HW Security at NIST

A.J. Stein

Security Components and Mechanism

National Institute of Standards and Technology

Agenda

Overview of Program

CHIPS Act & NIST

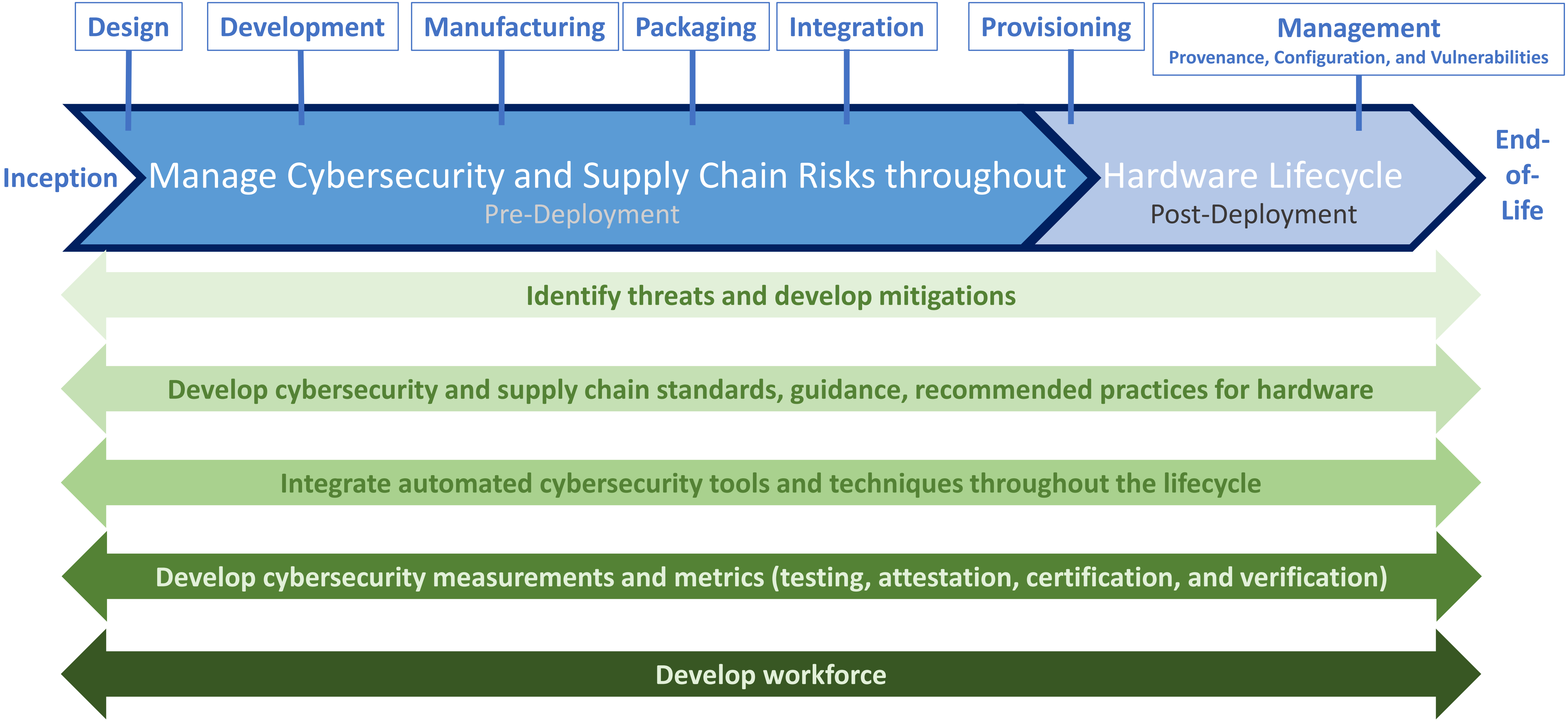
Challenge & Next Steps

Hardware Cybersecurity Program

Develop Standards, Guidelines, Best Practices, Reference Design Kits, Demos and Support Research in the field of **Semiconductor Design** Security and Trust

Why	• Cybersecurity challenges and Hardware vulnerabilities often go undetected • Semiconductor continues to be pervasive including for critical commercial and military applications - Cybersecurity and Assurance in Semiconductor Design Development and Across Supply Chain
What	• Collaborate with Industry to establish best practices for trust, security risks and vulnerability management across semiconductor development chain industry • Develop Secure Data Sharing practices and standards • Best Practices for IP Protection • Vulnerability detection and management best practices during development and post deployment • Establish trust/provenance across supply chain
How	• Tech Transfer of 'what' in industry: Reference Design kits, Standards bodies, Develop foundational builds with external partners to demonstrate use. • Leverage Applied Sec Division/NCCoE capabilities

Cybersecurity across the Life Cycle



Design

Development

Manufacturing

Packaging

Integration

Provisioning

Management

Provenance, Configuration, and Vulnerabilities

Inception

Manage Cybersecurity and Supply Chain Risks throughout Hardware Lifecycle

Pre-Deployment

Post-Deployment

End-of-Life

Identify threats and develop mitigations

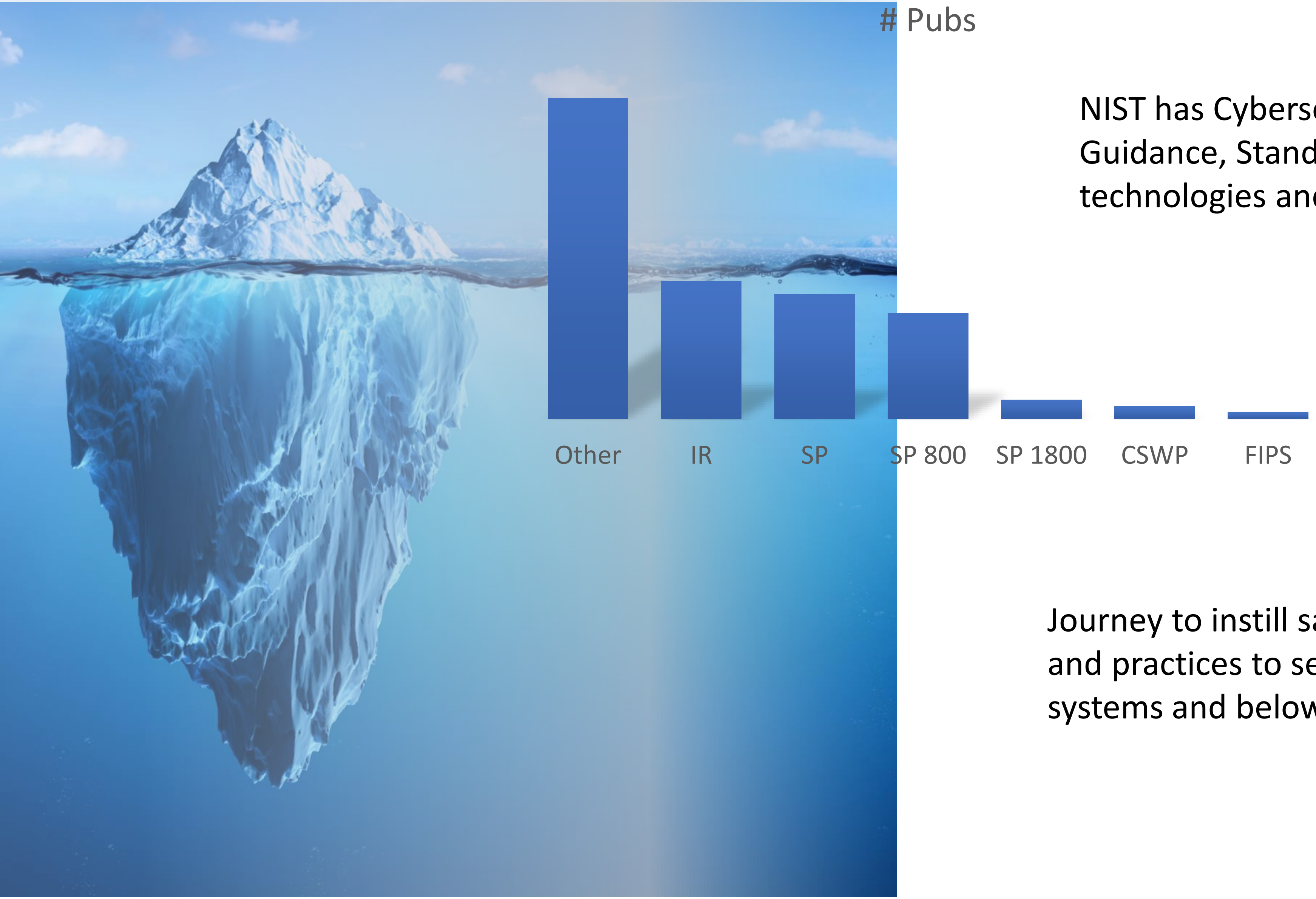
Develop cybersecurity and supply chain standards, guidance, recommended practices for hardware

Integrate automated cybersecurity tools and techniques throughout the lifecycle

Develop cybersecurity measurements and metrics (testing, attestation, certification, and verification)

Develop workforce

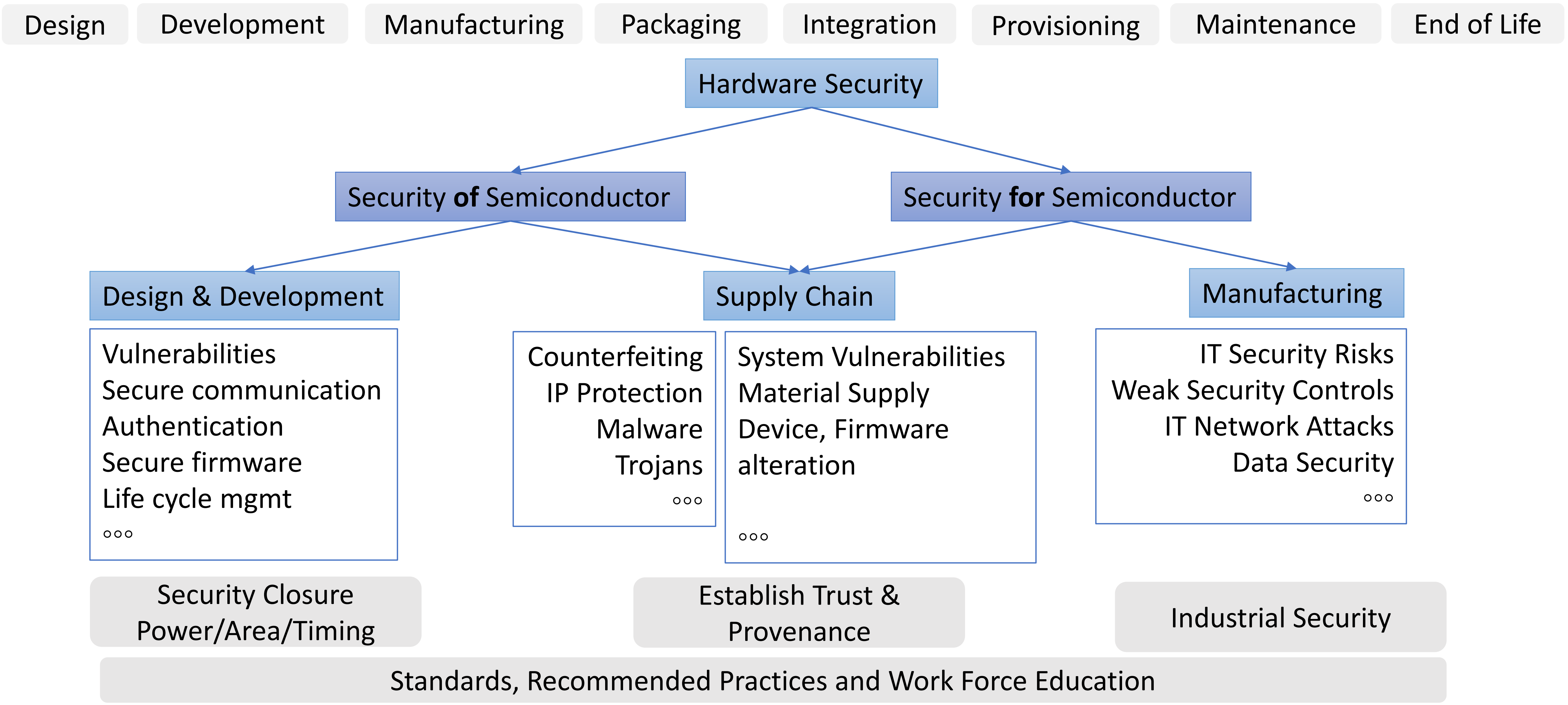
Cybersecurity practice



NIST has Cybersecurity Research, Guidance, Standards across multiple technologies and Sectors

Journey to instill same rigor zeal and practices to semiconductor systems and below

Purpose and Scope



Design | Development | Manufacturing | Packaging | Integration | Provisioning | Maintenance | End of Life

Hardware Security

Security **of** Semiconductor

Security **for** Semiconductor

Design & Development

- Vulnerabilities
- Secure communication
- Authentication
- Secure firmware
- Life cycle mgmt
- ○○○

Supply Chain

- Counterfeiting
- IP Protection
- Malware
- Trojans
- ○○○

- System Vulnerabilities
- Material Supply
- Device, Firmware alteration
- ○○○

Manufacturing

- IT Security Risks
- Weak Security Controls
- IT Network Attacks
- Data Security
- ○○○

Security Closure
Power/Area/Timing

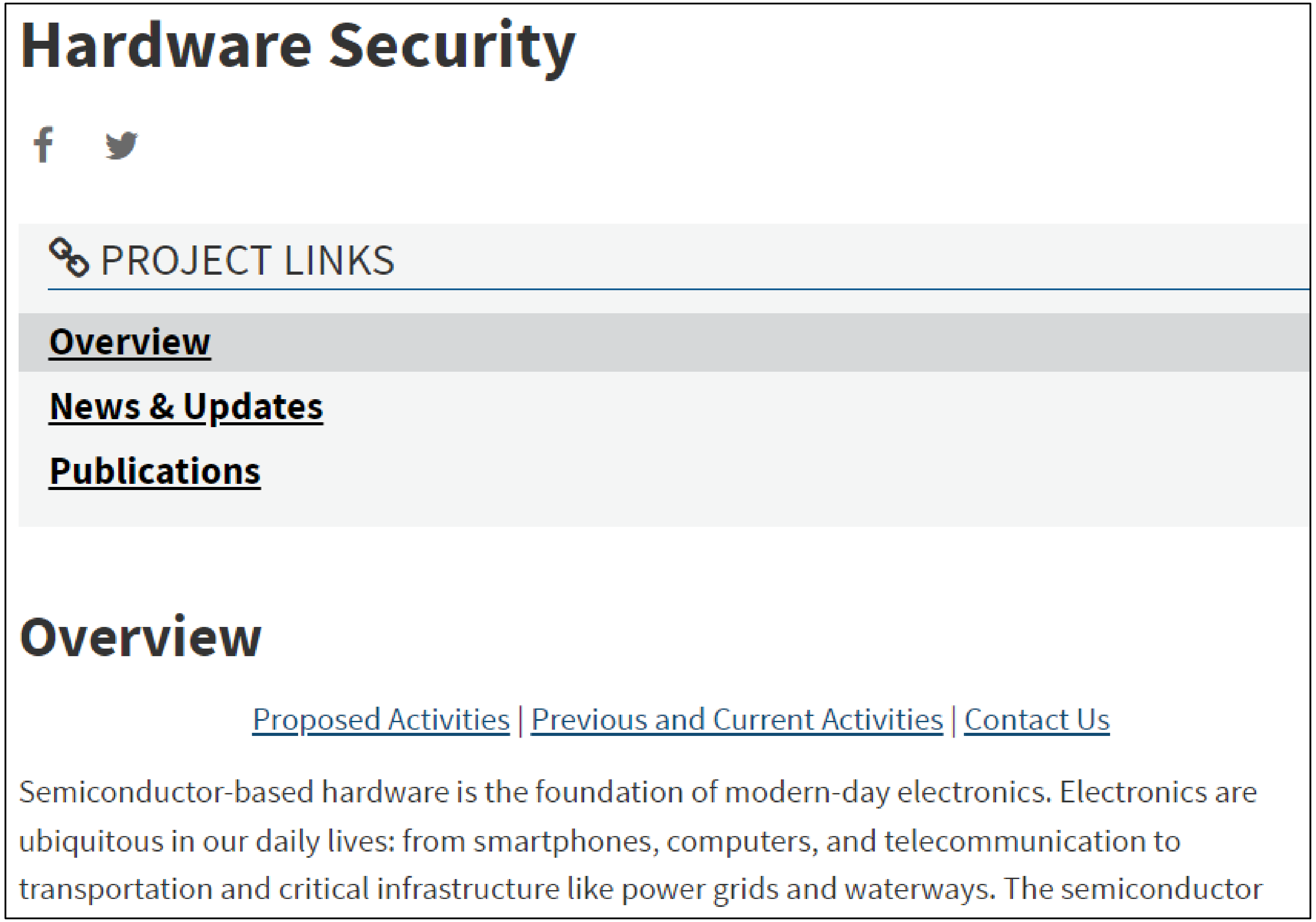
Establish Trust &
Provenance

Industrial Security

Standards, Recommended Practices and Work Force Education

Activities

https://csrc.nist.gov/Projects/hardware-security



Hardware Security

PROJECT LINKS

Overview

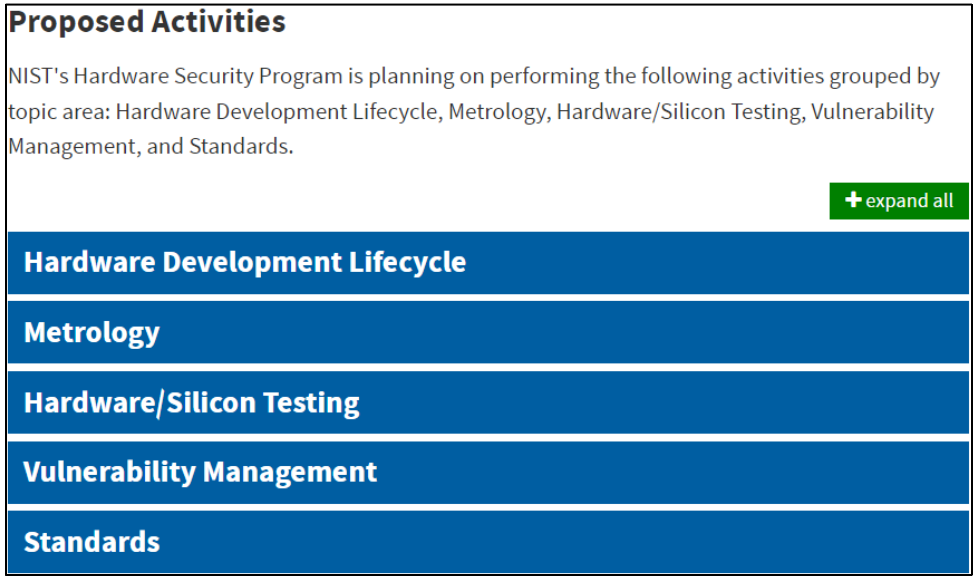
News & Updates

Publications

Overview

Proposed Activities | Previous and Current Activities | Contact Us

Semiconductor-based hardware is the foundation of modern-day electronics. Electronics are ubiquitous in our daily lives: from smartphones, computers, and telecommunication to transportation and critical infrastructure like power grids and waterways. The semiconductor

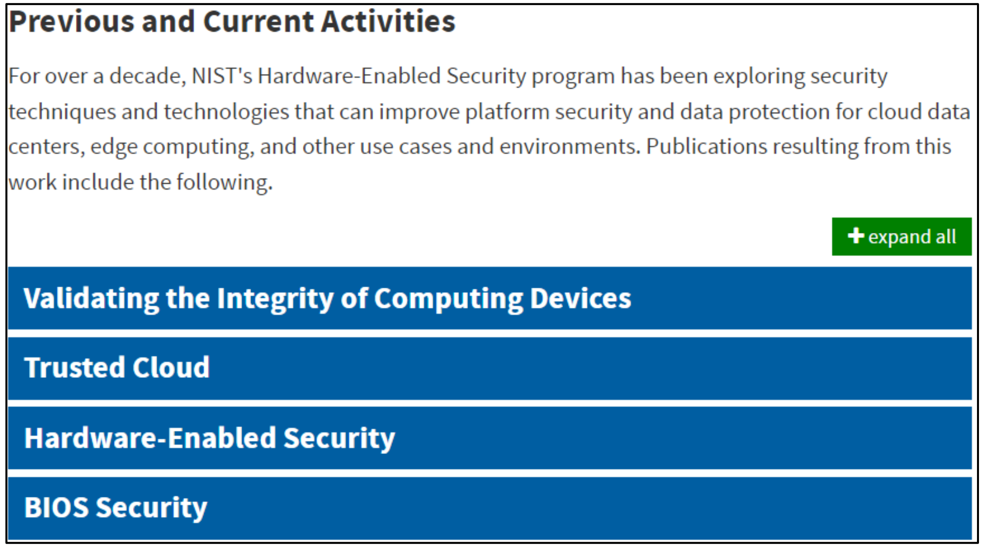


Proposed Activities

NIST's Hardware Security Program is planning on performing the following activities grouped by topic area: Hardware Development Lifecycle, Metrology, Hardware/Silicon Testing, Vulnerability Management, and Standards.

+ expand all

- **Hardware Development Lifecycle**
- **Metrology**
- **Hardware/Silicon Testing**
- **Vulnerability Management**
- **Standards**



Previous and Current Activities

For over a decade, NIST's Hardware-Enabled Security program has been exploring security techniques and technologies that can improve platform security and data protection for cloud data centers, edge computing, and other use cases and environments. Publications resulting from this work include the following.

+ expand all

- **Validating the Integrity of Computing Devices**
- **Trusted Cloud**
- **Hardware-Enabled Security**
- **BIOS Security**

CHIPS Intro

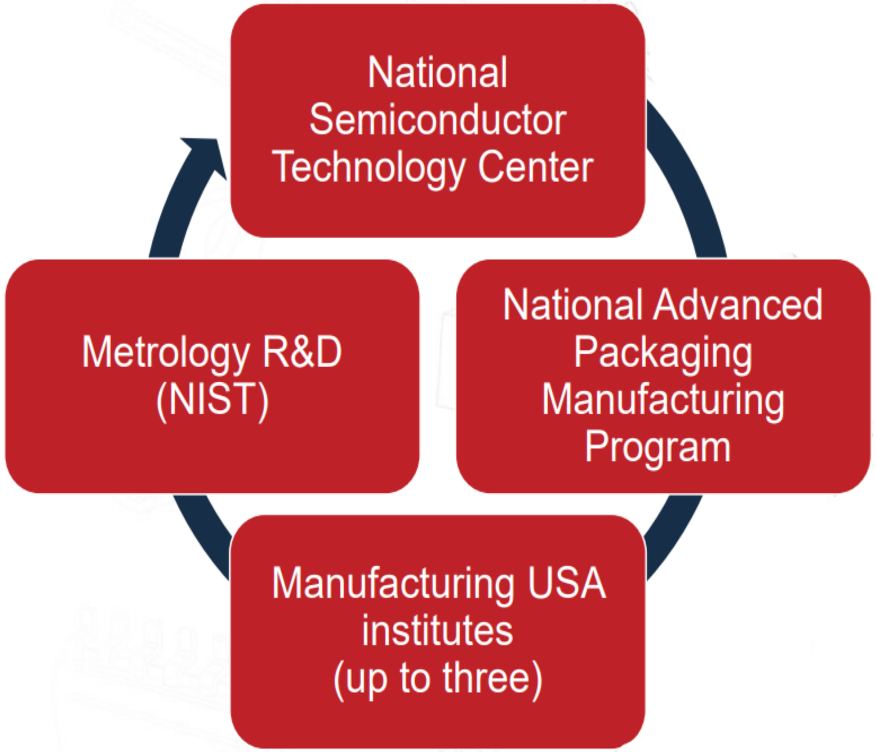
NIST

$39 billion for manufacturing

Two component programs:

1. Attract large-scale investments in advanced technologies such as leading-edge logic and memory
2. Incentivize expansion of manufacturing capacity for mature and other types of semiconductors

$11 billion for R&D



National Semiconductor Technology Center

National Advanced Packaging Manufacturing Program

Manufacturing USA institutes (up to three)

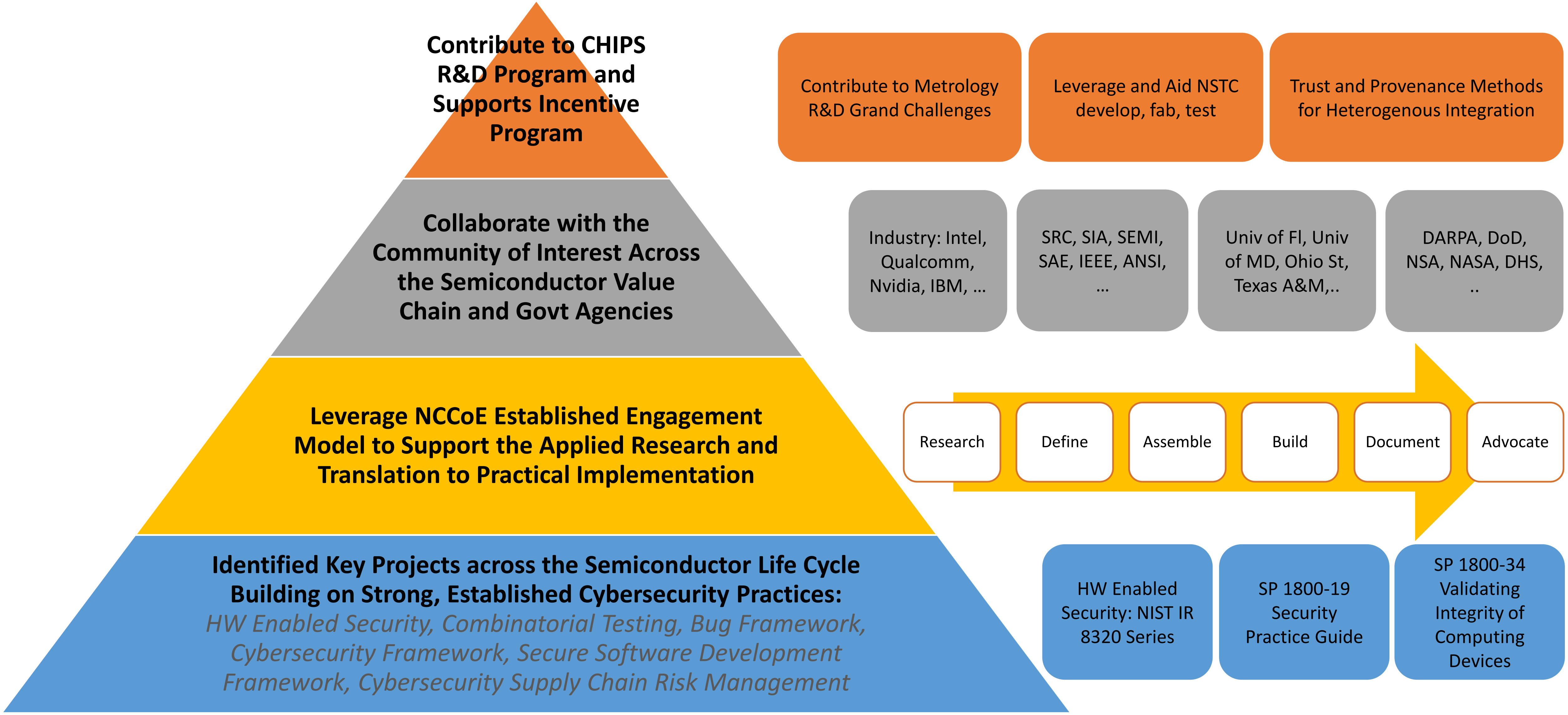
Metrology R&D (NIST)

Plus CHIPS initiatives from other agencies, including DOD, State, NSF, and Treasury

Workforce development

Eric Lin, Deputy Dir, CHIPS R&D, 26 Apr'23

Collaboration with the Community to Develop Guidance and Practical Implementations to Support Industry Needs



Contribute to CHIPS R&D Program and Supports Incentive Program

Contribute to Metrology R&D Grand Challenges

Leverage and Aid NSTC develop, fab, test

Trust and Provenance Methods for Heterogenous Integration

Collaborate with the Community of Interest Across the Semiconductor Value Chain and Govt Agencies

Industry: Intel, Qualcomm, Nvidia, IBM, …

SRC, SIA, SEMI, SAE, IEEE, ANSI, …

Univ of Fl, Univ of MD, Ohio St, Texas A&M,..

DARPA, DoD, NSA, NASA, DHS, ..

Leverage NCCoE Established Engagement Model to Support the Applied Research and Translation to Practical Implementation

Research → Define → Assemble → Build → Document → Advocate

Identified Key Projects across the Semiconductor Life Cycle Building on Strong, Established Cybersecurity Practices:
HW Enabled Security, Combinatorial Testing, Bug Framework, Cybersecurity Framework, Secure Software Development Framework, Cybersecurity Supply Chain Risk Management

HW Enabled Security: NIST IR 8320 Series

SP 1800-19 Security Practice Guide

SP 1800-34 Validating Integrity of Computing Devices

Objective of NIST's Workshop on Cybersecurity

- Convene semiconductor security experts from industry, academia, and government
- Gather input to inform NIST strategic planning
- Leverage cybersecurity expertise
- Collaborate to prioritize:
  - Research activities
  - Approaches to advance standards, guidance and example implementations

Road ahead

NIST workshop report

What we heard

- Strengthen semiconductor manufacturing through development and adoption of NIST Cybersecurity Framework (CSF) 2.0 community profile for semiconductor manufacturing with the community (e.g., SEMI, SIA, Government, Academia, etc.)
- Investigate and leverage existing standards and best practices for developing a Cybersecurity Framework for Semiconductors covering the full lifecycle in collaboration with the community to include a strategy, roadmap and appropriate recommendations focusing on the semiconductor supply chain traceability and provenance
- Research and formulate practical cybersecurity measurements and metrics for semiconductor to inform verification and testing of the countermeasures

Continue our engagement

- Request for stakeholder participation as we kick initiatives

Feedback/Suggestions/Ideas: hwsec@nist.gov

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

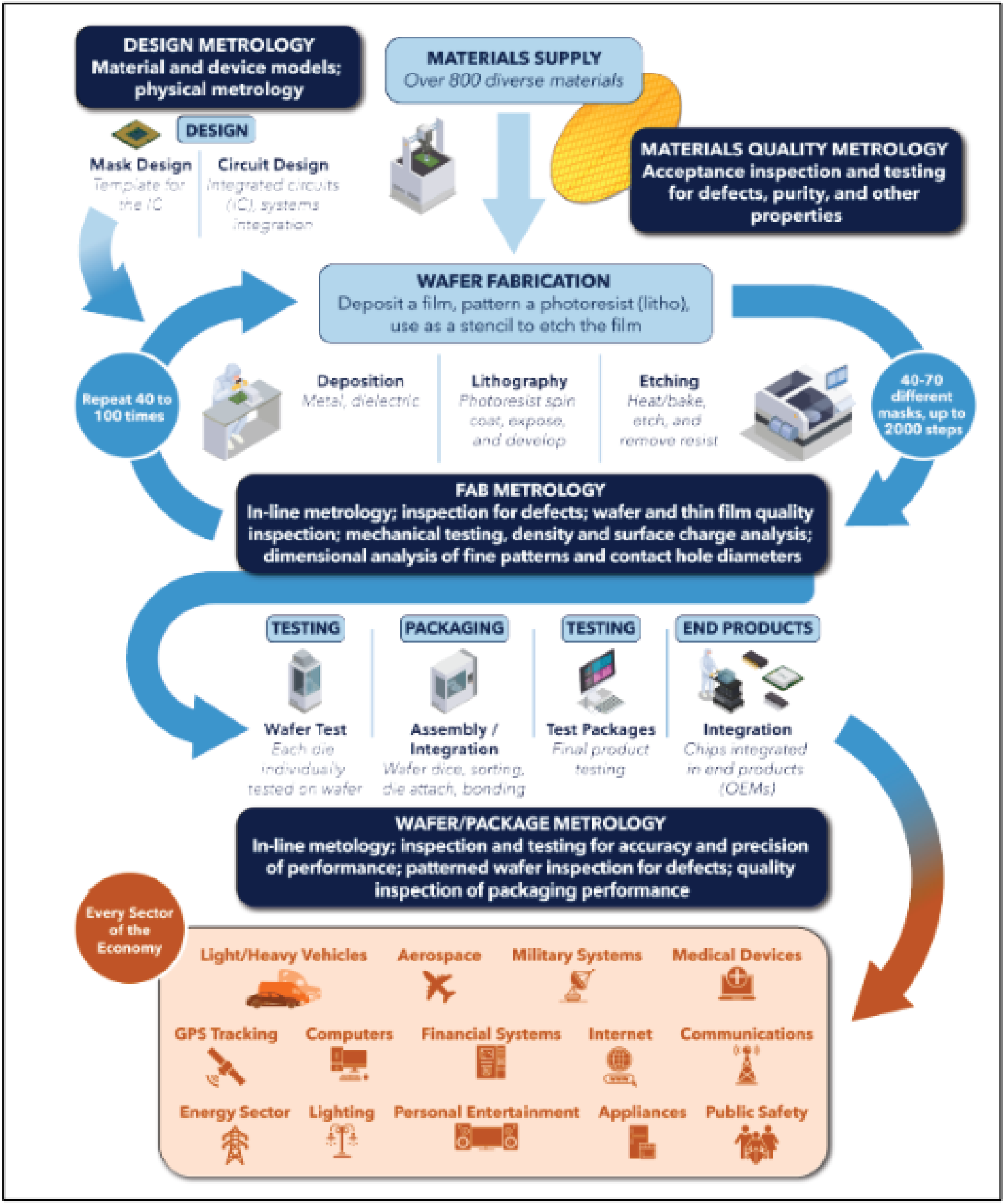
Q&A

nccoe.nist.gov

@NISTcyber

✉ **hwsec@nist.gov**

Appendix: The Grand Challenges



DESIGN METROLOGY
Material and device models; physical metrology

MATERIALS SUPPLY
Over 800 diverse materials

DESIGN

Mask Design
Template for the IC

Circuit Design
Integrated circuits (IC), systems integration

MATERIALS QUALITY METROLOGY
Acceptance inspection and testing for defects, purity, and other properties

WAFER FABRICATION
Deposit a film, pattern a photoresist (litho), use as a stencil to etch the film

Repeat 40 to 100 times

Deposition
Metal, dielectric

Lithography
Photoresist spin coat, expose, and develop

Etching
Heat/bake, etch, and remove resist

40-70 different masks, up to 2000 steps

FAB METROLOGY
In-line metrology; inspection for defects; wafer and thin film quality inspection; mechanical testing, density and surface charge analysis; dimensional analysis of fine patterns and contact hole diameters

TESTING

Wafer Test
Each die individually tested on wafer

PACKAGING

Assembly / Integration
Wafer dice, sorting, die attach, bonding

TESTING

Test Packages
Final product testing

END PRODUCTS

Integration
Chips integrated in end products (OEMs)

WAFER/PACKAGE METROLOGY
In-line metology; inspection and testing for accuracy and precision of performance; patterned wafer inspection for defects; quality inspection of packaging performance

Every Sector of the Economy

Metrology Grand Challenges

1. **GC1** : Metrology for Materials Purity, Properties, and Provenance
2. **GC2** : Advanced Metrology for Future Microelectronics Manufacturing
3. **GC3** : Enabling Metrology for Integrating Components in Advanced Packaging
4. **GC4** : Modeling and Simulating Semiconductor Materials, Designs, and Components
5. **GC5** : Modeling and Simulating Semiconductor Manufacturing Processes
6. **GC6** : Standardizing New Materials, Processes, and Equipment for Microelectronics
7. **GC7** : Metrology to Enhance Security and Provenance of Microelectronic based Components and Products