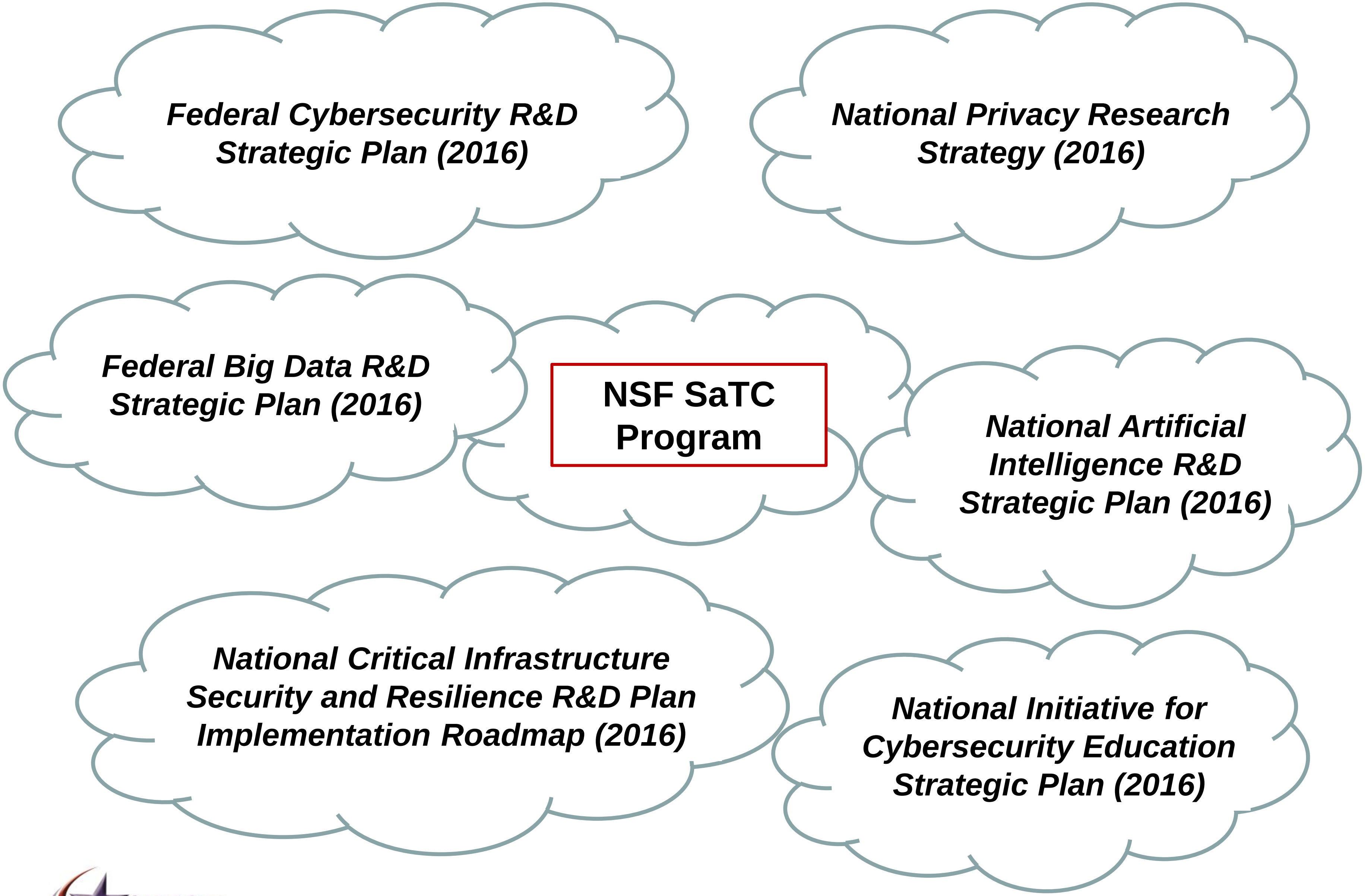
**Networking and Information Technology Research and Development Program**

# Federal Cybersecurity and Privacy R&D Strategic Plans

## 2017 NSF SaTC PI Meeting Panel

| | |
|---|---|
| **Lorrie Cranor** | Chief Technologist, FTC |
| **Erwin Gianchandani** | Deputy Assistant Director, NSF/CISE |
| **Erin Kenneally** | Program Manager, DHS S&T |
| **Naomi Lefkovitz** | Senior Privacy Policy Advisor, NIST |
| **Paul Lopata** | Associate Director, Cyber Technologies, OSD |
| **Bill Newhouse** | Deputy Director, NIST/NICE |
| **Tomas Vagoun** | R&D Coordinator, NITRD |



*Federal Cybersecurity R&D Strategic Plan (2016)*

*National Privacy Research Strategy (2016)*

*Federal Big Data R&D Strategic Plan (2016)*

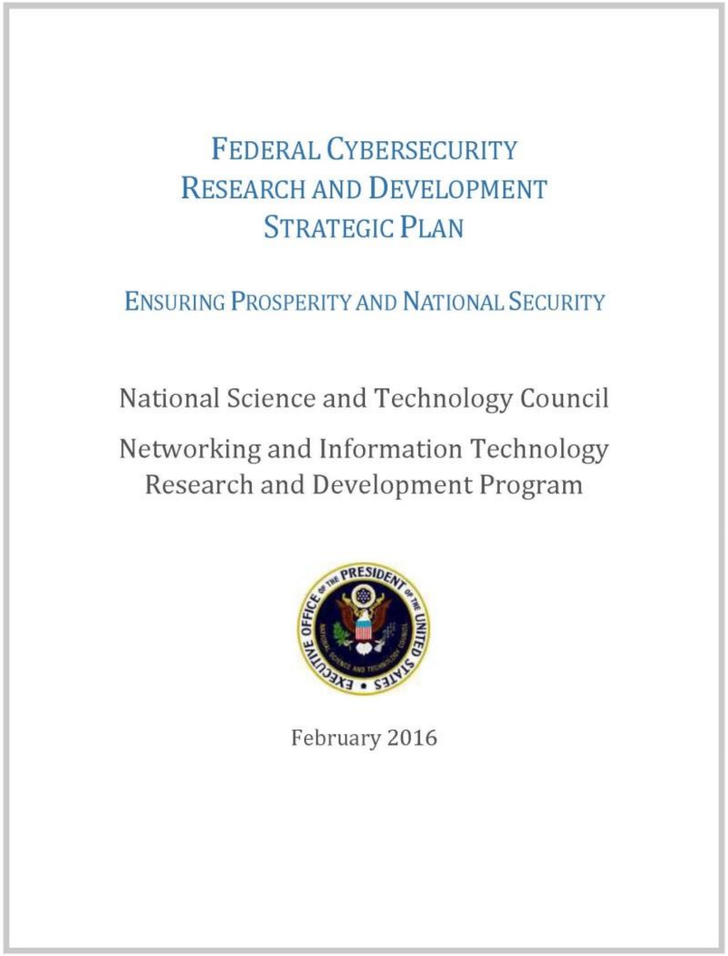
**NSF SaTC Program**

*National Artificial Intelligence R&D Strategic Plan (2016)*

*National Critical Infrastructure Security and Resilience R&D Plan Implementation Roadmap (2016)*

*National Initiative for Cybersecurity Education Strategic Plan (2016)*

# For Today's Discussion



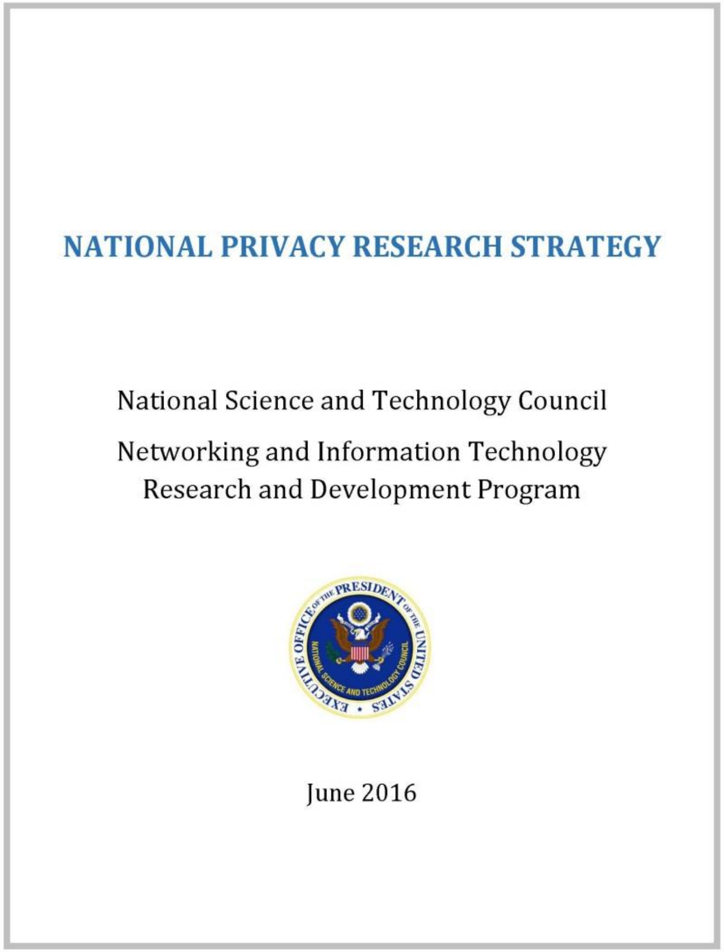
FEDERAL CYBERSECURITY
RESEARCH AND DEVELOPMENT
STRATEGIC PLAN

ENSURING PROSPERITY AND NATIONAL SECURITY

National Science and Technology Council

Networking and Information Technology
Research and Development Program

February 2016



NATIONAL PRIVACY RESEARCH STRATEGY

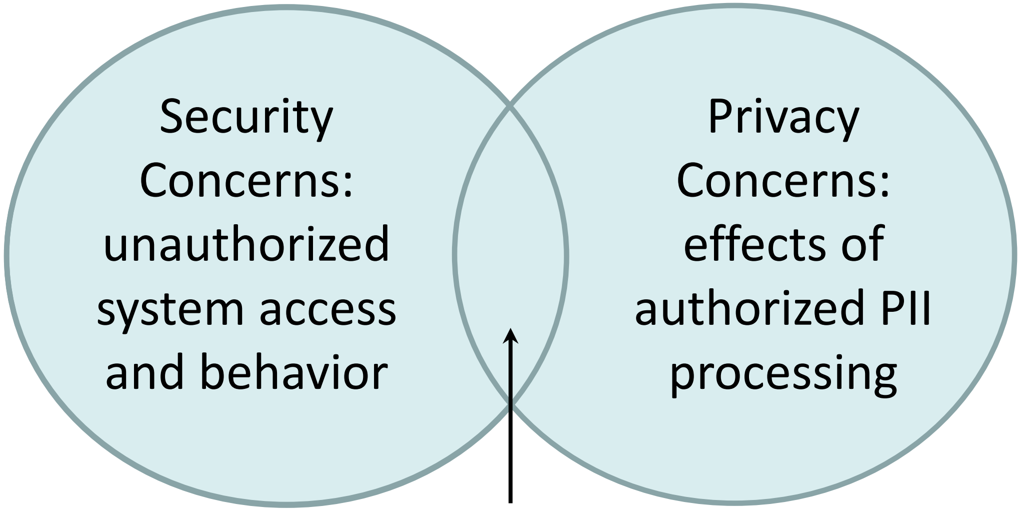
National Science and Technology Council

Networking and Information Technology
Research and Development Program

June 2016

# Information Security and Privacy

Security challenge: build systems that satisfy technical requirements



Security Concerns: unauthorized system access and behavior

Privacy Concerns: effects of authorized PII processing

Security of PII

Privacy challenge: build systems that satisfy social requirements: privacy expectations (norms and laws)

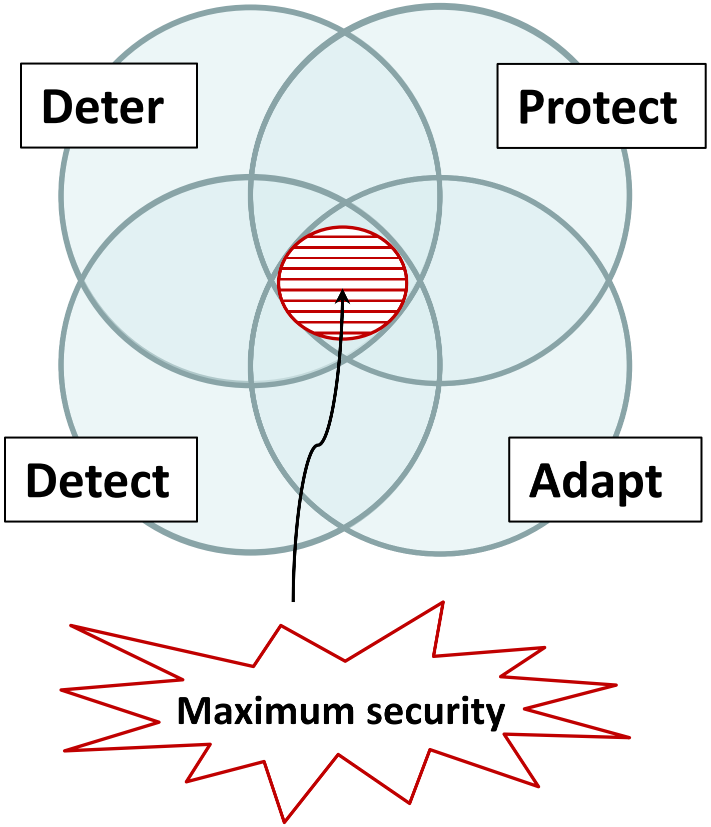
<u>Security Engineering Objectives</u>

- Confidentiality
- Integrity
- Availability
- Nonrepudiation
- …

<u>Privacy Engineering Objectives</u>

- Predictability (contextual integrity)
- Disassociability (unlinkability)
- Manageability (intervenability)
- Transparency
- …
- [see NIST IR 8062/Privacy Engineering]

# Focus for Federal Cybersecurity R&D



Federal Cybersecurity R&D Goals

- S&T for **effective and efficient risk management**
- S&T for **sustainably secure systems development and operation**
- S&T for **effective and efficient defensive deterrence**

Critical Dependencies

Success depends on advances in:

- Scientific foundations
- Risk management
- Human aspects
- Transition to practice
- Workforce development
- Infrastructure for research

# Key Challenges

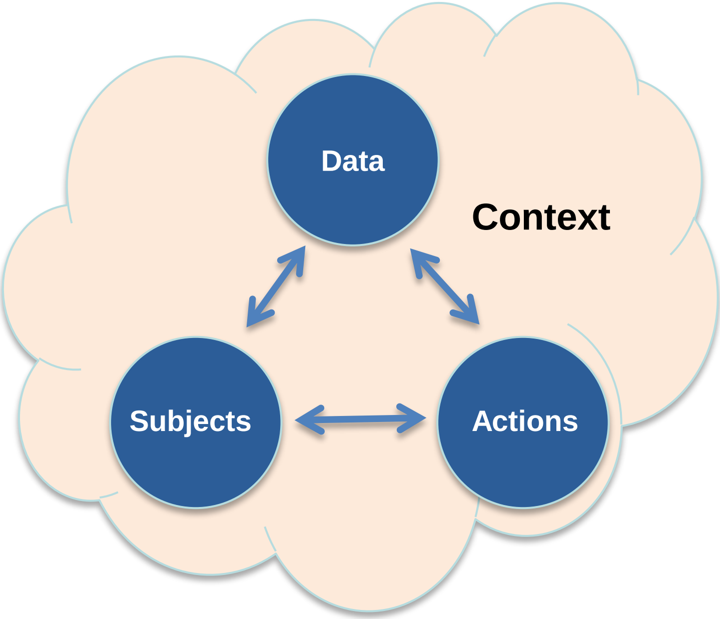
- Deter
  - Measurement of adversary level of effort, results, and risks
  - Effective and timely attribution, information sharing for attribution
  - Robust investigative tools
- Protect
  - Limit Vulnerabilities (Design for security, Build secure, Verify security, Maintain security, Verify authenticity)
  - Enforce Security Principles (Authenticate users & systems, Access controls, Cryptography)
  - Mitigate vulnerabilities
- Detect
  - Enable robust situational awareness
  - Identify weaknesses in systems
  - Reliably detect malicious cyber activities
- Adapt
  - Dynamic assessment
  - Adaptive response
  - Coordination at multiple scales

Progress requires strong focus on

**Evidence of Efficacy and Efficiency**

# Focus for Federal Privacy R&D

## Privacy As



## Role of Research

- Understand the nature of privacy
  - Privacy concerns solitude, confidentiality, the control of dissemination of personal information, the control of one's identity
  - Privacy is about the negotiation of personal spaces with those of peers, and with commercial and government entities
  - Privacy is contextual
- Understand privacy perspectives
  - Individual, Commerce, Government, Society
- Create knowledge and tools
  - To identify and mitigate emerging risks to privacy
  - To develop IT systems that can support privacy expectations and prevent unlawful discrimination, while supporting innovation

# Federal Priorities for Privacy Research

- Foster multidisciplinary approach to privacy research and solutions
- Understand and measure privacy desires and impacts
- Develop system design methods that incorporate privacy desires, requirements, and controls
- Increase transparency of data collection, sharing, use, and retention
- Assure that information flows and use are consistent with privacy rules
- Develop approaches for remediation and recovery
- Reduce privacy risks of analytical algorithms

# Taking pulse

# NSF SaTC PI Survey

“select all topics that describe your projects”

| **Cybersecurity Defensive Elements (1370 responses)** | | |
|---|---|---|
| Deter | 219 | 16% |
| Protect | 561 | 41% |
| Detect | 343 | 25% |
| Adapt | 174 | 13% |
| Does Not Apply | 73 | 5% |
| **Cybersecurity Critical Areas (1309 responses)** | | |
| Scientific Foundations | 454 | 35% |
| Human Aspects | 208 | 16% |
| Transition to Practice | 193 | 15% |
| Cybersecurity Workforce | 155 | 12% |
| Risk Management | 131 | 10% |
| Research Infrastructure | 125 | 10% |
| Does Not Apply | 43 | 3% |
| **Privacy Research Priorities (1278 responses)** | | |
| Does Not Apply | 252 | 20% |
| Foster multidisciplinary approach to privacy research and solutions | 212 | 17% |
| Understand and measure privacy desires and impacts | 148 | 12% |
| Develop system design methods that incorporate privacy desires, requirements, and controls | 269 | 21% |
| Assure that information flows/use are consistent with privacy rules | 144 | 11% |
| Increase transparency of data collection, sharing, use, and retention | 103 | 8% |
| Reduce privacy risks of analytical algorithms | 79 | 6% |
| Develop approaches for remediation and recovery | 71 | 6% |

NITRD

# For More Information

Tomas Vagoun, PhD
Cybersecurity and Privacy R&D Technical Coordinator
National Coordination Office for NITRD
vagoun@nitrd.gov

Federal Cybersecurity R&D Strategic Plan (2016), The White House/NSTC,
https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

National Privacy Research Strategy (2016), The White House/NSTC,
https://www.whitehouse.gov/sites/default/files/nprs_nstc_review_final.pdf

Federal Big Data R&D Strategic Plan (2016), The White House/NSTC,
https://www.whitehouse.gov/sites/default/files/microsites/ostp/NSTC/bigdatardstrategicplan-nitrd_final-051916.pdf

National Artificial Intelligence R&D Strategic Plan, The White House/NSTC,
https://www.whitehouse.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf

Implementation Roadmap for the National Critical Infrastructure Security and Resilience R&D Strategic Plan (2016), The White House/NSTC,
https://www.whitehouse.gov/sites/default/files/microsites/ostp/NSTC/cisr_rd_implementation_roadmap_final.pdf

Strategic Plan for the National Initiative for Cybersecurity Education (2016), NIST,
http://csrc.nist.gov/nice/about/strategicplan.html