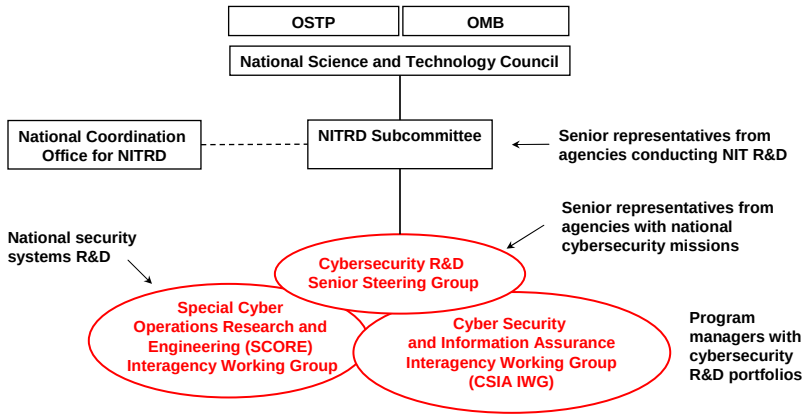
NITRD Program

- 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 14 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

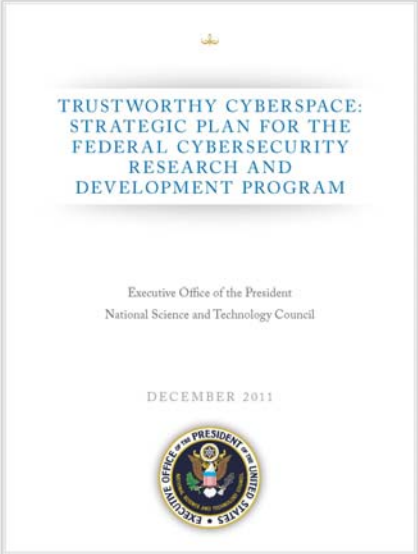
NITRD Structure for US Federal Cybersecurity R&D Coordination



Coordinated Effort on Game-Changers

- It's about trustworthiness of digital infrastructure
  - Security, reliability, resiliency, privacy, usability
  - How can we:
    - Enable risk-aware safe operations in compromised environments
    - Minimize critical system risk while increasing adversaries' costs and exposure
    - Support informed trust decisions, necessitating flexible security strategies, and allowing for effective risk/benefit analyses and implementations
- Strong commitment to focus on game-changing technologies for coordinated cybersecurity R&D agenda

Federal Cybersecurity R&D Strategic Plan



- 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

- Theme ≠ Hard Problem
- Themes provide shared vision of desired end state
- Themes compel a new way of operating / doing business
- Themes attack underlying causes to bring about changes
- 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

In the physical world, we operate in many spaces with many characteristics

- Home, school, workplace, shopping mall, doctor's office, bank, theatre
- Different behaviors and controls are appropriate in different spaces

Yet we tend to treat the cyber world as a homogenous, undifferentiated space

The vision is of a flexible, distributed trust environment that can support functional, policy, and trustworthiness requirements arising from a wide spectrum of activities in the face of an evolving range of threats

TTS 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 create new environments with mutually agreed characteristics and lifetimes
- Basing trust decisions on verifiable assertions

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]

Moving Target

- 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

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
- Shift burden of processing onto attackers

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]

Cyber Economics & Incentives

- A focus on what impacts cyber economics and what incentives can be provided to enable ubiquitous security:
  - New theories and models of investments, markets, and the social dimensions of cyber economics
  - Data, data, and more data with measurement and analysis based on that data
  - Improved SW development models and support for “personal data ownership”

CEI Paradigm

- Promotion of science-based understanding of markets, decision-making and investment motivation
  - Security deployment decisions based on knowledge, metrics, and proper motivations
  - Promote the role of economics as part of that understanding
- Creation of environments where deployment of security technology is balanced
  - Incentives to engage in socially responsible behavior
  - Deterrence for those who participate in criminal and malicious behavior

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

Designed-In Security

- Designing and developing SW systems that are resistant to attacks
- Generating assurance artifacts to attest to the system's capabilities to withstand attacks

Designed-In Security Paradigm

- Require verifiable assurance about system's attack-resistance to be natively part of the SW design, development, and evolution 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

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]

Strategic Thrusts

- Research Themes
  - TTS, MT, CEI, DIS
- ⇨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

Some Potential Science of Security Research Topics

- Methods to model adversaries
- Techniques for component, policy, and system composition
- A control theory for maintaining security in the presence of partially successful attacks
- Sound methods for integrating the human in the system: usability and security
- Quantifiable, forward-looking, security metrics (using formal and stochastic modeling methods)
- Measurement methodologies and testbeds for security properties
- Development of comprehensive, open, and anonymized data repositories

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

Drivers for next-generation 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

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