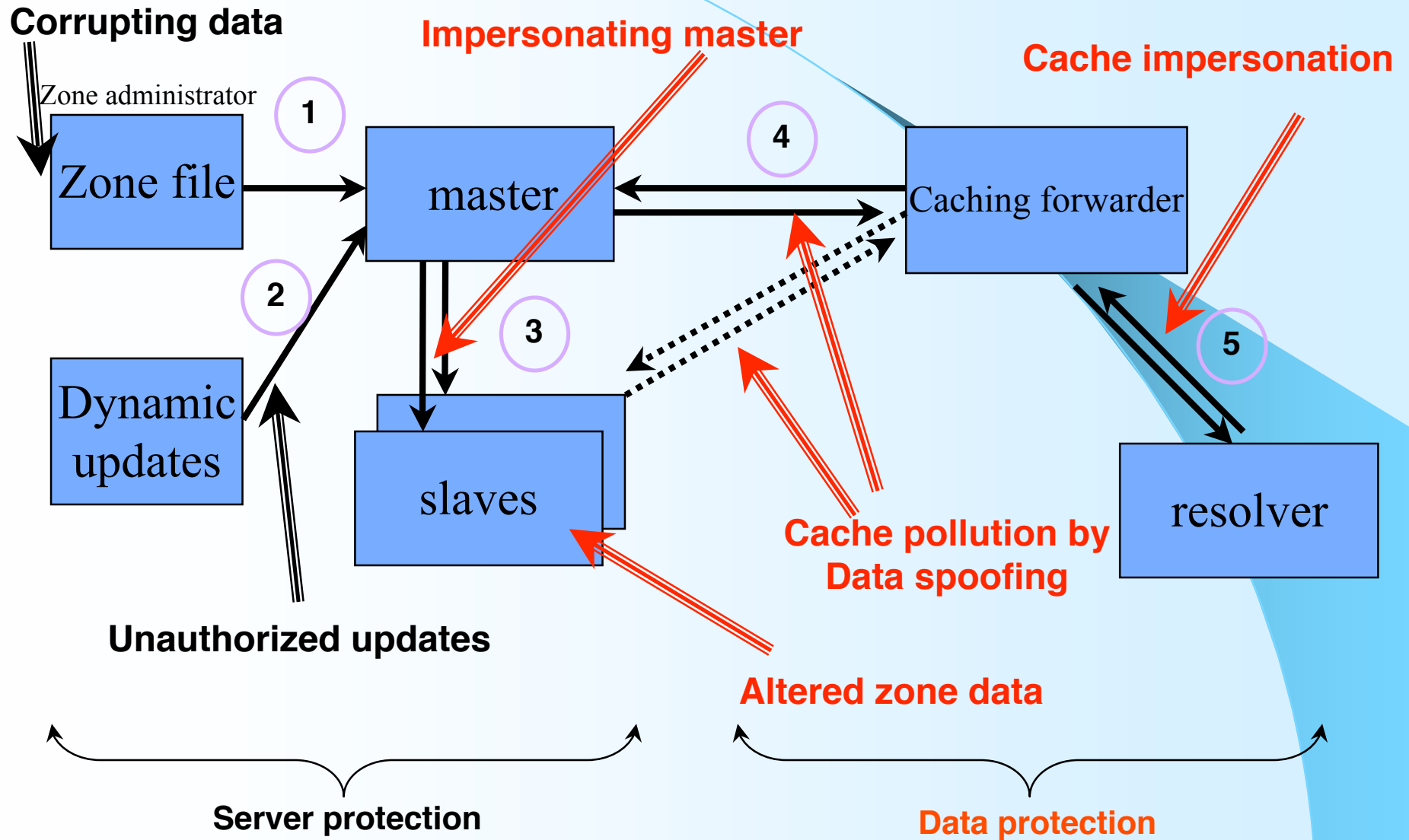
What is www.sita.aero's address?



DNS: Data Flow



DNS Vulnerabilities



DNSSEC Deployment

- Serious deployment activities emerging around the world:
 - <http://secspider.cs.ucla.edu/> tracking ~300 signed zones
 - Europe/RIPE region most active
- U.S. Government taking leadership role in North America
 - DNSSEC requirements included in latest Federal Information Security Management Act (FISMA) requirements
 - Federal Information Processing Standards (FIPS) 199 & 200.
 - Requires incremental deployment of DNSSEC across USG agencies
....
 - and the contractors that provide IT resources/services to them

Dependencies

- Signing vs Checking?
 - Resolvers ask for signed responses
 - Name servers give signed answers
- Top down, bottom up, other?
 - Enterprises
 - Top level domains
 - Root
 - Speciality zones

Tool Dependencies

- Registration process software
 - Registries
 - Registrars
 - IANA, NTIA, VeriSign, Root Server Ops
- Name server software
 - BIND
 - other
- Resolvers
 - Operating systems
 - Browsers
 - Mail

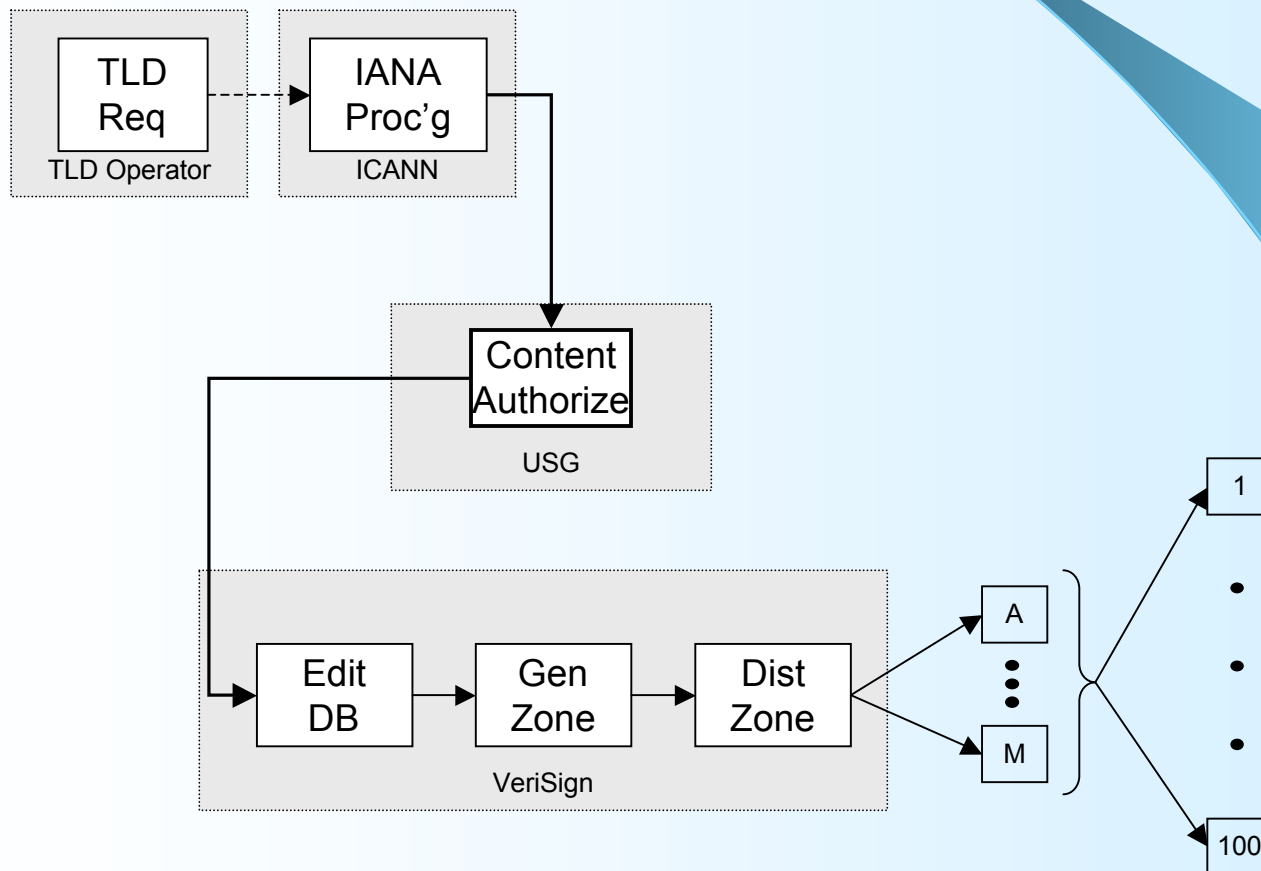
Deployment Status

- Specs and Software exist
- TLD deployment has begun
 - Sweden (.SE) is operational
 - RIPE's portion of in-addr.arpa is signed
 - .ORG, .COM and .NET have test beds
 - Others are in progress (.AERO, et al)
- Browser and desktop will take a while

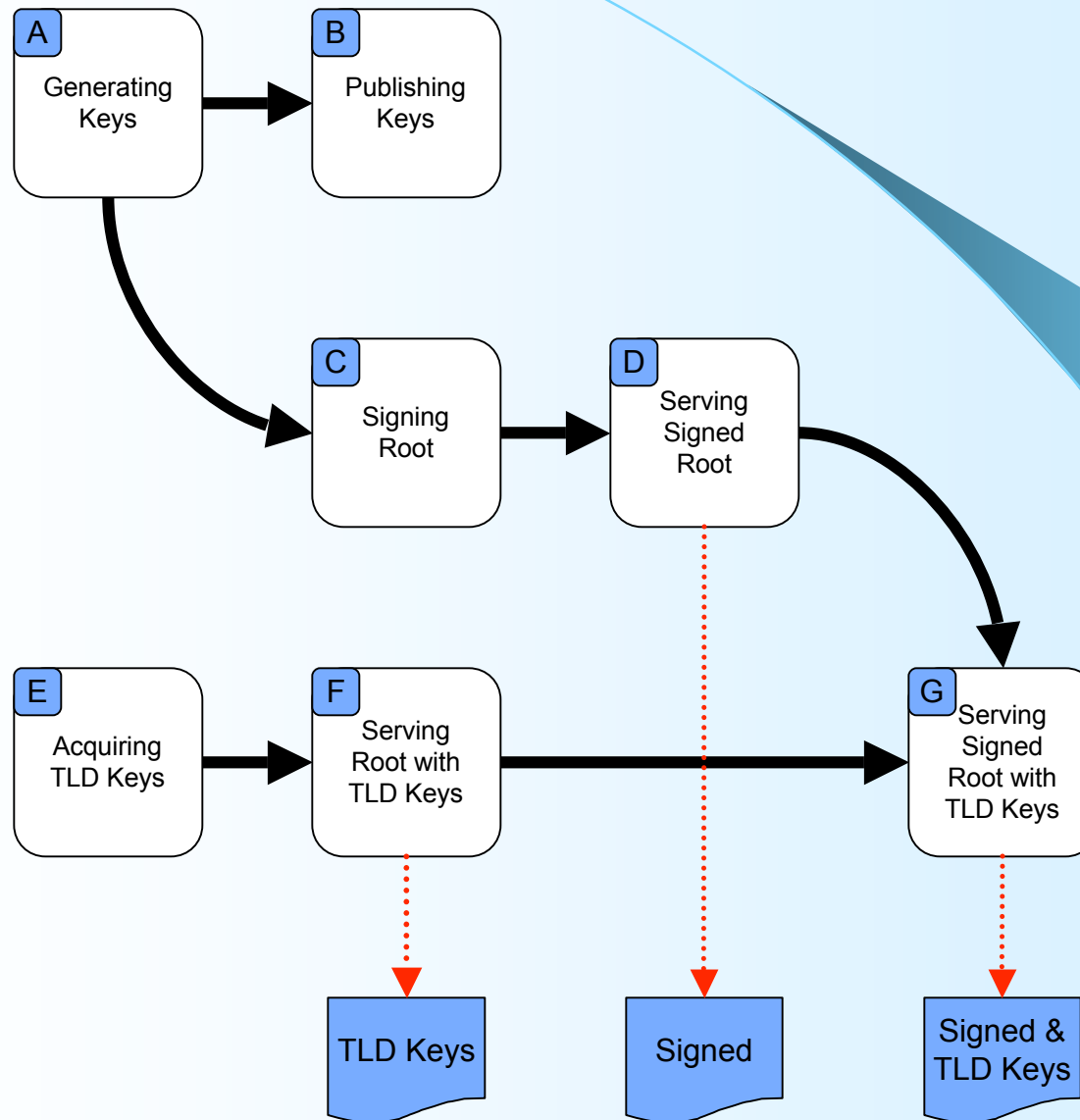
Zones

- Root
- Registries & Registrars
- Enterprises
- Governments

Root Zone Update Process



Root Signing Road Map



Who runs name servers?

- Enterprises
- Universities
- Government agencies

Who runs name servers?

- Enterprises
- Universities
- Government agencies

- Registrars
- Hosting providers
- Managed DNS service providers

DNS Service Providers

- DNS service provider can implement DNSSEC without zero impact domain holder
 - Except, possibly for a charge
- DNS Service Providers are the path to substantial numbers of signed zones
 - In the immediate future, mutual hosting
- Might lead to pressure from the bottom

DNSSEC Deployment

- Serious deployment activities emerging around the world:
 - <http://secspider.cs.ucla.edu/> tracking ~300 signed zones
 - Europe/RIPE region most active
- U.S. Government taking leadership role in North America
 - DNSSEC requirements included in latest Federal Information Security Management Act (FISMA) requirements
 - Federal Information Processing Standards (FIPS) 199 & 200.
 - Requires incremental deployment of DNSSEC across USG agencies
 - and the contractors that provide IT resources/services to them

Government

- Deployment inside the U.S. Gov't
- Requirements on others
- Other governments

Inside the USG

- USG owns .mil, .gov, .us
 - .mil for the Defense Dept
 - .gov for the rest of the federal gov't
 - Some state gov use too
 - .us is the U.S.'s country code top level domain
 - Not as popular as .de, .uk, etc.

U.S. Gov't Deployment

- .mil is moving toward DNSSEC
 - DISA is the lead agency
 - Marine Corp is most advanced
 - Name servers first; resolvers later
- .gov is in planning stages
 - OMB and GSA are formulating tasking
 - NIST documents emerging

USG Plan for Staged Deployment

- NIST special publication 800-53R1
 - Specifies mandatory minimum security controls necessary to comply with FISMA
 - See: <http://csrc.nist.gov/publications/drafts.html>
 - Agencies must comply within 12 months of publication
- Includes plan for staged deployment of DNSSEC technology within federal IT systems.
 - Initial steps require agencies to sign (include digital signatures) in DNS zones that are part of medium- and high-impact systems (FISMA classifications)

Other Governments

- Internal adoption
 - NZ, UK, SE, CA, AU, ...
- Sponsorship for ccTLD adoption
 - Many

For more information,
read DNSSEC THIS MONTH
(<http://www.dnssec->



DNSSEC This Month

MAY 1, 2006

VOLUME 1, NUMBER 1

Welcome to the first edition of DNSSEC This Month, a monthly newsletter about advances in securing the Internet's naming infrastructure in the government, business and education sectors. Some 10 percent of servers in the network today are vulnerable to domain name system (DNS) attacks, and many experts expect a serious attack on the underlying infrastructure within the next decade. The [DNS Security Extensions \(DNSSEC\) Deployment Coordination Initiative](#).

White House unveils R&D plan to boost IT infrastructure security: A new *Federal Plan for Cyber Security and Information Assurance Research and Development* has been issued by the White House Office of Science and Technology Policy, providing "a blueprint for coordination of Federal R&D across agencies that will maximize the impact of investments in this key area of the national interest," according to John H. Marburger III, Science Adviser to the President. The plan, available in a preprint here (http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf), notes the expanding role of the domain name system, and with it, "an increased need to assure the authenticity of the DNS responses and an increased possibility that the DNS itself will be targeted for attacks." Public comments on the report were taken during April; to order a print copy of the report, click: (<http://www.nitrd.gov/pubs/request.php>).

DNS Security Extensions (DNSSEC) on path to be included in new federal standards: DNSSEC has been proposed as part of a new standard that aims to help federal agencies improve their information technology security and comply with the Federal Information Security Management Act (FISMA) of 2002. A plan for staged deployment of DNSSEC technology within federal IT systems was included in recently released Draft Special Publication 800-53, Revision 1: Recommended

Contacts & Resources

- Steve@shinkuro.com
- www.dnssec-deployment.org
- Slides and other DNSSEC material at:
www.ripe.net/training/dnssec/
- <http://www.nlnetlabs.nl/dnssec/>
- <http://www.dnssec.net/>

Support provided by U.S. Dept. of Homeland Security, Science and Technology Directorate and ICANN

Cooperative work with Sparta, NIST, MIT Lincoln Laboratory