Homeland Security Advanced Research Projects Agency

What has the Government done for you lately?

Douglas Maughan, Ph.D.
Division Director

October 22, 2012

Homeland Security
Science and Technology

Homeland Security
Science and Technology

Environment: Greater Use of Technology, More Threats, Less Resources

Homeland Security
Science and Technology

DHS S&T Mission Guidance

Strategic Guidance

Homeland Security Act 2002 → QHSR (Feb 2010) → BUR (July 2010) → S&T Strategic Plan (2011)

QHSR

Threats

Smaller Scale Terrorism | Trafficking, Crime | Pandemics, Accidents, Natural Hazards | Violent Extremism | High Consequence WMD

Core Missions

1. Preventing terrorism & enhancing security
2. Securing and managing our borders
3. Enforcing & administering immigration laws
4. Safeguarding and securing cyberspace
5. Ensuring resilience to disasters

Operational Directives

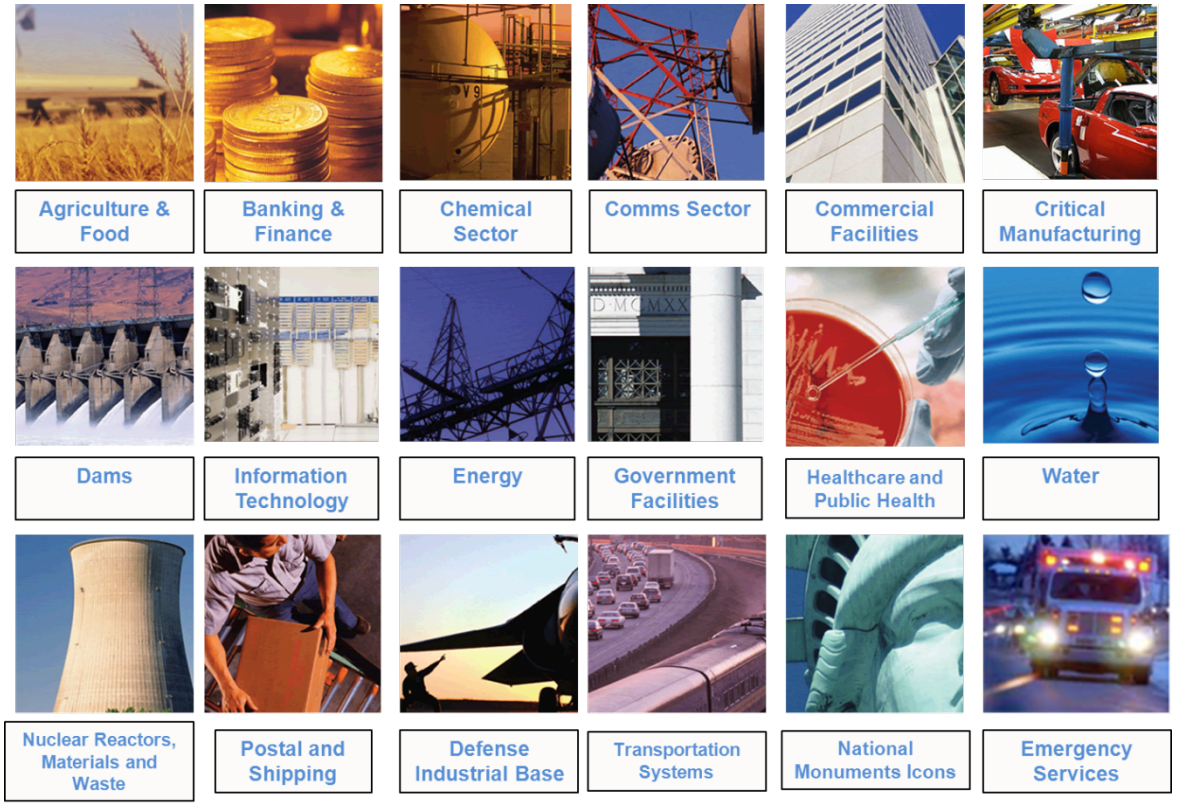
HSPD-5 National Incident Management System (2003) → HSPD-9 Defense of U.S. Agriculture & Food (2004) → HSPD-10 Biodefense for the 21st Century (2004) → HSPD-22 Domestic Chemical Defense (2007) → PPD-8 National Preparedness (2011)

Prevention, Protection, Mitigation, Response, Recovery

Homeland Security
Science and Technology

Cybersecurity for the 18 Critical Infrastructure Sectors

DHS provides advice and alerts to the 18 critical infrastructure areas …



… DHS collaborates with sectors through Sector Coordinating Councils (SCC)

In the future, DHS will provide cybersecurity for …

- ❑ The .gov and critical .com domains with a mix of:
  - ➢ Managed security services
  - ➢ Developmental activities
  - ➢ Information sharing
- ❑ Linkages to our U.S. – CERT (Computer Emergency Readiness Team)

National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 center for production of a common operating picture …

DHS S&T Mission

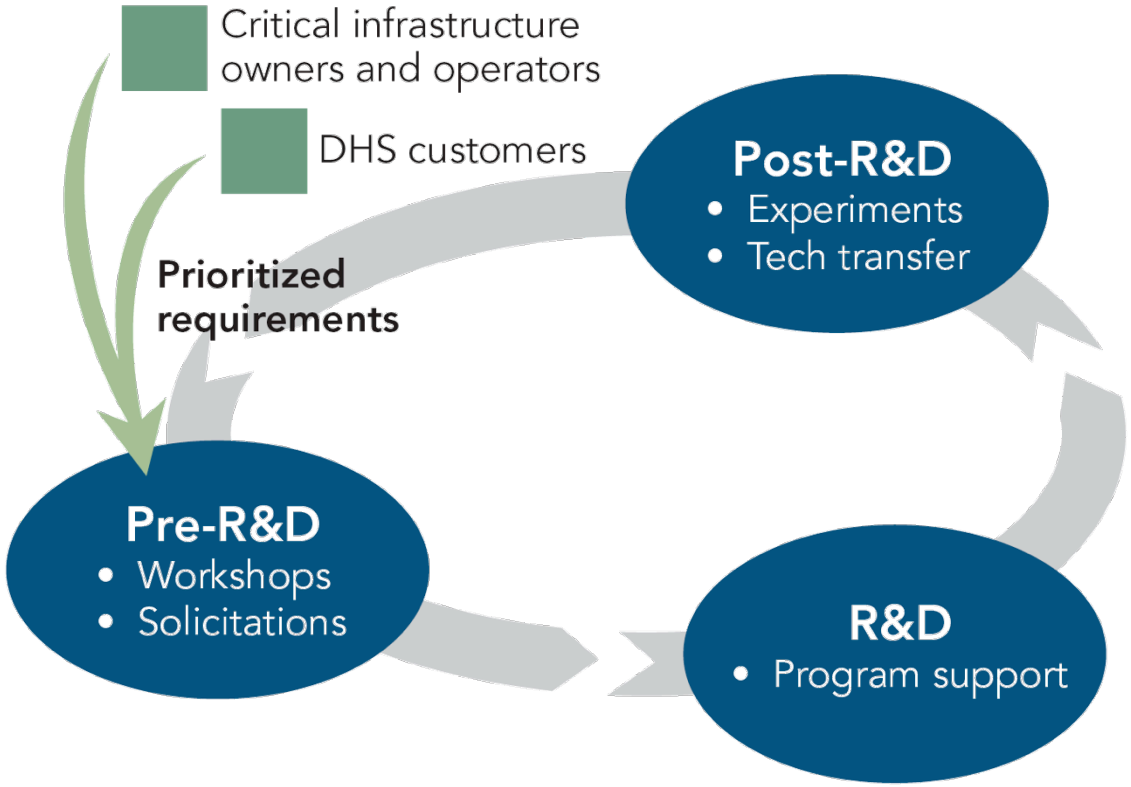
Strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise

1) Create new technological capabilities and knowledge products
2) Provide Acquisition Support and Operational Analysis
3) Provide process enhancements and gain efficiencies
4) Evolve US understanding of current and future homeland security risks and opportunities

Homeland Security
Science and Technology

Homeland Security
Science and Technology

CSD R&D Execution Model



Research
Development
Test and Evaluation &
Transition (RDTE&T)

Successes

- Ironkey – Secure USB
  - Standard Issue to S&T employees from S&T CIO
- Komoku – Rootkit Detection Technology
  - Acquired by Microsoft
- HBGary – Memory and Malware Analysis
  - Over 100 pilot deployments as part of Cyber Forensics
- Endeavor Systems – Malware Analysis tools
  - Acquired by McAfee
- Stanford – Anti-Phishing Technologies
  - Open source; most browsers have included Stanford R&D
- Secure Decisions – Data Visualization
  - Pilot with DHS/NCSD/US-CERT; Acquisition

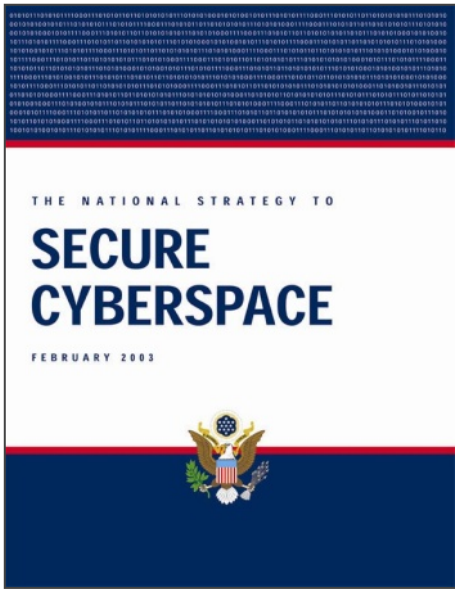
Discussion Topics

- DNSSEC
- RPKI / BGPSEC and Other Routing Stuff
- IPv6
- Internet Measurement
- HOST and Open Source
- PREDICT Data Repository
- Cybersecurity Competitions
- Research Strategic Plans
- Discussions with NANOG community about what more DHS S&T can do to help

Homeland Security
Science and Technology

National Strategy to Secure Cyberspace

- The National Strategy to Secure Cyberspace (2003) recognized the Domain Name System (DNS) as a critical weakness
  - NSSC called for the Department of Homeland Security to coordinate public-private partnerships to encourage the adoption of improved security protocols
  - **The security and continued functioning of the Internet will be greatly influenced by the success or failure of implementing more secure and more robust BGP and DNS**. The Nation has a vital interest in ensuring that this work proceeds. **The government should play a role when private efforts break down due to a need for coordination or a lack of proper incentives.**



Homeland Security
Science and Technology

OMB memo on DNSSEC

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf

August 22, 2008

M-08-23

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Securing the Federal Government's Domain Name System Infrastructure
(Submission of Draft Agency Plans Due by September 5, 2008)

The efficient and effective use of our networks is important to promote a more citizen centered and results oriented government. The Government's reliance on the Internet to disseminate and provide access to information has increased significantly over the years, as have the risks associated with potential unauthorized use, compromise, and loss of the .gov domain space.

Almost every instance of network communication begins with a request to the Domain Name System (DNS) to resolve a human readable name for a network resource (e.g., www.usa.gov) into the technical information (e.g., Internet Protocol address) necessary to actually access the remote resource. This memorandum describes existing and new policies for deploying Domain Name System Security (DNSSEC) to all Federal information systems by December 2009.

Homeland Security
Science and Technology

DNSSEC Standards Produced or Influenced by Deployment Project

- RFC4033
- RFC4034
- RFC4035
- RFC4431
- RFC4470
- RFC4509
- RFC4641
- RFC4955
- RFC4956
- RFC4986
- RFC5011
- RFC5074
- RFC5155
- RFC5702
- RFC5933
- RFC6014
- RFC6605
- And others …..

Homeland Security
Science and Technology

ccTLD Signed Map

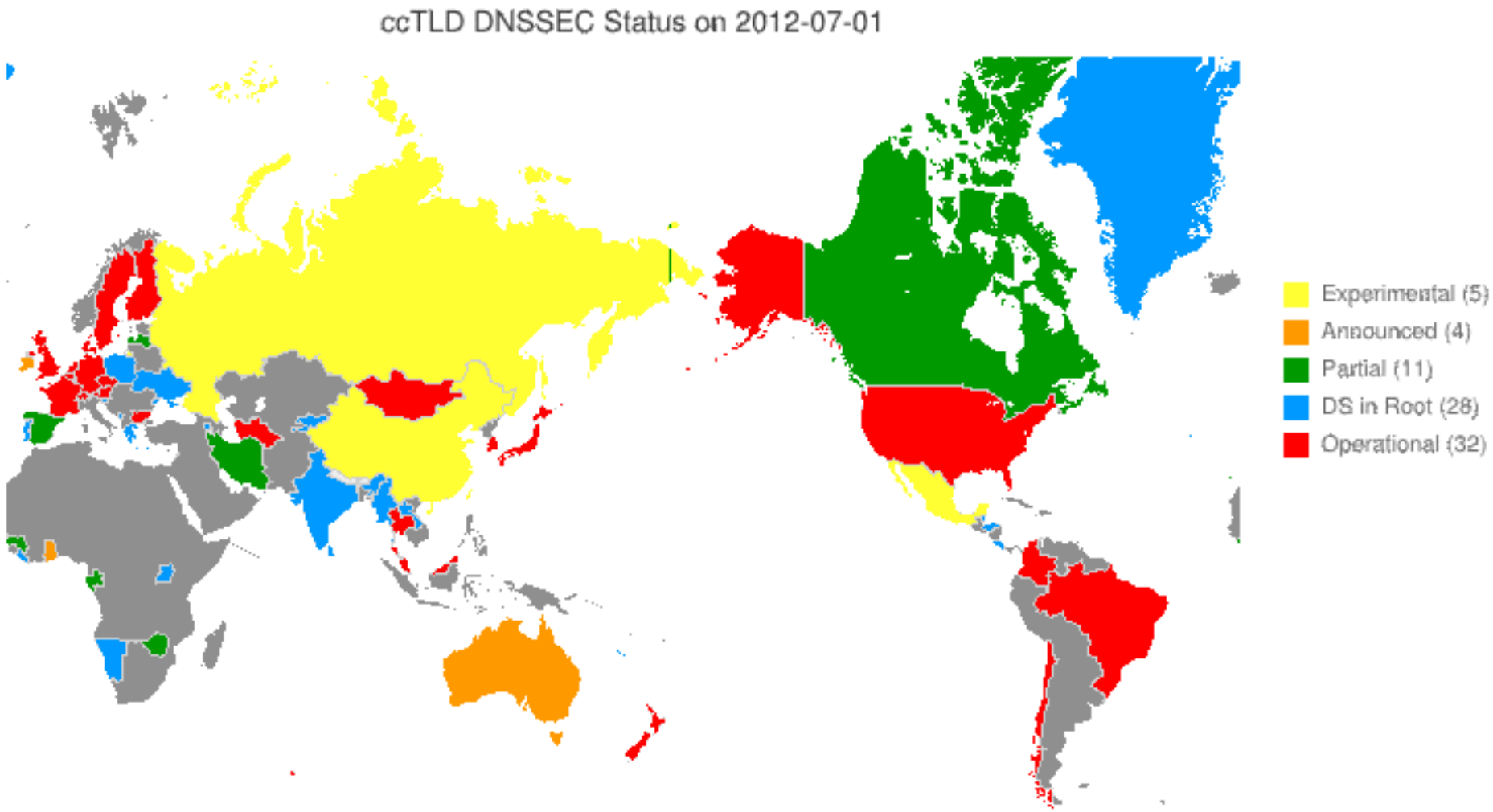


Image Credit: Shinkuro

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

DNSSEC Related Controls in SP 800-53r4

- SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
  - *"Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns **in response to external name/address resolution queries;**"* (Emphasis mine)
  - Control Enhancement on providing the security status of child zones (i.e. DS RR's) incorporated into the base control
  - Related to: AU-10, SC-13, SC-17, SC-21, SC-22
- Labeled P1 (Priority Code 1) – a control that should be implemented first (i.e. high priority).

Making DNSSEC the Trust Infrastructure

DNSSEC

U.S. Department of Homeland Security

DNSSEC Related Controls in SP 800-53r4

- SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
  - *"The information system requests and performs data origin authentication and data integrity verification on the name/ address resolution responses the system receives from authoritative sources."*
  - **Supplemental Guidance**: *"Each client of name resolution services either performs this validation on its own, or has authenticated channels to trusted validation providers."*
  - Applies to all levels (Low, Moderate and High)
  - Related to: SC-20 and SC-22
- Labeled P1 (Priority Code 1) – a control that should be implemented first (i.e. high priority).

Homeland Security
Science and Technology

What's next for DNSSEC?

- Working to transition DNSSEC Deployment Initiative activities to ISOC's Deploy360 program for longer-term support
- Are there remaining (S&T) activities that the USG should consider "helping"?
  - DANE
  - Other Application Development??
  - Now's the chance to let us know

Homeland Security
Science and Technology

Secure Routing Activities

- The IETF has been working to define the specs
- Steps 1&2: Resource Certification and Origin Authorization
  - 13 RFCs published in February 2012
    - http://datatracker.ietf.org/wg/sidr/
    - Certs, ROAs, certificate policy, repository structure, cache-to-router protocol, certificate management protocol (aka "up/down"), error reporting info, etc.
  - Two more documents approved for publication
    - BGP route validation; RPKI cache -> routers
  - Other operational documents in progress
    - Concept of operations and guidance, local trust anchors
- Step 3: Path validation
  - In progress in the SIDR working group

Homeland Security
Science and Technology

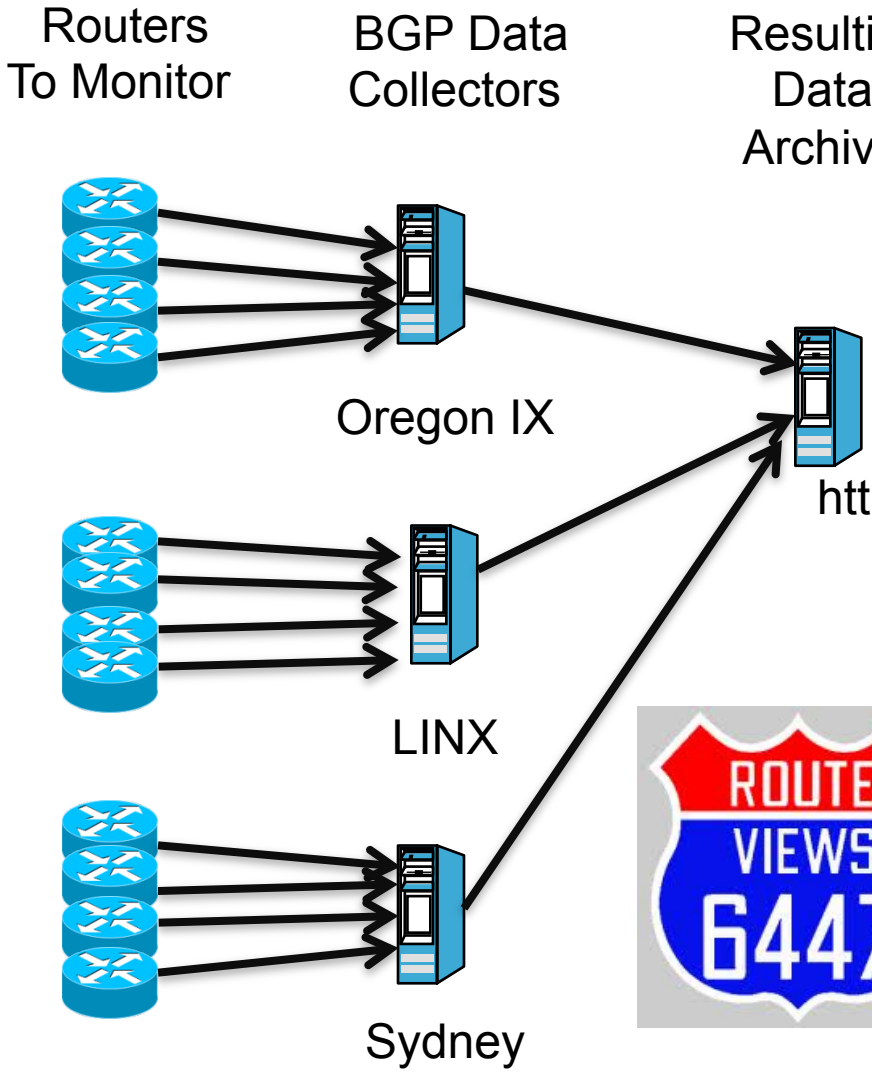
Secure Routing Activities - 2

- Commercial implementations underway
  - Cisco
  - Juniper
- Implementation of RPKI-based validation of BGP routes
- Relying Party
  - Rpki.net http://www.rpki.net/
  - RPSTIR from BBN http://sourceforge.net/projects/rpstir/
  - BGP-SRx from NIST http://www-x.antd.nist.gov/bgpsrx/
  - RIPE NCC RPKI Validator 2.0 http://www.ripe.net/lir-services/resource-management/certification/making-better-routing-decisions-through-rpki-validation
- Independent CA service
  - Rpki.net http://www.rpki.net
- Operations Tools
  - RPKI Looking Glass from LACNIC www.labs.lacnic.net/rpkitools/looking_glass/
  - BRITE from NIST https://brite.antd.nist.gov/statics/about
  - RTRlib RPKI-router Client C library http://rpki.realmv6.org/
  - Router configuration from RIPE NCC http://www.ripe.net/lir-services/resource-management/certification/router-configuration
  - Validator and cache tools from Euro-Transit http://rpki01.fra2.de.euro-transit.net/

BRITE - BGPSEC / RPKI Interoperability Test & Evaluation

- Web-based test and evaluation framework for BGP security technologies
- BRITE allows users to login, select a specific test case, interactively configure and run the test case and then browse/download detailed test reports, packet captures and log files.
  - rsync of RPKI objects from BRITE test suite repositories
  - RPKI/Router Protocol (draft-ietf-sidr-rpki-rtr-12)
  - BGP-4 (tested with Cisco IOS, JUNOS, Quagga, OpenBGPD and BIRD)
- Collaborative effort with NIST's Advanced Network Technologies Division (ANTD)
- http://brite.antd.nist.gov

Routing Activities – RouteViews / BGPmon



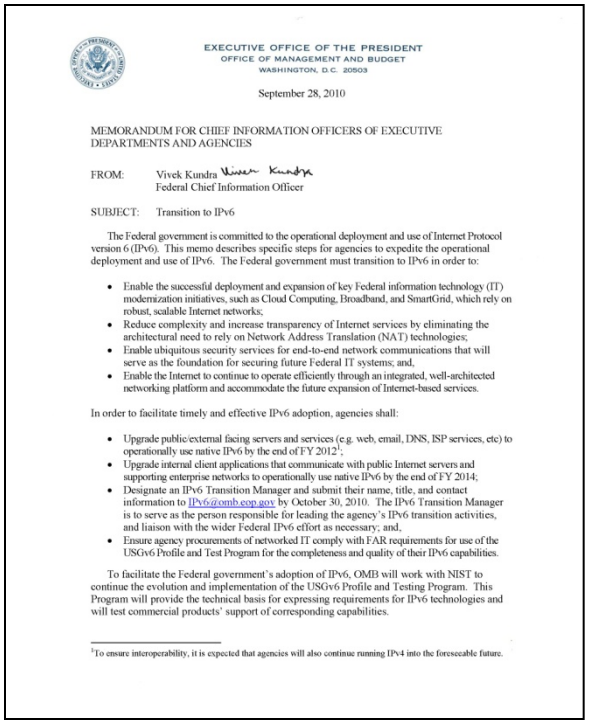
- All Route Updates Are Logged
  - 15 minute intervals

http://archive.routeviews.org/bgpdata/

- Collector also archives routing table of each peer router
  - 2 hour intervals

USG as IPv6 Early Adopter

- **Key USG Milestones and Objectives:**
  - http://www.cio.gov/documents/**IPv6**MemoFINAL.pdf
  - **Upgrade public external facing services** (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 **by the end of FY2012**;
  - **Upgrade internal client applications** that communicate with public Internet servers and supporting enterprise networks to operationally use native **IPv6 by the end of FY2014**;
  - **Continuously monitor and measure the status** of production deployments within the USG and other domains.
  - **Ensure agency procurements of networked IT comply** with FAR requirements for use of the **USGv6 Profile and Testing Program** for the completeness and quality of their IPv6 capabilities.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 28, 2010

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Vivek Kundra
Federal Chief Information Officer

SUBJECT: Transition to IPv6

The Federal government is committed to the operational deployment and use of Internet Protocol version 6 (IPv6). This memo describes specific steps for agencies to expedite the operational deployment and use of IPv6. The Federal government must transition to IPv6 in order to:

- Enable the successful deployment and expansion of key Federal information technology (IT) modernization initiatives, such as Cloud Computing, Broadband, and SmartGrid, which rely on robust, scalable Internet networks;
- Reduce complexity and increase transparency of Internet services by eliminating the architectural need to rely on Network Address Translation (NAT) technologies;
- Enable ubiquitous security services for end-to-end network communications that will serve as the foundation for securing future Federal IT systems; and,
- Enable the Internet to continue to operate efficiently through an integrated, well-architected networking platform and accommodate the future expansion of Internet-based services.

In order to facilitate timely and effective IPv6 adoption, agencies shall:

- Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012[1];
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
- Designate an IPv6 Transition Manager and submit their name, title, and contact information to IPv6@omb.eop.gov by October 30, 2010. The IPv6 Transition Manager is to serve as the person responsible for leading the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and,
- Ensure agency procurements of networked IT comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

To facilitate the Federal government's adoption of IPv6, OMB will work with NIST to continue the evolution and implementation of the USGv6 Profile and Testing Program. This Program will provide the technical basis for expressing requirements for IPv6 technologies and will test commercial products' support of corresponding capabilities.

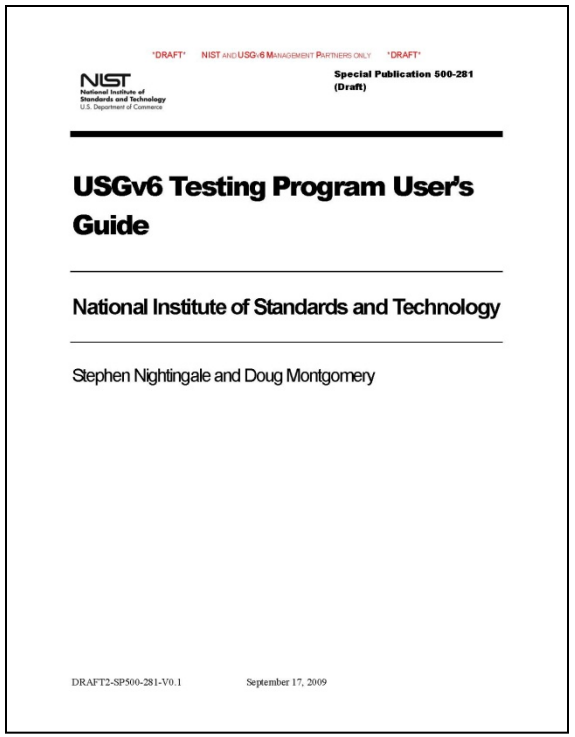
[1] To ensure interoperability, it is expected that agencies will also continue running IPv4 into the foreseeable future.

NIST National Institute of Standards and Technology

INFORMATION TECHNOLOGY LABORATORY

USGv6 Testing Program

- **Establish a unified testing program:**
  - Conformance, Interoperability, and Functional testing for Hosts, Routers, NPDs
- **Goal: One-stop Worldwide Testing.**
  - Establish program based upon accredited labs, public test specifications and validated test methods.
  - Establish common means of reporting test results.
  - Establish means of tracing vendor's declarations back to accredited test results.
- **Flexible / Open Program:**
  - Support 1st, 2nd, 3rd party conformance testing.
  - Support 2nd, 3rd party interoperability testing and NPD functional testing.
  - Using commercial labs and accreditors.
- **Operational 2009:**
  - Includes Accredited Labs, with tested products


"DRAFT" NIST AND USGv6 MANAGEMENT PARTNERS ONLY "DRAFT"

NIST National Institute of Standards and Technology U.S. Department of Commerce

Special Publication 500-281 (Draft)

USGv6 Testing Program User's Guide

National Institute of Standards and Technology

Stephen Nightingale and Doug Montgomery

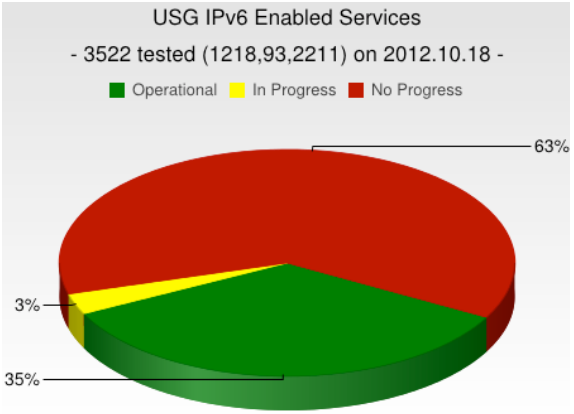
DRAFT2-SP500-281-V0.1 September 17, 2009

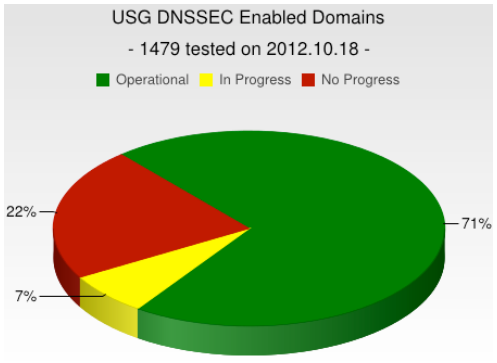
NIST National Institute of Standards and Technology

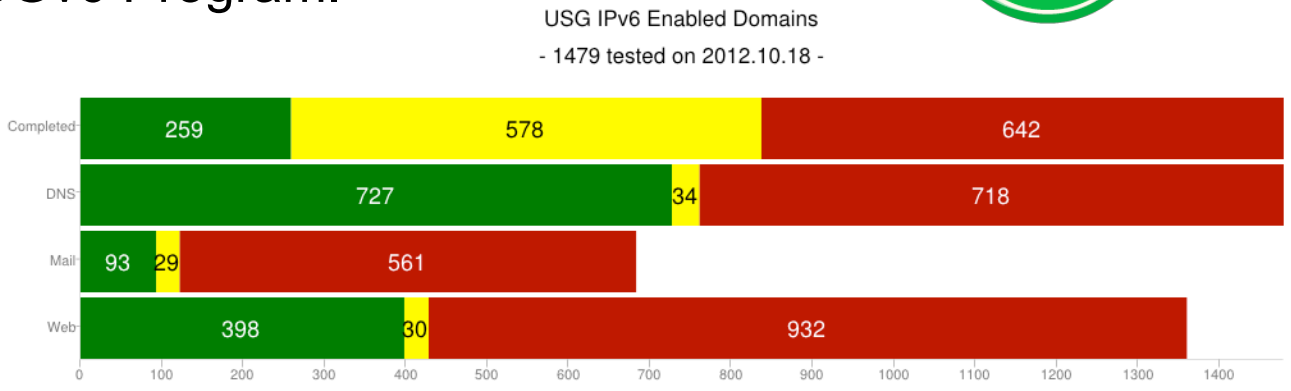
INFORMATION TECHNOLOGY LABORATORY

USG Progress to Date

- **In just two years…**
  - ~800 distinct domains / enterprises deployed operational IPv6 services.
  - ~1200 unique public .gov services are IPv6 enabled.
  - ~30% of public web .gov sites monitored are IPv6 enabled.
  - Scores of commercial products have been conformance and interoperability tested through the USGv6 Program.



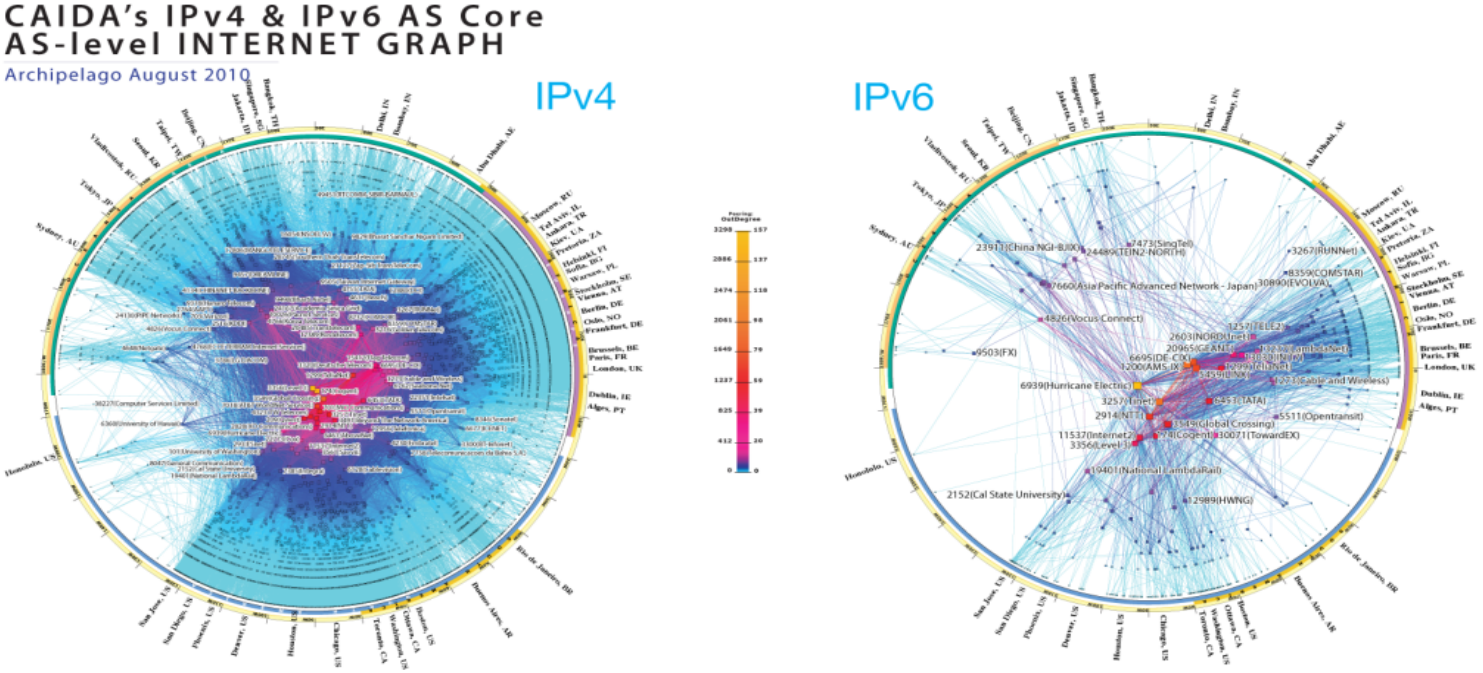




Homeland Security
Science and Technology

Internet Measurement and Attack Modeling (IMAM)

- The protection and defense of critical cyber infrastructures depends on the ability to both identify critical Internet resources that are subject to attack, and to research, develop and apply modeling and analysis capabilities to predict and mitigate effects.
- The development of tools and techniques for mapping cyberspace (with a focus on Internet routes) to detect and model malicious behavior, and identify critical infrastructure within cyberspace is essential to the Homeland Security Enterprise



Homeland Security
Science and Technology

Internet Measurement - 2

Integrated strategic measurement & analysis capabilities:

1. Ark Measurement platform: software, data, access
2. Topology analysis: software, data kits, papers
3. Dual router- and AS-level graphs: software, viz
4. AS taxonomy and relationships: published algorithms, interactive web service (AS Rank)
5. Graph visualization: part of AS Rank web service

HOST Program

HOST = Homeland Open Security Technology

Closing government cybersecurity gaps by sponsoring open source projects

- Suricata Intrusions Detection System
- OpenSSL FIPS validation

…and helping government be able to find and deploy existing open source cybersecurity solutions

- Inventory of solutions, **opencybersecurity.org**
- Use cases & lessons learned reports
- Improved policy

Open Information Security Foundation and Suricata

- A new model for managing and sustaining innovation
  - A non-profit to develop and "own" the code
  - Software Freedom Law Center created the License pro bono
  - A consortium of companies providing support in exchange for not having to release changes
- Ground-up rewrite
  - Multi-Threaded
  - Automated Protocol Detection
  - File Identification and Extraction
  - GPU Acceleration

~$1.2m in DHS funding was matched by ~$8m in commercial sponsorship

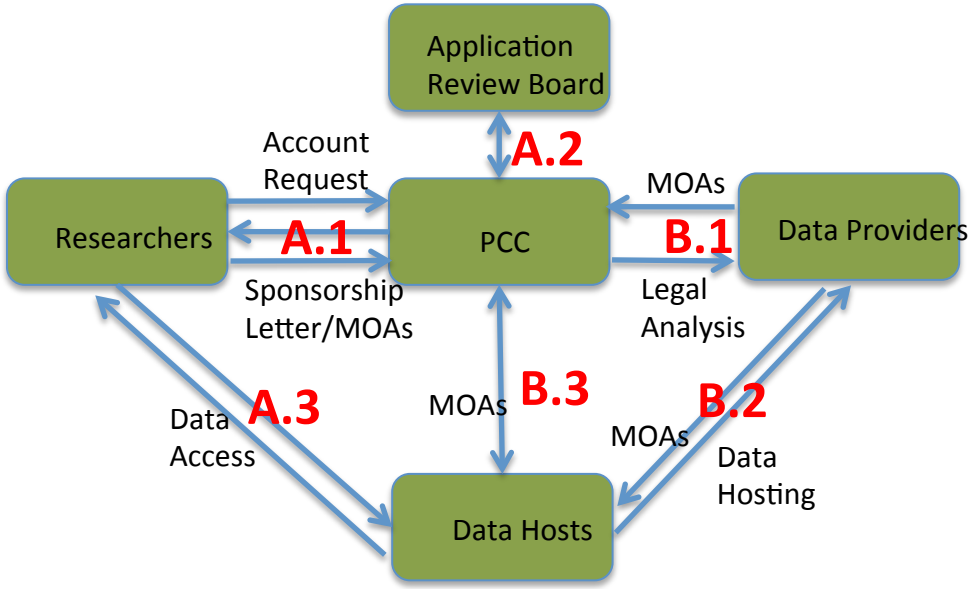
Let us know how we can work together

Homeland Security
Science and Technology

- Include your open source efforts in our inventory
  - Project owners maintain small .xml, we crawl for updates
- Let us know of projects that Gov should be using so we can share them with other Gov agencies
- Let us know if there are some successes that would make a good case study
- Let us know of open source cybersecurity projects that might benefit from some government funding

PREDICT Overview

- Rationale / Background:
  - Researchers with insufficient access to data unable to adequately test their research prototypes
  - Support for scientific method via repeatability of tests and evaluations
  - Unclear legal and ethical policies for Internet research
- PREDICT project is the only freely-available legally collected repository of large-scale datasets containing real network traffic and system logs.
- Dissemination of data is supported by a streamlined legal framework that controls distribution while protecting researchers, data providers and data hosts.



PREDICT Activities

- Support data collection activities to make high quality, timely and relevant dataset available to the research community.
- Support the advancement of tools and techniques for analyzing Internet datasets to extract useful information and the representation of that information.
- Advance the state of the art in data collection techniques, packet formats, new data types, storage techniques, data cataloging/annotation, cross dataset analysis.
- Investigate and highlight legal and ethical issues in Internet data collection and analysis.
- Datasets: Address Space Allocation Data, BGP Routing Data, Darknet Address Space Data, DNS, Internet Topology, Traffic Flow Data, etc.

PREDICT Impact

- Over 250 research papers/journals/technical reports within the last 3 years, based on research done with data from the PREDICT data repository
- 350+ TB of data is available
- Research groups include:
  - 26 academic institutions
  - 24 commercial entities
  - 11 Government organizations
  - 4 non-profit organizations
- Menlo Report – First attempt at documenting ICTR ethical issues. Still working (expect another 2-3 years) to implement policies on ethical issues with universities, government agencies, professional groups (ACM, IEEE), etc.

- *Data provides operational insights such as as-rank, topology datasets, DNS traffic patterns, impact of MegaUpload shutdown, censorship activity and botnet activity.*

Homeland Security
Science and Technology

Cybersecurity Competitions

- DHS funds multiple competitions including National Collegiate Cyber Defense Competition and the US Cyber Challenge
  - Over 2500 students participated in 2012
  - Starting efforts to utilize the various competitions around the country to address national needs
- Competitions drive improvements in all four areas of NICE
  - Awareness – increasing the number of people exposed to cybersecurity
  - Formal Education – provides a means to enhance formal programs with practical applications
  - Cybersecurity Workforce Structure
  - Cybersecurity Workforce Training and Professional Development
- Competitions drive technology transition
  - Technology insertions from development programs
  - Students gain insight into new capability

History of National Cyber Security Work

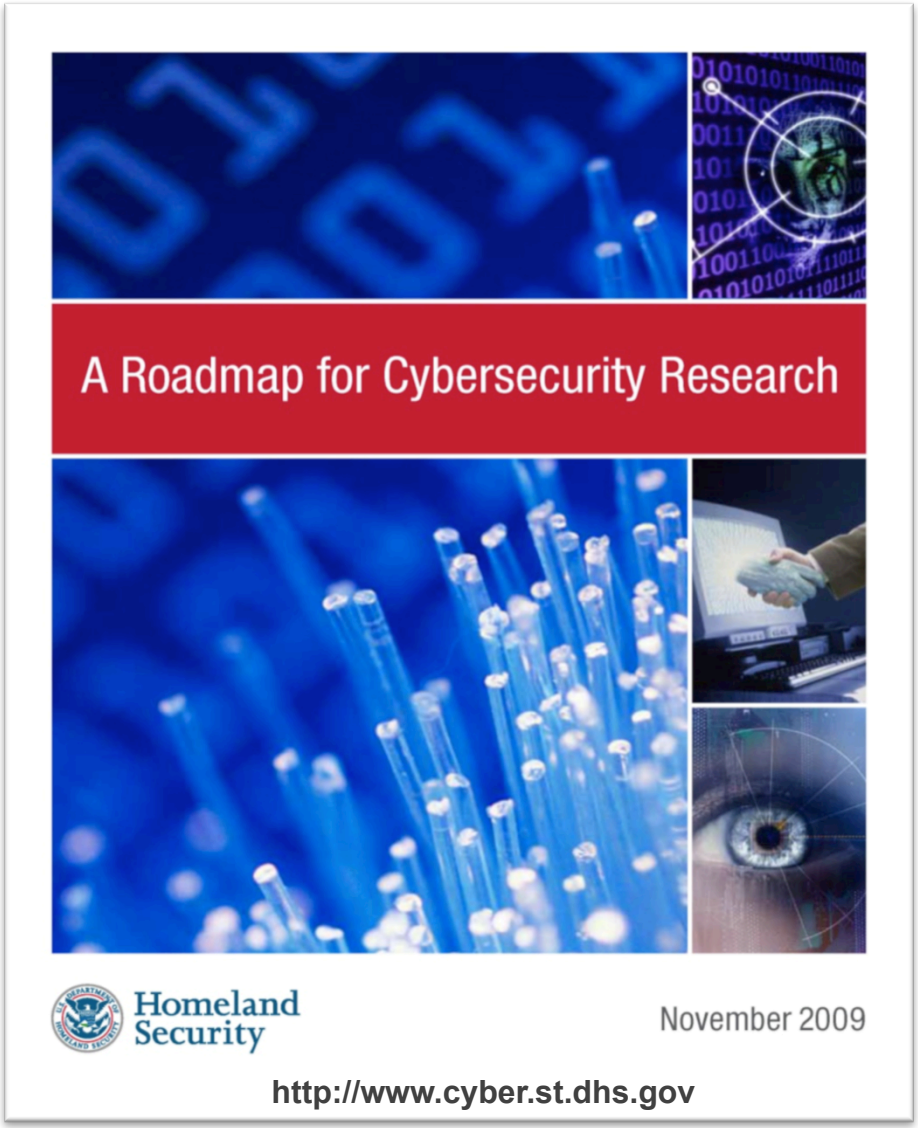
Homeland Security
Science and Technology

All documents available at:
http://www.cyber.st.dhs.gov/resources/

A Roadmap for Cybersecurity Research

Identified critical research gaps in:

- Scalable Trustworthy Systems
- Enterprise Level Metrics
- System Evaluation Lifecycle
- Combating Insider Threats
- Combating Malware and Botnets
- Global-Scale Identity Management
- Survivability of Time-Critical Systems
- Situational Understanding and Attack Attribution
- Information Provenance
- Privacy-Aware Security
- Usable Security



Homeland Security
Science and Technology

Federal Cybersecurity R&D Strategic Plan

- Science of Cyber Security
- Research Themes
  - Tailored Trustworthy Spaces
  - Moving Target Defense
  - Cyber Economics and Incentives
  - Designed-In Security (New for FY12)
- Transition to Practice
  - Technology Discovery
  - Test & Evaluation / Experimental Deployment
  - Transition / Adoption / Commercialization
- Support for National Priorities
  - Health IT, Smart Grid, NSTIC (Trusted Identity), NICE (Education), Financial Services

Released Dec 6, 2011

http://www.whitehouse.gov/blog/2011/12/06/federal-cybersecurity-rd-strategic-plan-released

DHS S&T Long Range Broad Agency Announcement (LRBAA) 12-07

- S&T seeks R&D projects for revolutionary, evolving, and maturing technologies that demonstrate the potential for significant improvement in homeland security missions and operations
- Offerors can submit a pre-submission inquiry prior to White Paper submission that is reviewed by an S&T Program Manager
- CSD has 14 Topic Areas (CSD.01 – CSD.14) – SEE NEXT SLIDE
- LRBAA 12-07 Closes on 12/31/12 at 11:59 PM
- S&T BAA Website: https://baa2.st.dhs.gov
- Additional information can be found on the Federal Business Opportunities website (www.fbo.gov) (Solicitation #:DHSS-TLRBAA12-07)

Homeland Security
Science and Technology

LRBAA Summary Listing

- **CSD.01** – Comprehensive National Cybersecurity Initiative and Federal R&D Strategic Plan topics
- **CSD.02** – Internet Infrastructure Security
- **CSD.03** – National Research Infrastructure
- **CSD.04** –Homeland Open Security Technology
- **CSD.05** – Forensics support to law enforcement
- **CSD.06** – Identity Management
- **CSD.07** – Data Privacy and Information Flow technologies.
- **CSD.08** – Software Assurance
- **CSD.09** – Cyber security competitions and education and curriculum development.
- **CSD.10** – Process Control Systems and Critical Infrastructure Security
- **CSD.11** – Internet Measurement and Attack Modeling
- **CSD.12 –** Securing the mobile workforce
- **CSD.13 -** Security in cloud based systems
- **CSD.14 –** Experiments – Technologies developed through federally funded research requiring test and evaluation in experimental operational environments to facilitate transition.

Homeland Security

Science and Technology

Summary

- Cybersecurity research is a key area of innovation needed to support our future
- DHS S&T continues with an aggressive cyber security research agenda
  - Working to solve the cyber security problems of our current (and future) infrastructure and systems
  - Working with academe and industry to improve research tools and datasets
  - Looking at future R&D agendas with the most impact for the nation, including education
- Need to continue strong emphasis on technology transfer and experimental deployments
- Interested in discussions with NANOG community about what more DHS S&T can do to help

Homeland Security

Science and Technology

Douglas Maughan, Ph.D.

Division Director

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

douglas.maughan@dhs.gov

202-254-6145 / 202-360-3170

For more information, visit

http://www.cyber.st.dhs.gov

Homeland Security

Science and Technology