Networking and Information Technology Research and Development Program

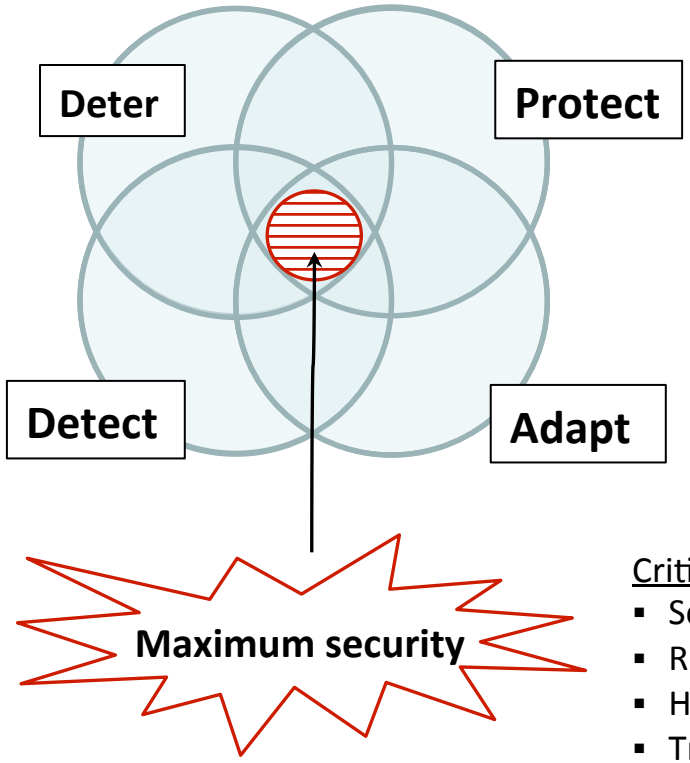
CCC
Leadership in Embedded Security Workshop 2017

Tomas Vagoun

Cybersecurity R&D Coordinator

National Coordination Office for NITRD

Strategic Plan for Federal Cybersecurity R&D

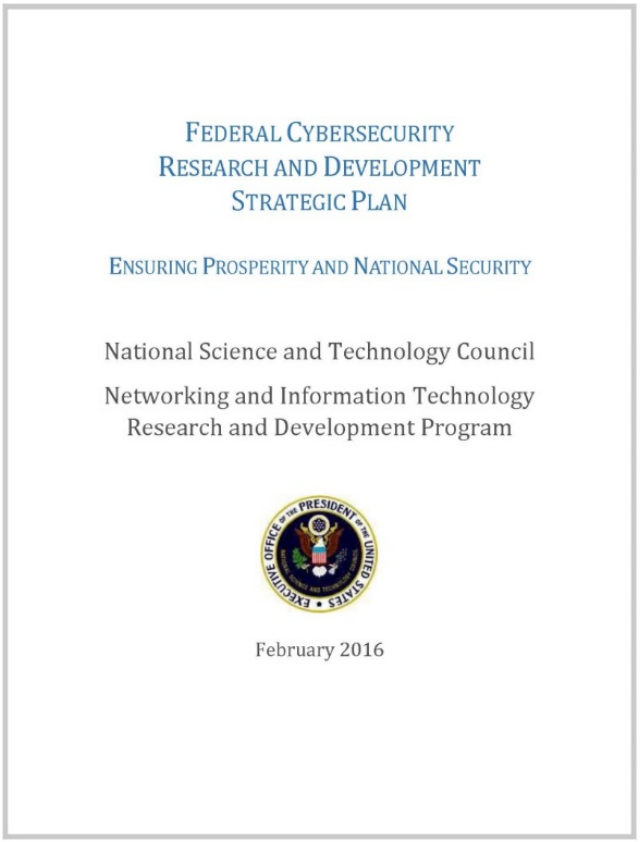


Federal Cybersecurity R&D Goals

- 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

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


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

Trends in Hardware Security Research

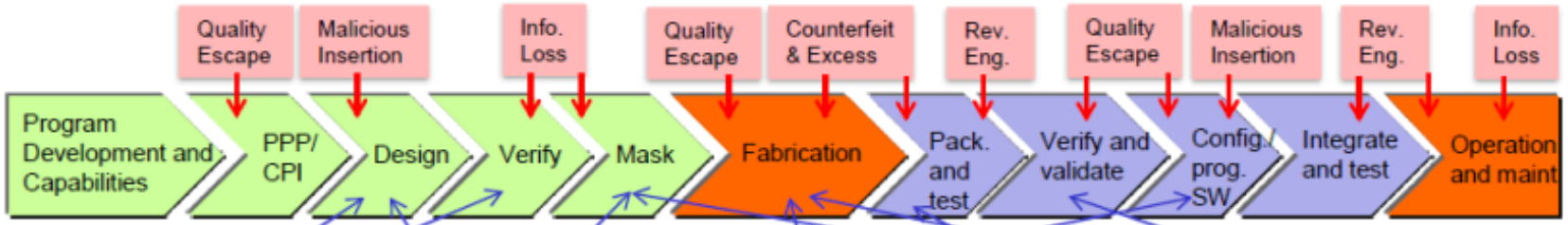
- Supply chain: tamper resistant hardware, Trojan detection, split manufacturing, IC Tracing
- Security of split manufacturing 3D IC
- Side Channels
  - Techniques to suppress side channel
  - Techniques to create/detect covert channels
  - Application of side channel: Trojan Detection
- Security implications of emerging technologies such as NVM
- Secure execution environments, e.g. security enclaves (improvement over Intel SGX or AMD SEV)
- CPS/IoT: Increased interest in secure hardware - new threat models
- Secure Design and Verification: better secure design, test, and verification for hardware
- Post-Quantum Crypto
- Continued interest in
  - Physical Unclonable Functions (PUF) and Random Number Generators (RNG)
  - Detection of IC counterfeiting
  - Logic obfuscation and logic locking
  - Homomorphic encryption

Trusted Microelectronics as a Strategic Issue

- Issue
  - Most COTS electronics used in the US, including those used by the DoD, are manufactured overseas—creating a significant security risk from potential tampering for the Nation
  - With large strategic investments (e.g., $150B by China, $100B by Saudi Arabia) and national subsidies, Asia is becoming the world-class center of microelectronics design and production, severely handicapping the US national security interests
- What actions are needed to reverse this trend?
  - Invest in innovative secure design solutions, which would allow the USG to use offshore state of the art commercial microelectronics capabilities, while satisfying the needs for trust
  - The secure design approach combines SW and HW assurance tools and verification capabilities to provide for trusted manufacturing outcomes
- Example
  - DoD Microelectronics Innovation for National Security & Economic Competitiveness (MINSEC) Program
  - DoD to invest $2 billion in MINSEC between fiscal year 2019 and FY-2023

NITRD

Trusted Microelectronics: New Trust and Assurance Approaches



Design for trust	IP protection	Low-volume/high-mix production	Electronic component markers	Imaging technologies and forensics
• Designing techniques to limit full use/functionality to trusted operation	• Preventing exploitation, including control of use, concealment, reconfiguring, partitioning, or employment	• Innovative methods to permit cost-effective, Trusted and assured low volume manufacturing of state-of-the-art ICs	• Tagging/marking ICs and subassemblies to authenticate and track supply chain movements	• Advanced capabilities to efficiently evaluate dense, state-of-the-art commercial components

Source: DoD/OSD

NITRD