Challenges of Engineering Cybersecurity: Government Perspective

Tomas Vagoun
Cybersecurity R&D Coordinator

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)
  - Established by the High-Performance Computing Act of 1991
- Scope
  - Approximately $4B/year across 16 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management
  - High Confidence Software and Systems
  - High End Computing
  - Large Scale Networking
  - Software Design and Productivity
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development

CSIA R&D Budgets (Unclassified) in NITRD

Selected Agencies	Cyber Security & Information Assurance (CSIA) R&D (Unclassified)	
	FY 2014 Actual	FY 2016 Requests
DARPA	$265M	$298M
OSD, DoD Service Research Organizations	$182M	$156M
NSF	$103M	$112M
DHS	$78M	$69M
NIST	$62M	$73M
DOE	$31M	$30M
Total	$721M	$738M

Source: "NITRD Supplement to the President's Budget FY 2016," https://www.nitrd.gov/pubs/2016supplement/FY2016NITRDSupplement.pdf

Challenge

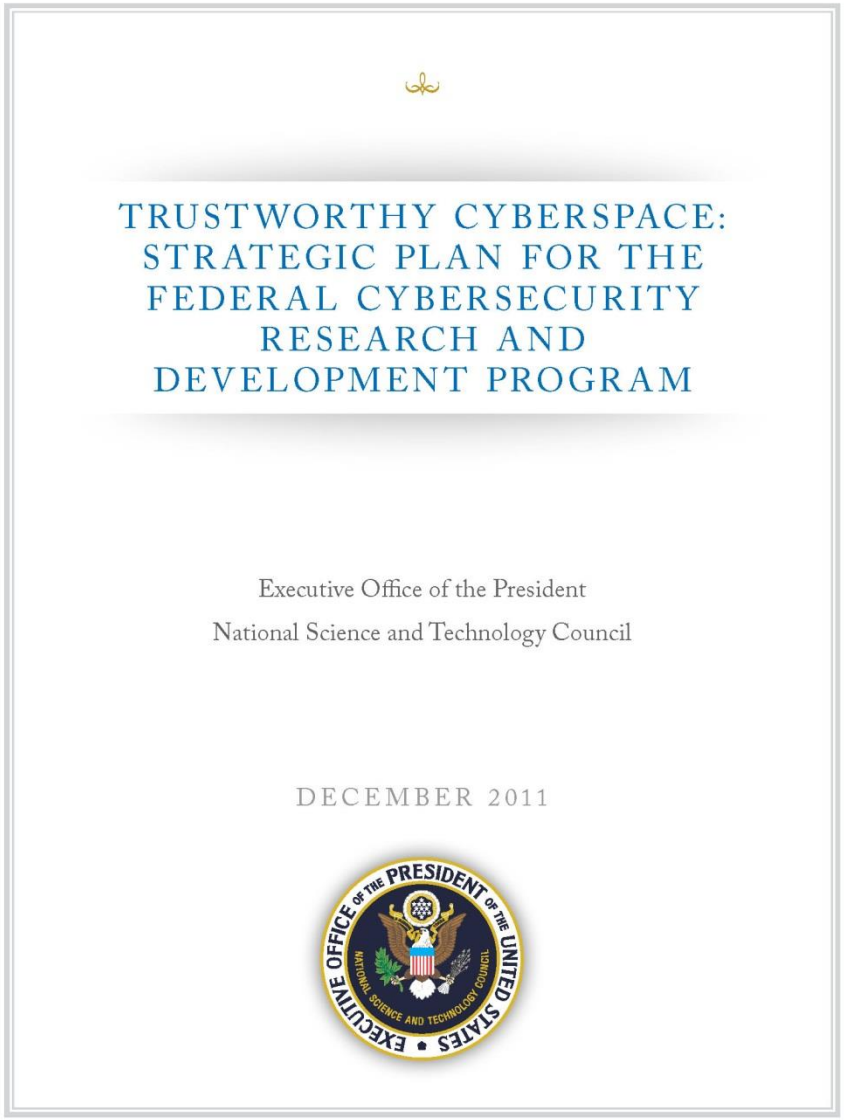
Given limited/finite financial resources, what should be the goals for Federal Government's basic research in cybersecurity?

Underlying Cybersec Deficiencies

Systems are static and homogeneous	→	Great ROI on attack reuse
Users take actions in absence of verified trust	→	We don't know when we've been had
Weak capabilities to measure, assess, and maintain SW security	→	Security fix-loop is slower than attack development-loop: always one (n) steps behind attackers
Cybersecurity is substantially an economic, social, and behavioral issue	→	Technical fixes may not be the most effective solutions

Need game-changing, not incremental solutions

Federal Cybersecurity R&D Strategic Plan



- Research Themes
  - Tailored Trustworthy Spaces
  - Moving Target
  - Cyber Economic Incentives
  - Designed-In Security
- 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

Strategic Plan Research Themes

- Moving Target
  - Providing resilience through agility
- Tailored Trustworthy Spaces
  - Supporting context specific trust decisions
- Designed-In Security
  - Developing secure software systems
- Cyber Economic Incentives
  - Providing incentives to good security
- Science of Security
  - Improving our understanding of fundamentals that underpin cybersecurity

Moving Target Defense

Monoculture Problem

- Identical systems → same attack disables all systems
- Unchanging systems → same attack works repeatedly

↳ Need dynamic diversity that makes systems unique and increases work for attackers

Long Repair-Cycle Problem

- Long lead time to patch
- Patch cycle is slower than attack development cycle

↳ Need adaptation

Biology to the rescue?

Biology Inspiration for Security

Fortress	Biological
Impenetrable (hopefully) barrier with unprotected inside	Many partial and overlapping barriers
Monolithic	Heterogeneous
Rigid	Adaptation is a core mechanism
Need perfect components	Fallible components
Design reflects scarcity of resources	Abundance of resources
Evolutionary pressure: price-performance tradeoff	Evolutionary pressure: survivability
No system-wide survivability	Diversity for population survival, evolution

Example: DARPA CRASH Program

Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) Program

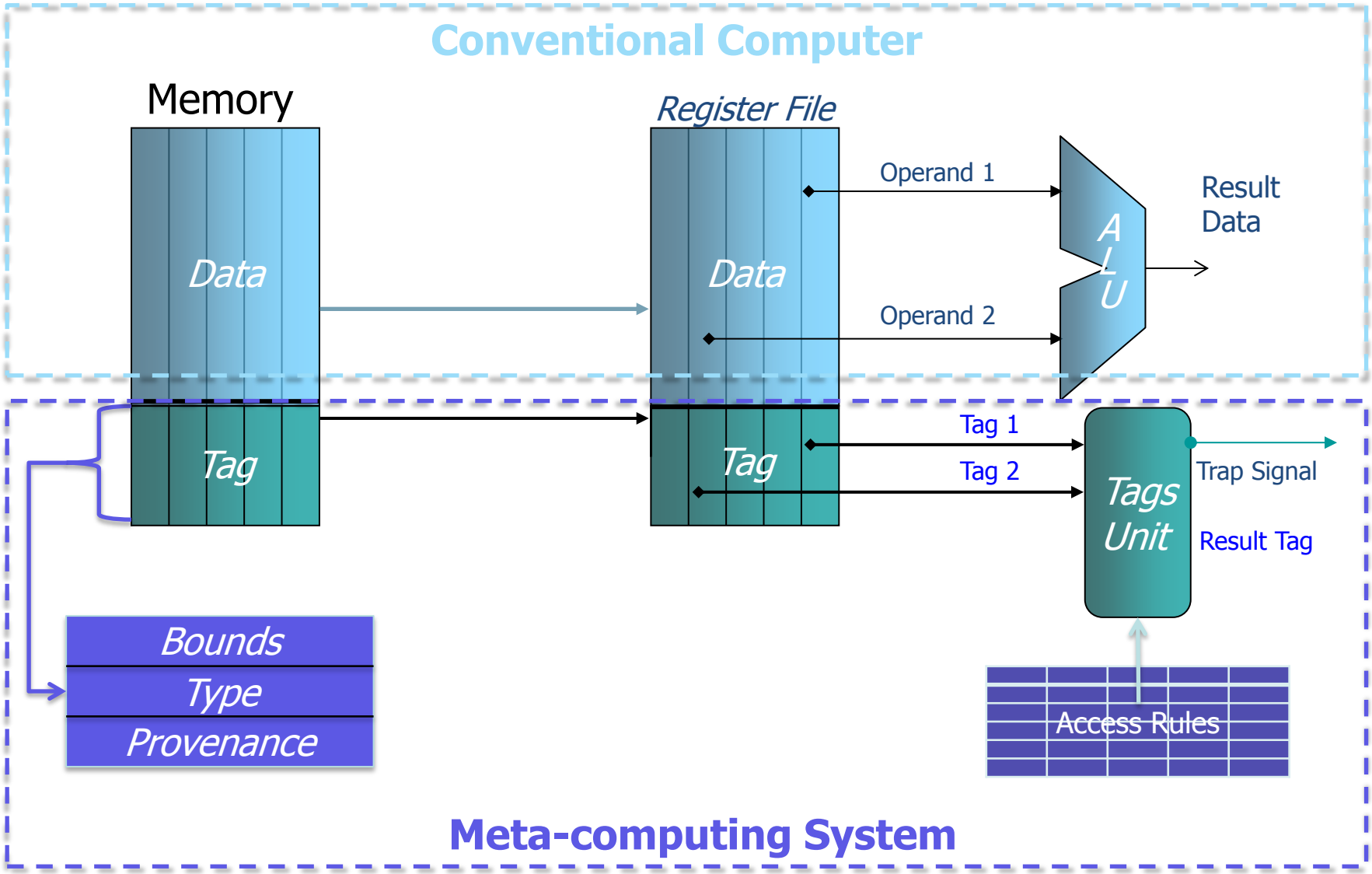
- Rethink computing systems → immune systems inspiration
- Design systems that can adapt and continue providing services after an attack, learn from attacks, and repair themselves

Rethink

- Hardware → Tag every piece of data and enforce access restriction on data in HW
- Programming languages → Incorporate rules about information flows and access rights
- Operating systems → Enforce security properties specified in the code
- Architecture → Redesign OS as independent modules suspicious of each other

Cybersecurity Problem	Biological Approach	DARPA CRASH
Systems are easily penetrated	Innate immunity: fast reacting defenses to known pathogens	New hardware and OS that eliminate common vulnerabilities
Repair is costly	Adaptive immunity: slower reacting defenses to unknown pathogens + Adaptation	Adaptive software that determines causes of vulnerabilities and dynamically repairs flaws
Computing homogeneity: large pool of targets, large ROI for attackers	Diversity: sustains population survival	Techniques that increase entropy, make systems unique, and raise work factor for attackers: instruction set randomization, address space randomization, functional redundancy

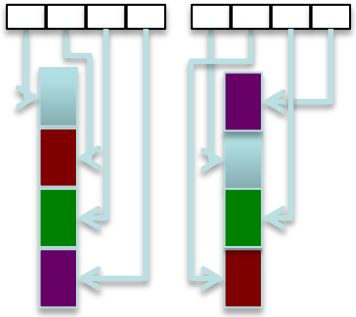
DARPA CRASH Innate Immunity: An Example Hardware Solution



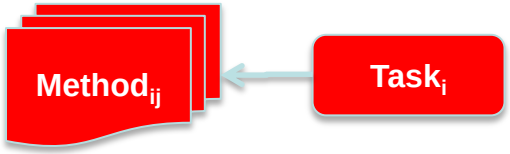
Source: DARPA CRASH Program

Dynamic Diversity Examples

Address space layout randomization

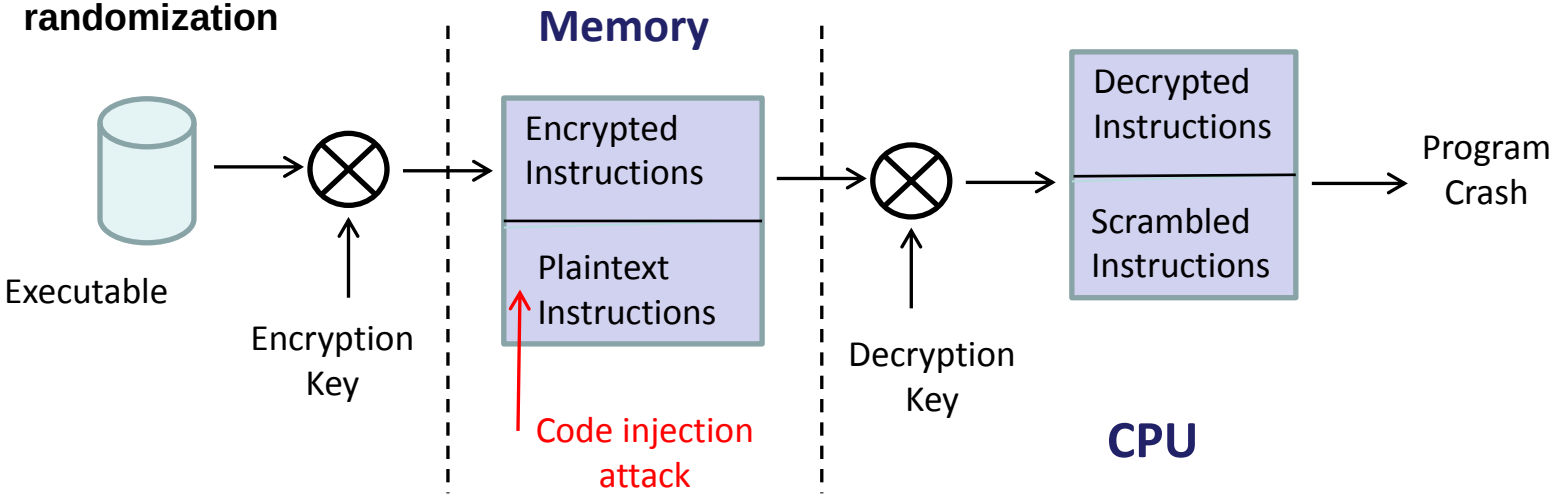


Functional Redundancy



Dynamic diversification techniques make systems look the **same** to the users but vary low-level details that attackers exploit, making each system look **different** to the attackers.

Instruction set randomization



Moving Target Defense: Challenge

MTD Dimension	Examples of MTD Techniques
Systems of Systems	Virtualization, Cloud Computing, Machine Rotations
Data	Secure Distributed Data Chunking, Self-aware Data
Networks	IP Hopping, Dynamic DSN, Dark IP Space
Software	Diversity in Software, Just-in-time Compiling
System	Instruction Set Randomization, Address Space Layout Randomization, OS Diversity
Hardware	Hardware Diversity, Multi-core Processing

↑ Agility
↑ Diversity
↑ Redundancy

↑ Complexity
↑ Support overhead

↓ Decreased attack ROI
↓ Additional work for attackers

=  Better Security

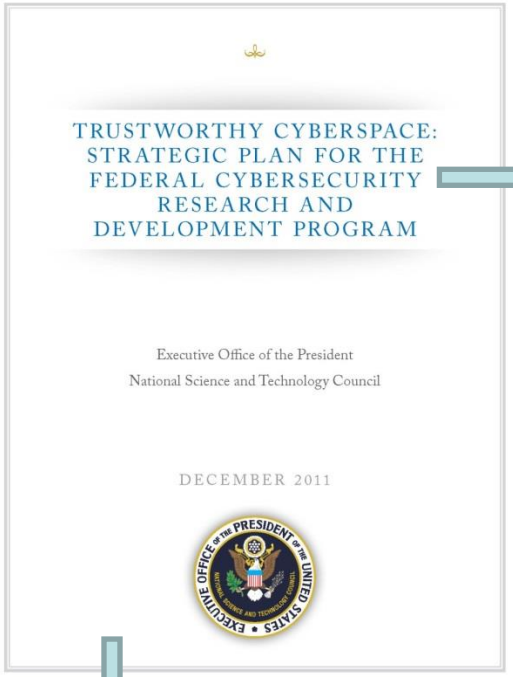
Do we understand:

- Costs (complexity) vs. Benefits (security)?
- Measurements of security benefits?
- Provable security properties?

FROM:
Patch & Pray

TO:
Standardized metrics
Repeatable experiments
Hypothesis testing
Engineering
Science

Need Focus on Science of Security



Priority Goal:
Developing Scientific
Foundations

How to nudge the creation of a science?

NSA Science of Security Initiative

Science of Security

0100
1011
0100

LABLETS

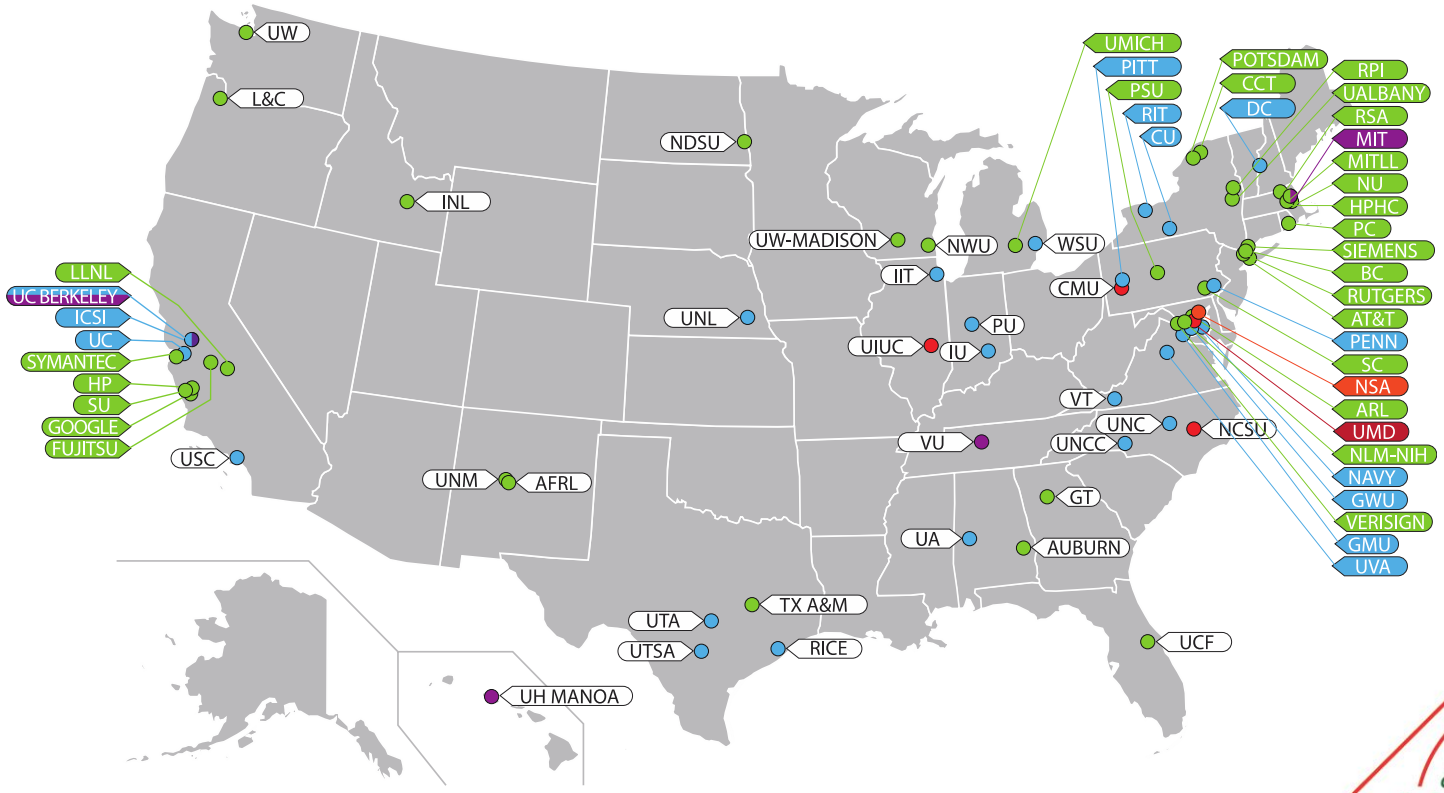
CMU, UIUC, NC State, UMD

5 Hard Problems

- Resilient Architectures
- Scalability and Composability
- Secure Collaboration
- Metrics
- Human Behavior

Other examples:
AFOSR: Science of Cyber Security MURI
ARL: Science for Cyber Portfolio program
OSD: Cyber Measurement Campaign

Science of Security Growing Community



2015 SYMPOSIUM & BOOTCAMP URBANA IL HOTSOS ON THE SCIENCE OF SECURITY

National Security Agency **Lablet (4)** **Sub-Lablet (26)**

Collaborator (68)

Advancing Science of Security

Annual NSA Competition

http://cps-vo.org/group/SoS

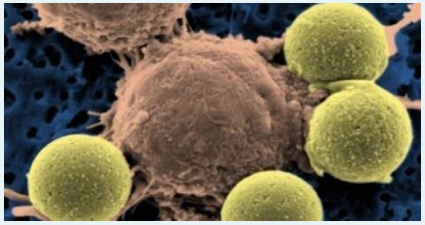
Take-Aways

I Want You
To Help
Build Game-Changing
Cybersecurity Solutions

Identify Problems
Systems are static and homogeneous
Users take actions without verified trust
Security is often added-on, not built-in
Cybersecurity is also an economic, social, and behavioral issue

Execute USG R&D Strategy
Moving Target (Defense)
Tailored Trustworthy Spaces
Designed-In Security
Cyber Economic Incentives

Innovate



Strengthen Science and Engineering

Some Useful Links

- Report on Implementing the Federal Cybersecurity Research and Development Strategy (2014)
  - http://www.nitrd.gov/PUBS/ImplFedCybersecurityRDStrategy-June2014.pdf
- Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (2011)
  - http://www.nitrd.gov/SUBCOMMITTEE/csia/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf
- NITRD Supplement to the President's Budget (FY 2016)
  - https://www.nitrd.gov/pubs/2016supplement/FY2016NITRDSupplement.pdf

Contact Information

Tomas Vagoun, PhD
Cybersecurity R&D 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