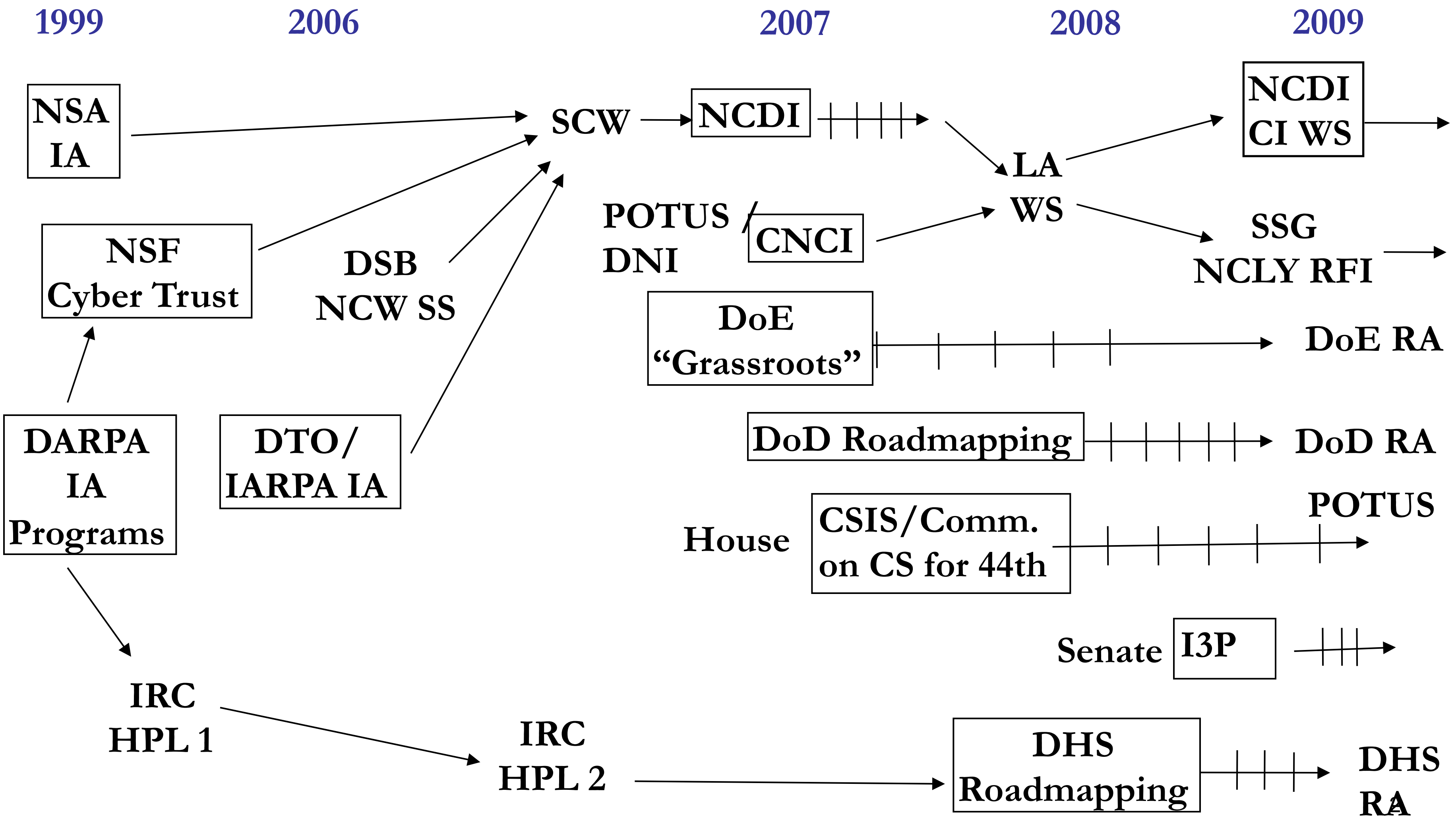
US Federal Cyber Security Research Program

Federal Cybersecurity R&D: National Dialogue



1999

2006

2007

2008

2009

NSA IA

SCW

NCDI

NCDI CI WS

NSF Cyber Trust

DSB NCW SS

LA WS

POTUS / DNI

CNCI

SSG NCLY RFI

DoE "Grassroots"

DoE RA

DARPA IA Programs

DTO/ IARPA IA

DoD Roadmapping

DoD RA

House

CSIS/Comm. on CS for 44th

POTUS

Senate

I3P

IRC HPL 1

IRC HPL 2

DHS Roadmapping

DHS RA

Vision of R&D under CNCI

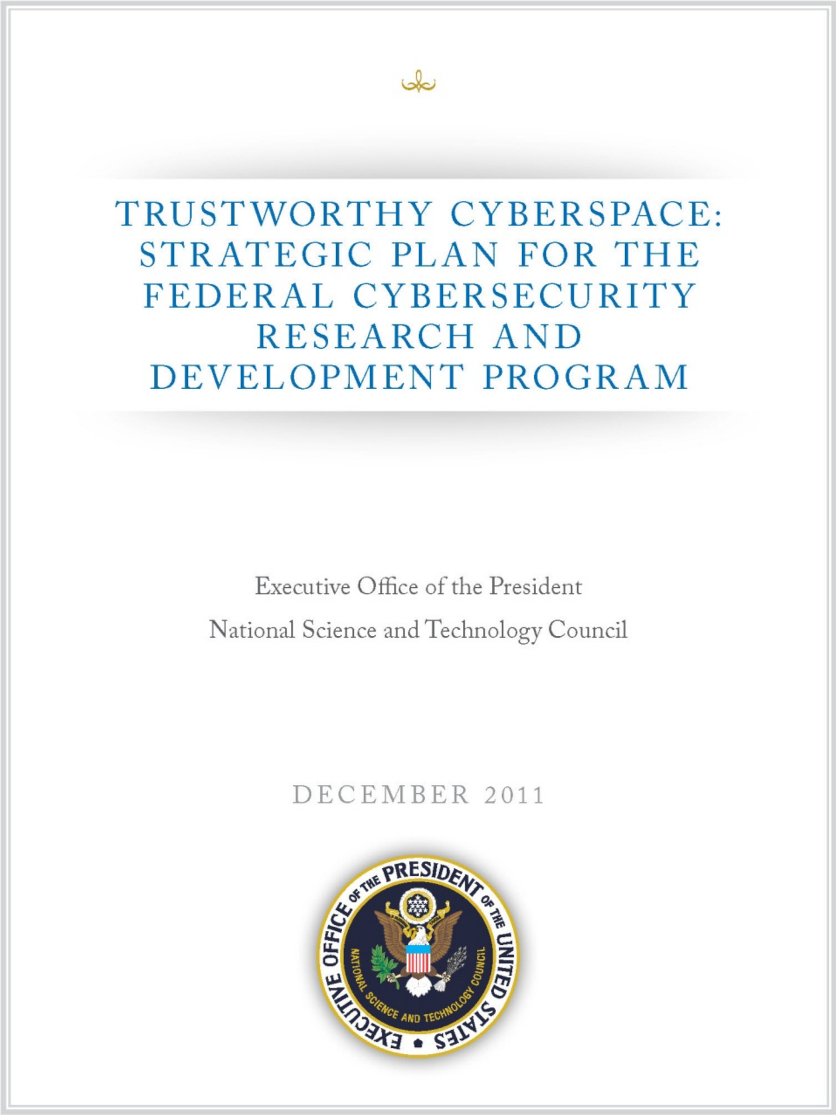
Comprehensive National Cybersecurity Initiative (CNCI), Presidential Directive, 2008

“to initiate coordinated set of Federal government activities over the next 10 years to:
to transform the cyber infrastructure so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances.”

Leap-Ahead/Game-Change R&D
Expand cybersecurity R&D in
high-risk, high-return areas

Coordination
NITRD
CSIA R&D SSG
CSIA IWG
SCORE

Federal Cybersecurity R&D Strategic Plan



TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

Executive Office of the President

National Science and Technology Council

DECEMBER 2011

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

- Research Themes
- Science of Cyber Security
- Support for National Priorities
- Transition to Practice

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

R&D Coordination Through Themes

- Hard Problem Lists ≠ Research Strategy
- Federal research strategy focuses on underlying causes of cyber in-security
- Themes provide shared vision of desired end state
- Themes compel a new way of operating / doing business
- Established through robust community discussion of what matters
- Themes recognize that independent thinking is vital to good research

Research Themes

- Tailored Trustworthy Spaces
  - Supporting context specific trust decisions
- Moving Target
  - Providing resilience through agility
- Cyber Economic Incentives
  - Providing incentives to good security
- Designed-In Security
  - Developing secure software systems
- Annually re-examine themes
  - Enrich with new concepts
  - Provide further definition or decomposition

Tailored Trustworthy Spaces Paradigm

- Users can select/create different environments for different activities satisfying variety of operating capabilities
  - Confidentiality, anonymity, data and system integrity, provenance, availability, performance
- Users can negotiate with others to dynamically create new environments with mutually agreed characteristics and lifetimes
- Users can base trust decisions on verifiable assertions

Moving Target Paradigm

- All systems are compromised; perfect security is unattainable
- Objective is to continue safe operation in a compromised environment, to have systems that are defensible, rather than perfectly secure
- MT provides controlled change across multiple system dimensions to:
  - Increase uncertainty and apparent complexity for attackers, reduce their windows of opportunity, and increase their costs in time and effort
  - Increase resiliency and fault tolerance within a system

Designed-In Security Paradigm

- Designing and developing SW systems that are resistant to attacks
- Require verifiable assurance about system’s attack-resistance to be natively part of the SW lifecycle
- Enable reasoning about a diversity of quality attributes (security, safety, reliability, etc.) and the required assurance evidence
- Stimulate further developments in methods and tools for detecting flaws in SW

Cyber Economic Incentives

- A focus on what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - Promotion of science-based understanding of markets, decision-making and investment motivation
  - Theories and models of the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models

Strategic Thrusts

- Research Themes
  - TTS, MT, DIS, CEI
- Science of Cyber Security
- Support for National Priorities
- Transition to Practice

Science of Cyber Security

- A major research initiative on the *science of security* that
  - Organizes the knowledge in the field of security
  - Investigates fundamental laws
  - Results in a cohesive understanding of underlying principles to enable investigations that impact large-scale systems
  - Enables repeatable experimentation
  - Supports high-risk explorations needed to establish such a scientific basis
  - Forms public-private partnerships of government agencies, universities, and industry

Drivers for game-change solutions

- Basing trust decisions on verifiable assertions
- Shifting burden of processing onto attackers
- SW (system) lifecycle must natively incorporate verifiable assurance about system’s attack-resistance
- Facilitating sound cybersecurity incentives and enabling effective business & personal cybersecurity decisions

For More Information

Tomas Vagoun, PhD
CSIA IWG Technical Coordinator

National Coordination Office for
Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230
Tel: (703) 292-4873
vagoun@nitrd.gov

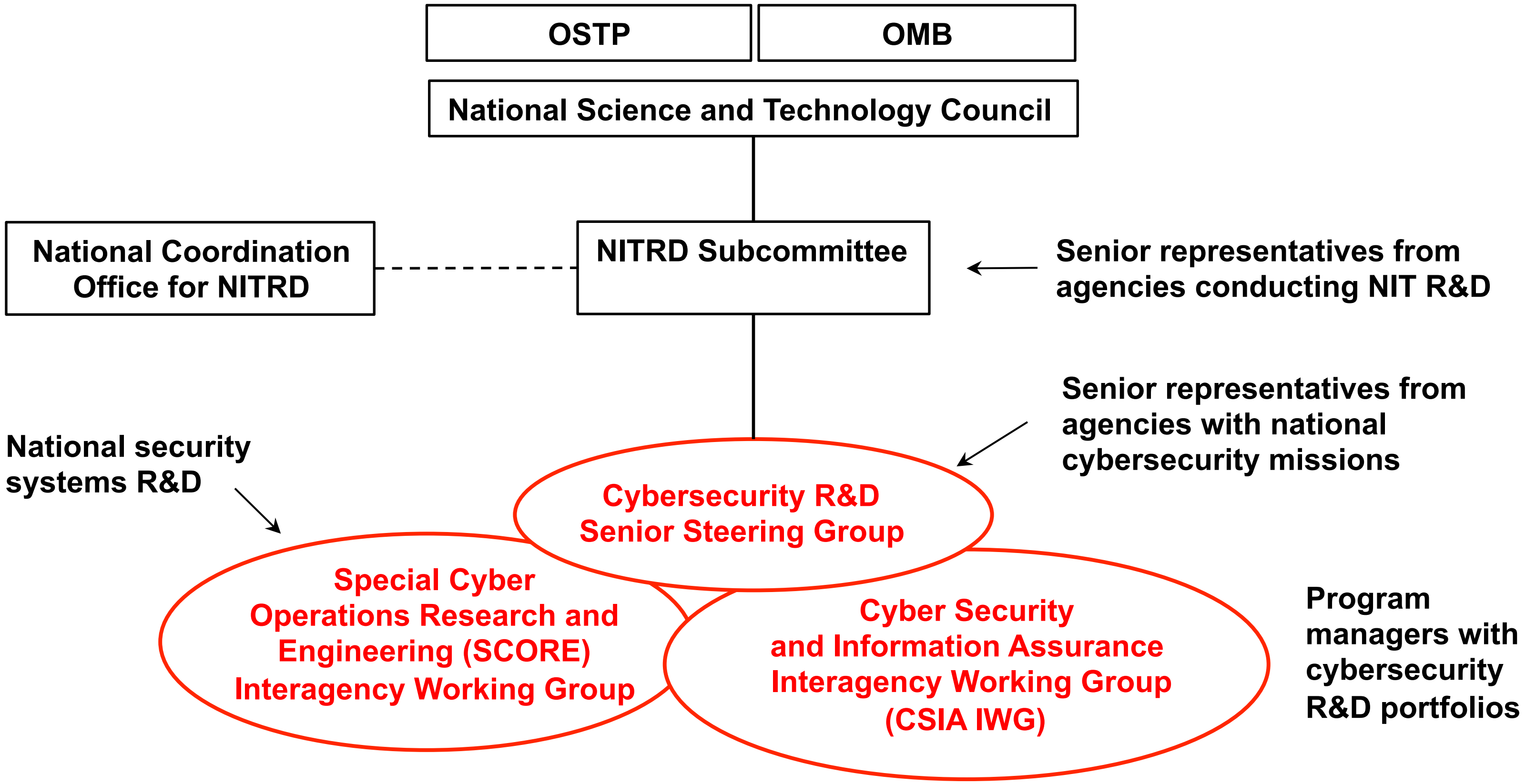
http://www.nitrd.gov
http://cybersecurity.nitrd.gov

Extra Slides

NITRD Program

- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Supports NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
- Scope
  - Approximately $4B/year across 15 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)
  - Established by the High-Performance Computing Act of 1991

NITRD Structure for US Federal Cybersecurity R&D Coordination



OSTP

OMB

National Science and Technology Council

National Coordination Office for NITRD

NITRD Subcommittee

Senior representatives from agencies conducting NIT R&D

Senior representatives from agencies with national cybersecurity missions

National security systems R&D

Cybersecurity R&D Senior Steering Group

Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group

Cyber Security and Information Assurance Interagency Working Group (CSIA IWG)

Program managers with cybersecurity R&D portfolios

Selected NITRD Agency Budgets in CSIA R&D

Selected Agencies	Cyber Security & Information Assurance (CSIA) R&D (Unclassified)	
	FY 2012 Estimates	FY 2013 Requests
DARPA	$223M	$247M
OSD, NSA and DoD Service Research Organizations	$145M	$157M
NSF	$98M	$114M
NIST	$47M	$55M
DHS S&T	$43M	$61M
DOE	$33M	$33M
Total	$589M	$667M

Source: "NITRD Supplement to the President's Budget FY 2013," http://www.nitrd.gov/PUBS/2013supplement/FY13NITRDSupplement.pdf

TTS R&D Program Examples

- Trusted foundation for cyberspace operations [OSD and Service Labs]
- High assurance security architectures [NSA, ONR, AFRL, NIST]
- Content and Context Aware Trusted Router (C2TR) [AFRL]
- Information Security Automation Program [NIST, NSA, DHS]
  - Security Content Automation Protocol (SCAP)
- Access Control Policy Machine [NIST]
- Military Networking Protocol (MNP) program [DARPA]
- High-Level Language Support for Trustworthy Networks [NSF]

MT R&D Program Examples

- Polymorphic Enclaves and Polymorphic Machines [AFRL]
- Self Regenerative, Incorruptible Enterprise that Dynamically Recovers with Immunity [AFRL]
- Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) [DARPA]
- Cyber Camouflage, Concealment, and Deception [DARPA]
- Morphing Network Assets to Restrict Adversarial Reconnaissance (Morphinator) [Army]
- Defensive Enhancements for Information Assurance Technologies (DEFIANT) [Army]
- Robust Autonomic Computing Systems [ONR]

CEI R&D Program Examples

- Secure and Trustworthy Cyberspace (SaTC) Program (FY12 Solicitation)
  - NSF Computer & Information Science & Engineering Directorate + NSF Social, Behavioral & Economic Sciences Directorate

DIS R&D Program Examples

- Survivable Systems Engineering [OSD/SEI CERT]
- Trusted Computing [DARPA, NSA, OSD, NIST]
- Software Development Environment for Secure System Software & Applications [ONR]
- META (flows, tools, and processes for correct-by-construction system design) [DARPA]
- Software Assurance Metrics And Tool Evaluation (SAMATE) [DHS, NIST]

Science of Security Program Examples

- AFOSR 2011 Science of Security MURI
  - Stanford, Berkeley, Cornell, CMU, U of Penn
- NSA Science of Security Lablets
  - UIUC, NC State, CMU
- NSF TRUST Program components
  - Berkeley, CMU, Cornell, San Jose SU, Stanford, Vanderbilt

Support for National Priorities

- Goals
  - Maximize cybersecurity R&D impact to support and enable advancements in national priorities
- Examples of Supported National Priorities
  - Health IT
  - Smart Grid
  - Financial Services
  - National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - National Initiative for Cybersecurity Education (NICE)

Transition to Practice

- Concerted effort to get results of federally funded research into broad use
  - Integrated demos
  - Conferences and workshops
  - “Matchmaking” efforts
    - Among Agencies
    - Between research and product
  - Potential funding for last mile