DHS S&T Cyber Security Division (CSD) Overview

AIMS-3 Workshop
February 9-11, 2011
UCSD

Edward Rhyne

Program Manager

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

edward.rhyne@dhs.gov

202-254-6121

2004-2010 S&T Mission

Conduct, stimulate, and enable **research, development, test, evaluation and timely transition** of homeland security capabilities to federal, state and local operational end-users.

Homeland Security

DHS S&T Mission

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

S&T Goals

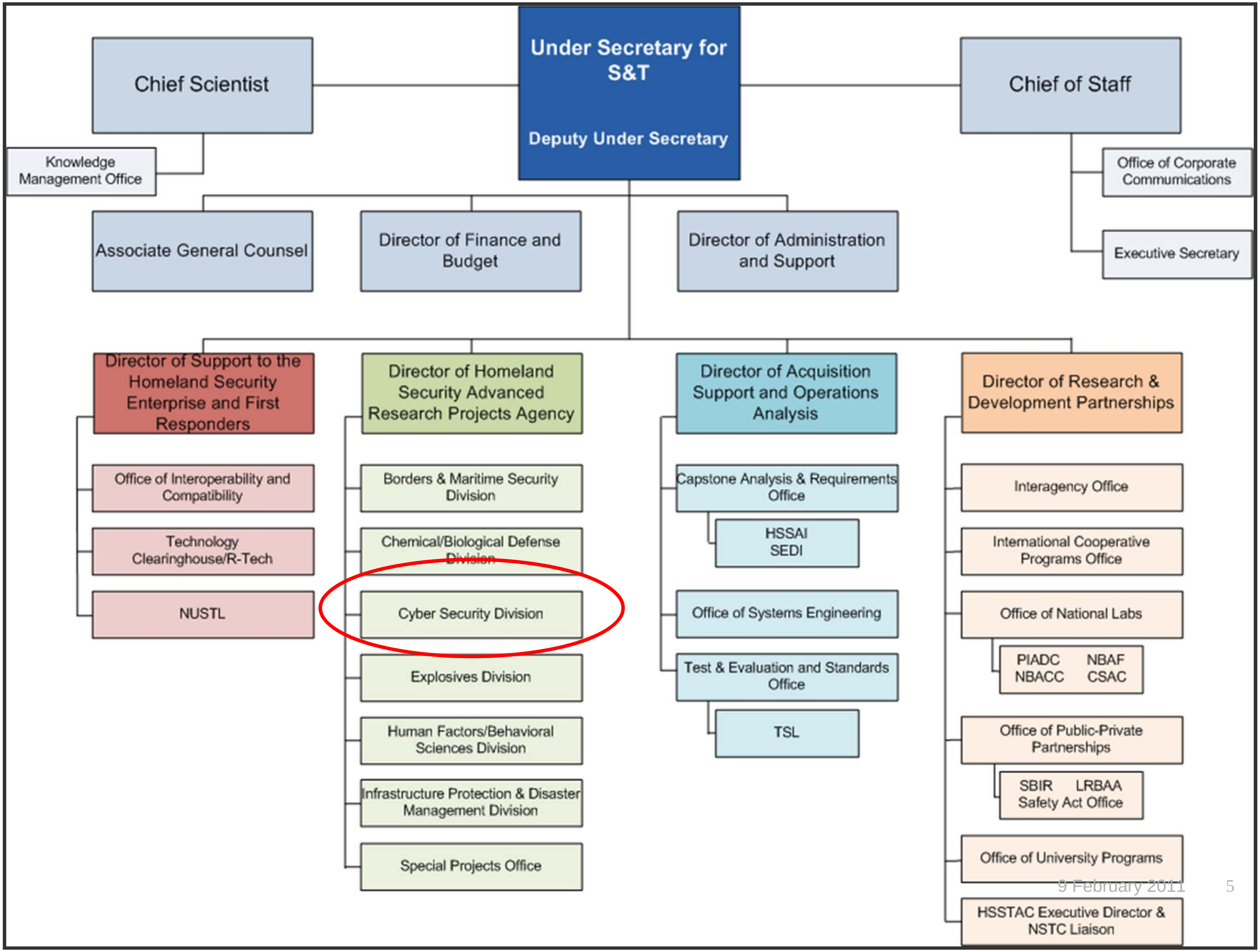
Goal 1: Rapidly develop and deliver knowledge, analyses, and innovative solutions that advance the mission of the Department

Goal 2: Leverage technical expertise to assist DHS components' efforts to establish operational requirements, and select and acquire needed technologies

Goal 3: Strengthen the Homeland Security Enterprise and First Responders' capabilities to protect the homeland and respond to disasters

Goal 4: Conduct, catalyze, and survey scientific discoveries and inventions relevant to existing and emerging homeland security challenges

Goal 5: Foster a culture of innovation and learning, in S&T and across DHS, that addresses challenges with scientific, analytic, and technical rigor



Under Secretary for S&T

Deputy Under Secretary

Chief Scientist

- Knowledge Management Office

Chief of Staff

- Office of Corporate Communications
- Executive Secretary

Associate General Counsel

Director of Finance and Budget

Director of Administration and Support

Director of Support to the Homeland Security Enterprise and First Responders

- Office of Interoperability and Compatibility
- Technology Clearinghouse/R-Tech
- NUSTL

Director of Homeland Security Advanced Research Projects Agency

- Borders & Maritime Security Division
- Chemical/Biological Defense Division
- Cyber Security Division
- Explosives Division
- Human Factors/Behavioral Sciences Division
- Infrastructure Protection & Disaster Management Division
- Special Projects Office

Director of Acquisition Support and Operations Analysis

- Capstone Analysis & Requirements Office
  - HSSAI
  - SEDI
- Office of Systems Engineering
- Test & Evaluation and Standards Office
  - TSL

Director of Research & Development Partnerships

- Interagency Office
- International Cooperative Programs Office
- Office of National Labs
  - PIADC
  - NBAF
  - NBACC
  - CSAC
- Office of Public-Private Partnerships
  - SBIR
  - LRBAA
  - Safety Act Office
- Office of University Programs
- HSSTAC Executive Director & NSTC Liaison

DHS S&T CSD Team

- Division Director:
  - Douglas Maughan
- Program Managers
  - Luke Berndt
  - Shane Cullen
  - Karyn Higa-Smith
  - Edward Rhyne
  - Gregory Wigton

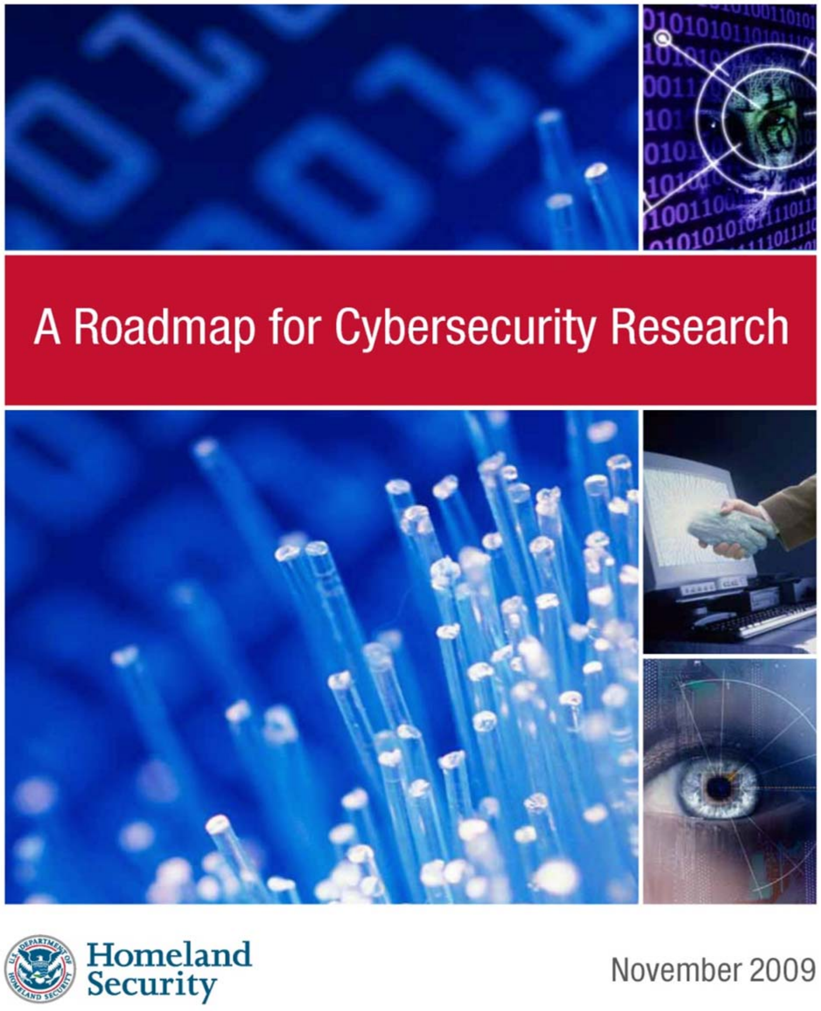
Contact us:

- SandT-Cyber@hq.dhs.gov

- SETA Staff
  - Amelia Brown
  - Kyshina Chandler
  - Shari Clayman
  - Tammi Fisher
  - Jeri Hessman
  - Megan Mahle
  - Jennifer Mekis
  - Michael Reagan
  - Elizabeth Reuss

A Roadmap for Cybersecurity Research

- **http://www.cyber.st.dhs.gov**
  - Scalable Trustrworthy Systems
  - Enterprise Level Metrics
  - System Evaluation Lifecycle
  - Combatting Insider Threats
  - Combatting Malware and Botnets
  - Global-Scale Identity Management
  - Survivability of Time-Critical Systems
  - Situational Understanding and Attack Attribution
  - Information Provenance
  - Privacy-Aware Security
  - Usable Security


A Roadmap for Cybersecurity Research

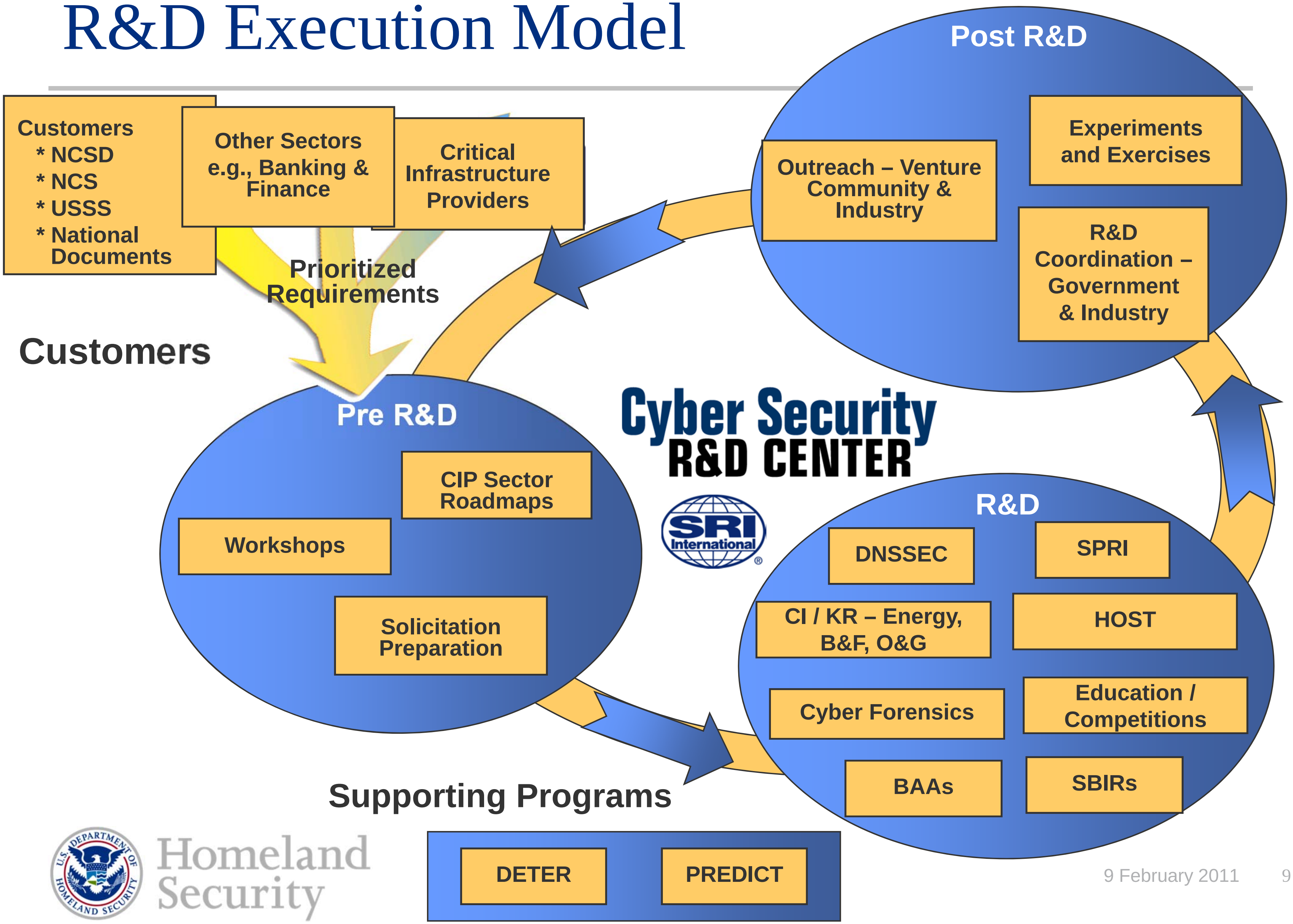
Homeland Security

November 2009

DHS S&T Roadmap Content

- What is the problem being addressed?
- What are the potential threats?
- Who are the potential beneficiaries? What are their respective needs?
- What is the current state of practice?
- What is the status of current research?
- What are the research gaps?
- What challenges must be addressed?
- What resources are needed?
- How do we test & evaluate solutions?
- What are the measures of success?

R&D Execution Model



Customers
* NCSD
* NCS
* USSS
* National Documents

Other Sectors e.g., Banking & Finance

Critical Infrastructure Providers

Prioritized Requirements

Customers

Pre R&D

CIP Sector Roadmaps

Workshops

Solicitation Preparation

Post R&D

Outreach – Venture Community & Industry

Experiments and Exercises

R&D Coordination – Government & Industry

Cyber Security R&D CENTER

SRI International

R&D

DNSSEC

SPRI

CI / KR – Energy, B&F, O&G

HOST

Cyber Forensics

Education / Competitions

BAAs

SBIRs

Supporting Programs

DETER

PREDICT

Homeland Security

Cyber Security Program Areas

- Internet Infrastructure Security
- Critical Infrastructure / Key Resources (CI/KR)
- National Research Infrastructure
- Cyber Forensics
- Homeland Open Security Technology (HOST)
- Identity Management / Data Privacy
- Internet Measurement and Attack Modeling
- Software Assurance - Tools and Infrastructure
- Next Generation Technologies
- Exp Deployments, Outreach, Education/Competitions
- Comp. National Cybersecurity Initiative (CNCI)
- Small Business Innovative Research (SBIR)

Internet Measurement / Attack Modeling

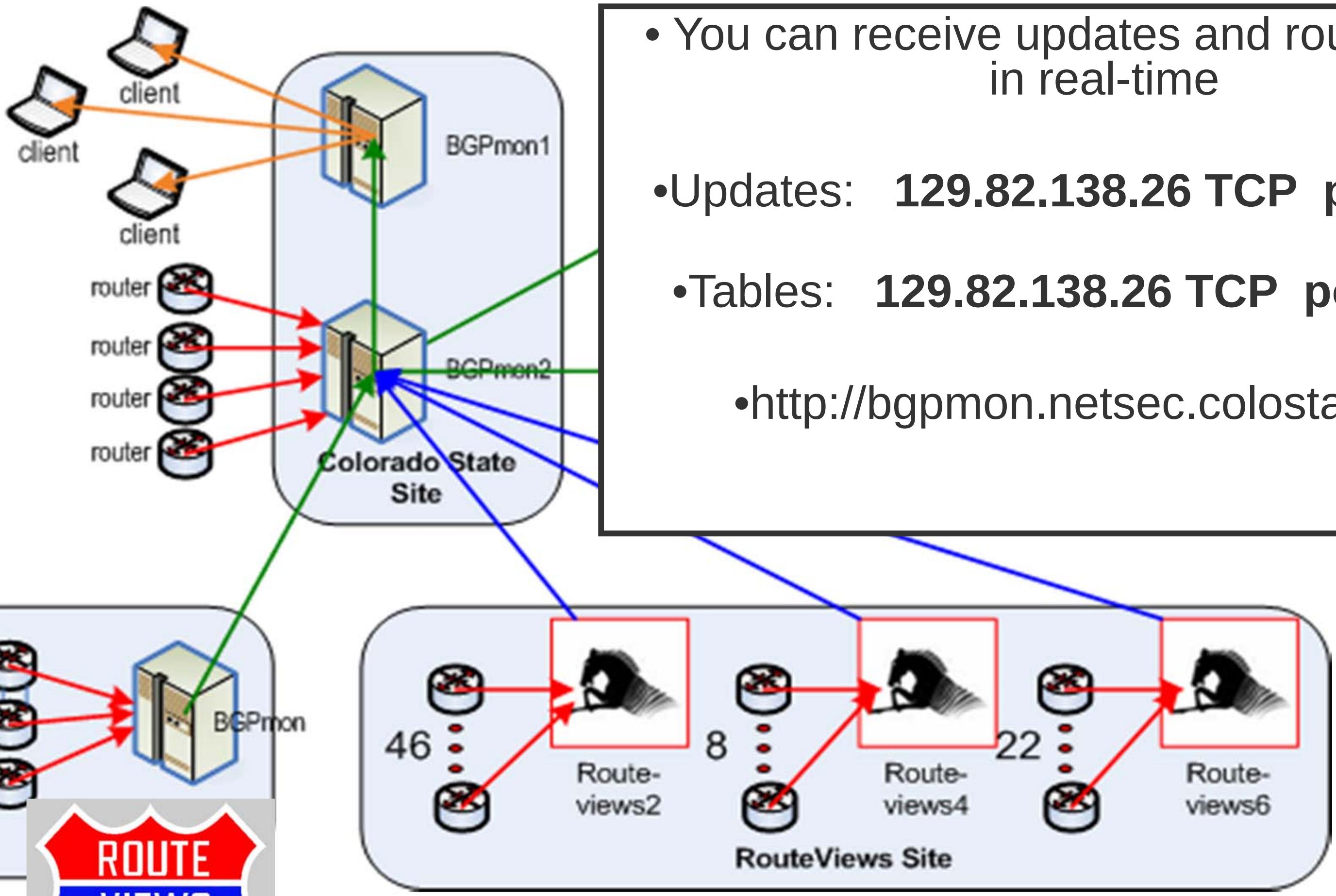
This TTA will yield technologies for the protection of key infrastructure via development of, and integration between, reliable capabilities such as:

- (1) Geographic mapping of Internet resources, (e.g., IPV4 or IPV6 addresses, hosts, routers, DNS servers, either wired or wireless), to GPS-compatible locations (latitude/longitude).
- (2) Logically and/or physically connected maps of Internet resources (IP addresses, hosts, routers, DNS servers and possibly other wired or wireless devices).
- (3) Detailed maps depicting ISP peering relationships, and matching IP address interfaces to physical routers.

Internet Measurement / Attack Modeling

- (4) Monitoring and archiving of BGP route information.
- (5) Development of systems achieving improvement to the security and resiliency of our nation's cyber infrastructure.
- (6) Monitoring and measurement applied to detection and mitigation of attacks on routing infrastructure, and supporting the development and deployment of secure routing protocols.
- (7) Monitoring and measurement contributing to understanding of Domain Naming System (DNS) behavior, both in terms of its changing role in distributed Internet scale malware activities, such as botnets, and DNS's behavior as a system under change through DNSSEC and other potential changes affecting the root level.

RouteViews Data in Real-Time



- You can receive updates and routing tables in real-time

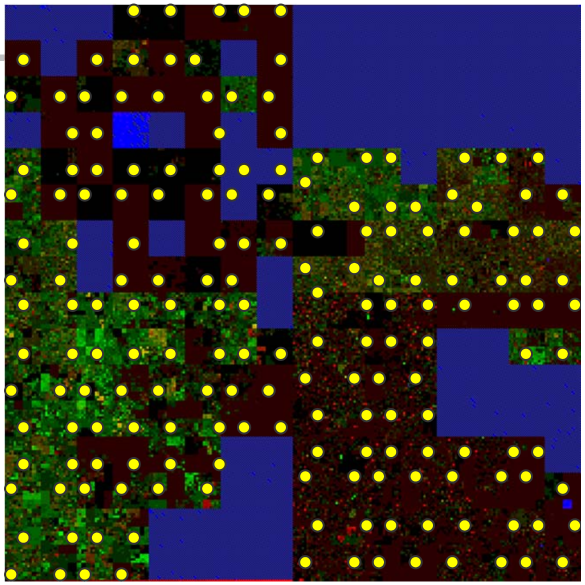
•Updates: **129.82.138.26 TCP port 50001**

•Tables: **129.82.138.26 TCP port 50002**

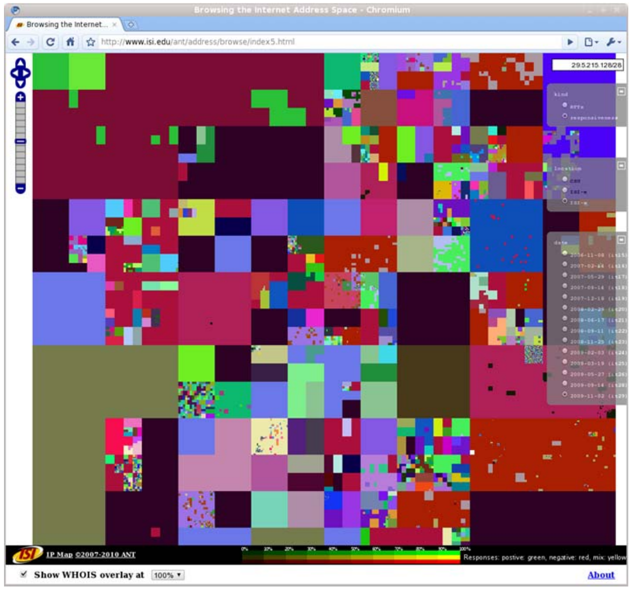
•http://bgpmon.netsec.colostate.edu

AMITE: New Results and Conclusions

IP hitlist evaluation



address visualization
improvements



Browsing the Internet Address Space - Chromium

Browsing the Internet...

http://www.isi.edu/ant/address/browse/index5.html

29.5.215.128/28

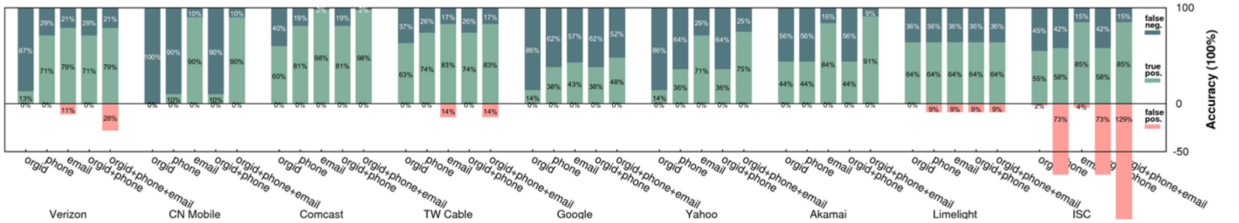
IP Map ©2007-2010 ANT

Responses: postive: green, negative: red, mix: yellow

☑ Show WHOIS overlay at 100% ▾

About

AS-to-org. mapping



http://www.isi.edu/ant/

U.S. Department of Homeland Security

Homeland Security

DHS S&T BAA

- Industry Day – Nov 17, 2010
  - https://www.fbo.gov/index?s=opportunity&mode=form&id=3459d2180c7625e61fff3e2764b7f78d&tab=core&_cview=0
  - Over 675 attendees
- BAA 11-02 posted Wed. Jan. 26
  - https://www.fbo.gov/index?s=opportunity&mode=form&id=6ab2a491c47ca628d3feb0f54ecee7be&tab=core&_cview=1
  - **https://baa2.st.dhs.gov** – Site for registration and submission of white papers and proposals
  - http://www.cyber.st.dhs.gov

DHS S&T BAA Schedule

- **White Paper Registration – Feb 14, 2011**
- White Papers – Due March 1, 2011
- Proposal Notification – April 12, 2011
- Full Proposals – Due May 26, 2011
- Funding Notification – July 18, 2011
- Contract Awards NLT Oct 31, 2011

BAA 11-02 Technical Topic Areas (TTAs)

● TTA-1	Software Assurance	*DHS, FSSCC*
● TTA-2	Enterprise-level Security Metrics	*DHS, FSSCC*
● TTA-3	Usable Security	*DHS, FSSCC*
● TTA-4	Insider Threat	*DHS, FSSCC*
● TTA-5	Resilient Systems and Networks	*DHS, FSSCC*
● TTA-6	Modeling of Internet Attacks	*DHS*
● TTA-7	Network Mapping and Measurement	*DHS*
● TTA-8	Incident Response Communities	*DHS*
● TTA-9	Cyber Economics	*CNCI*
● TTA-10	Digital Provenance	*CNCI*
● TTA-11	Hardware-enabled Trust	*CNCI*
● TTA-12	Moving Target Defense	*CNCI*
● TTA-13	Nature-inspired Cyber Health	*CNCI*
● TTA-14	Software Assurance MarketPlace (SWAMP)	*S&T*

Summary

- DHS S&T continues with an aggressive cyber security research agenda
  - Working with the community to solve the cyber security problems of our current (and future) infrastructure
    - Outreach to communities outside of the Federal government, i.e., building public-private partnerships is essential
  - 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

Edward Rhyne

Program Manager

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

edward.rhyne@dhs.gov

202-254-6121

For more information, visit

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