

Semiconductor Manufacturing Security

Information Security and Privacy Advisory Board
July 17, 2025

Program of National Interest

NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN

MAY 2024

Increased attacks on Semiconductor companies and high value targets

Reference to semiconductor in NDAA has elevated security of semiconductor as National Interest
Working towards Delivery of NCISP Initiative & Projects to Support CHIPS and Metrology Grand Challenge 7

Strategic Opportunities for U.S. Semiconductor Manufacturing

*Facilitating U.S. Leadership
and Competitiveness
through Advancements in
Measurements and Standards*

Initiative Number: 5.5.5

Initiative Title: Develop guidance for secure development and manufacturing of semiconductors

Initiative Description

The National Institute of Standards and Technology, in collaboration with the interagency and the semiconductor industry, will develop guidance for securing semiconductor development and manufacturing. This will include recommendations on securing semiconductors and a Cybersecurity Framework Profile tailored to the semiconductor manufacturing industry.

NCS Reference

... Extending this model to other critical technologies will require long-term, strategic collaboration between public and private sectors at home and abroad to rebalance global supply chains and make them more secure, resilient, and trustworthy.

Responsible Agency: NIST

Contributing Entities: DoD, NSA, ONCD

Completion Date: 3Q FY25



The challenge: Create the metrology advances needed to enhance the security and provenance of microelectronic components and products across supply chains and increase trust and assurance.



The strategy: Pursue a comprehensive approach to hardware security protection that includes standards, protocols, formal testing processes, and advanced computational technologies while providing avenues for assurance and provenance of microelectronic components across the supply chain and end products.

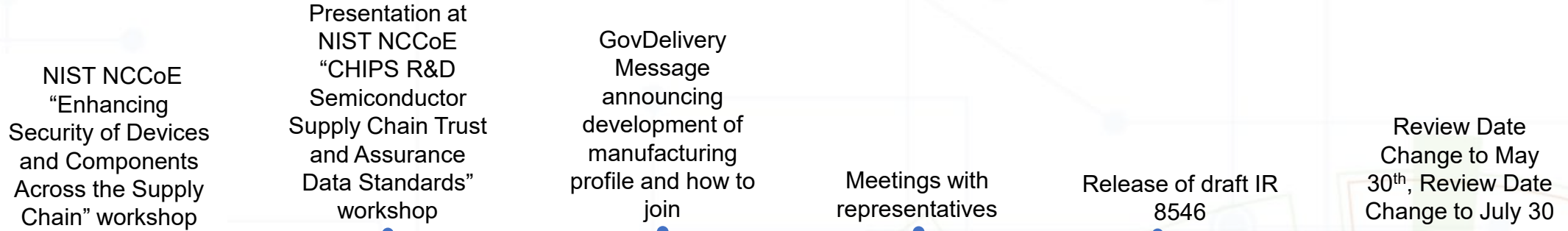
The path forward: Conduct activities to support the development of standards, protocols, and testing processes for analyzing security vulnerabilities in microelectronics across their entire life cycle. Critical areas of pursuit include:

- Methods, reference design kits, and guidelines for security analytics and automation, including pervasive security to address formalized threat models.
- Enhanced vulnerability management across the overall product life cycle from inception to end of life, including activities such as:
 - Formal testing and processes for independent V&V.
 - Tracking of materials and components, as well as detecting and mitigating trigger mechanisms.
 - Common test structures, test methods, and test and measurement strategies for end-to-end provenance.
- Documentary standards for hardware security and provenance.
- Development and use of trusted emerging techniques, e.g., AI and ML methods across the entire semiconductor value chain.

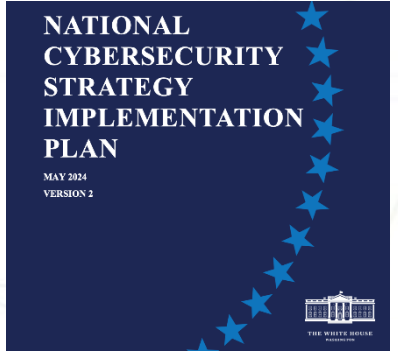
Activities from NIST Feb 2024 Workshop

- **Security for Semiconductor**
 - strengthen semiconductor manufacturing through development and adoption of ***NIST Cybersecurity Framework (CSF) 2.0 community profile for semiconductor manufacturing*** with the community
- **Security of Semiconductor –**
 - investigate and leverage existing standards and best practices for developing a ***Secure Development Framework for Semiconductors*** covering the full semiconductor lifecycle
 - Focus on the semiconductor supply chain traceability and provenance
- Research and formulate practical ***cybersecurity measurements and metrics for semiconductor*** to inform security verification, testing and validation

Journey so far



In-Person Visit to Office of the National Cybersecurity Directorate and agree to launch the effort (NIST, IBM, Intel, Peer group, SEMI)



May 2024: Section 5.5.5...create a “Cybersecurity Framework Profile tailored to the semiconductor manufacturing industry”

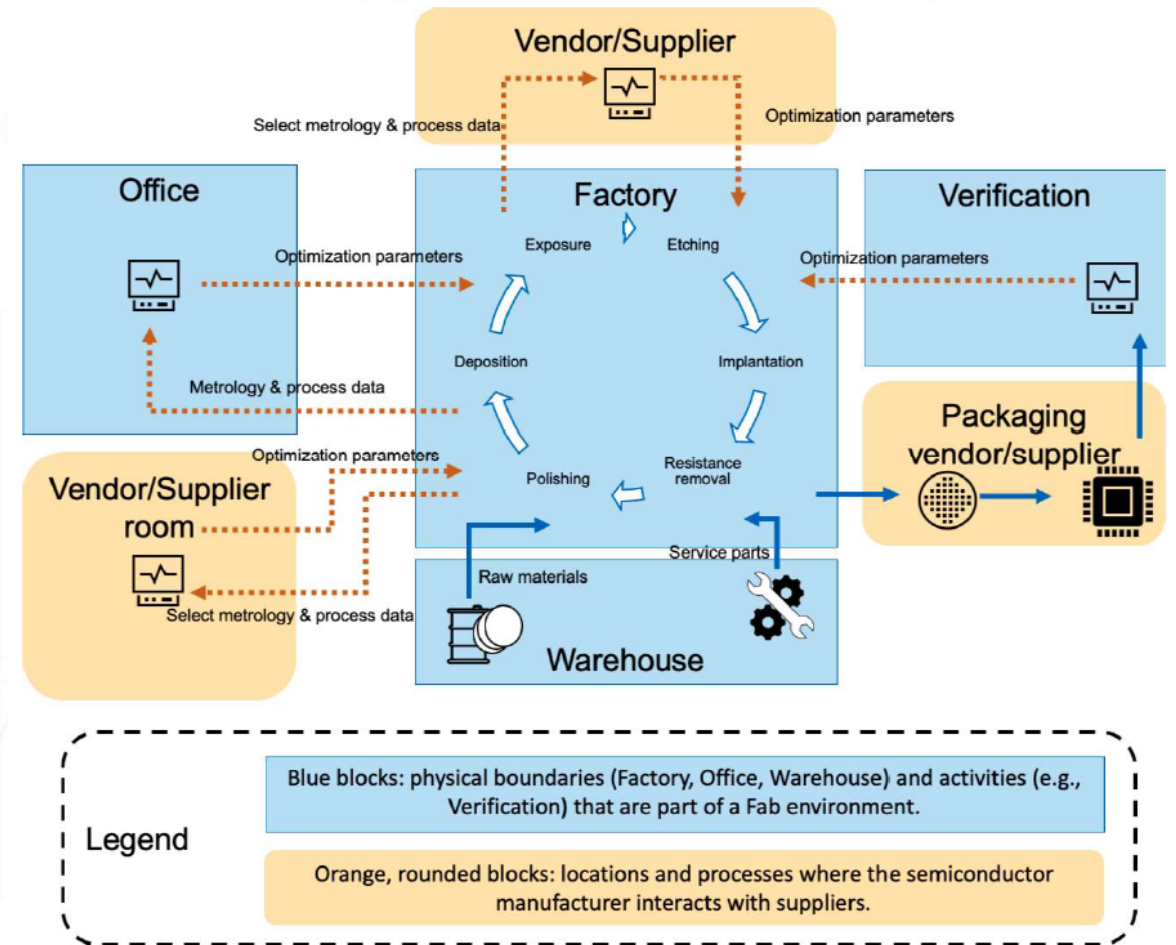


NIST Virtual Workshop and 1st Public Review of IPD



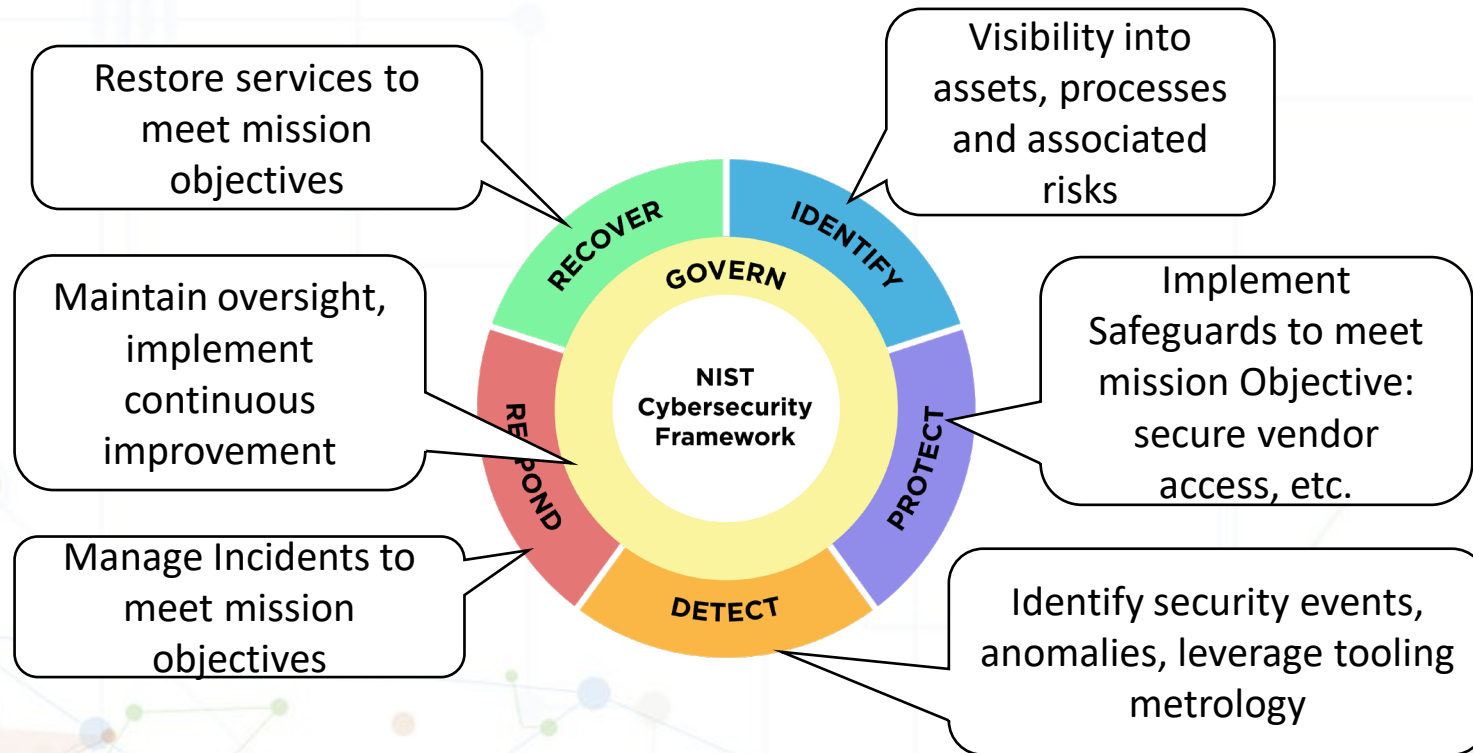
Functional Domains

- Enterprise IT
 - Enables monitoring, control, and threat response
 - Connects and supports both fab and equipment domains
- Fab Environment
 - Operational center of manufacturing
 - Interfaces with tooling and IT for real-time data & control
- Equipment & Tooling
 - Core to chip manufacturing and metrology
 - Supplied by vendors; integrated into fab operations



Improving cybersecurity requires aligned action across fabs, suppliers, and IT systems.

Overview



Next Steps

- Public Period Ends July 30
- Review All Feedback
- Comeback with recommendations by Sept, 2025

Focus Areas:

- Asset and Configuration Management – including legacy/OT systems
- Access control and convergence across IT/OT systems
- Highlight and manage 3rd party risks

Supply Chain Traceability and Provenance

Current Status

- Held the “Trust and Provenance in the Semiconductor Supply Chain” workshop on April 15’25.
 - Identified goals for Industry, Academia and Govt
- Traceability was identified as the main goal and Industry participants expressed urgency
- Subsequent clarification meetings with Industry

Partners :

- Scope: traceability of semiconductor devices and packages.
- Develop Business case with focus on Hyperscalers and Automobiles (AI in cloud and edge)
- Identify Govt Partners to work with
- Identify technical solution(s)
- Identify deliverables, e.g., standards, guidance, framework, etc.

Upcoming Work

- Workshop planned for Oct 21’25
- Expected Outcome
 - Validate the need for Traceability.
 - Decide short term (<1 year) and long-term goals.
 - Roadmap for collaboration/implementation.
- After the workshop, teams will be formed to implement the goals
 - SEMI is working on Phase 0 study
 - Plans to present in October Workshop
- NIST Expects: 2+ Workshops/Seminars per year to monitor/discuss the progress, course correct/syncup

Questions/Suggestions/Feedback

follow-up: *hwsec@nist.gov*