Semiconductor Supply Chain & Traceability Effort at NIST

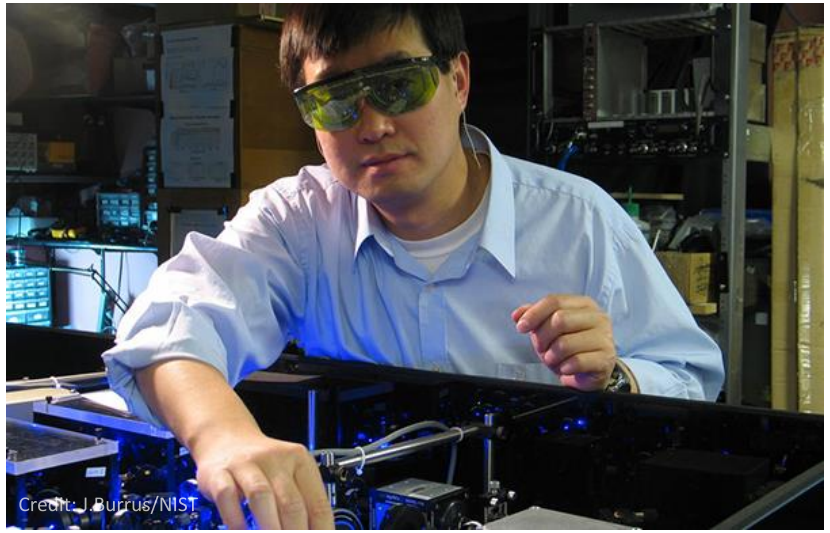
Suzanne Lightman – Transportation Cybersecurity
Kostas Amberiadis – Technical Contact
Sanjay (Jay) Rekhi – HW Security Group Lead

AGENDA

- NIST Mission, Cybersecurity, Industry Cooperation
- Hardware Security Programs at ITL
- Trust and Provenance in the Semiconductor Supply Chain Workshop
- Semiconductor Traceability and Provenance Workshop
- SEMI Phase 0 Chip Traceability: From design to application
- Next Steps

NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing
measurement science, standards, and technology
in ways that enhance economic security and improve our quality of life



Cybersecurity at NIST

NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet US needs. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

https://www.nist.gov/cybersecurity

The National Cybersecurity Center of Excellence

Collaborate with innovators to provide **real-world, standards-based** cybersecurity capabilities that address business needs.

Practical Guidance with Industry Collaboration

SECURITY GUIDANCE | OUR APPROACH | NEWS & INSIGHTS | GET INVOLVED

By Technology

- 5G Cybersecurity
- Applied Cryptography
- Artificial Intelligence
- Critical Cybersecurity Hygiene
- Data Classification
- Data Security
- DevSecOps
- Hybrid Satellite Networks
- Internet of Things (IoT)
- IPv6
- Mobile Device Security
- Supply Chain Assurance
- Trusted Cloud
- Zero Trust Architecture

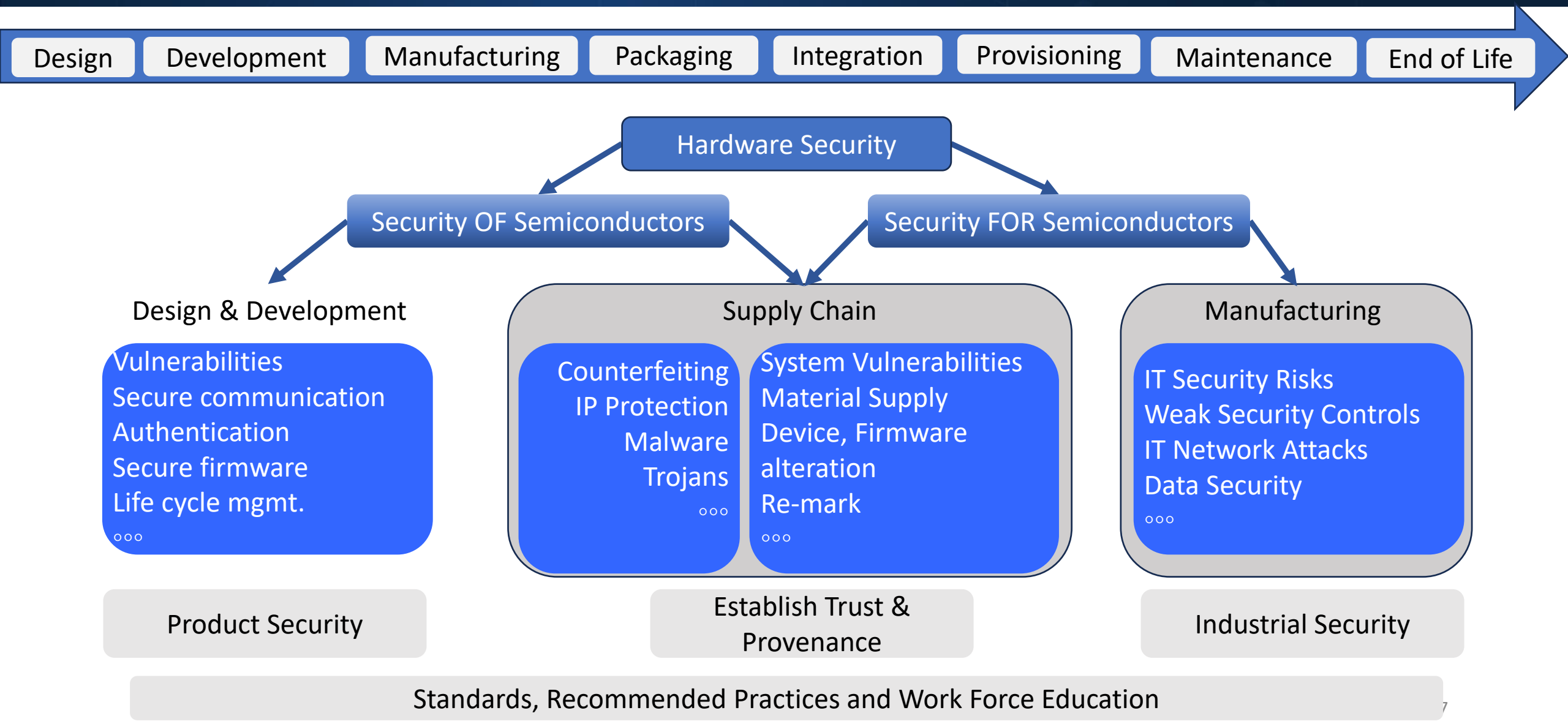
By Sector

- Consumer Data Protection
- Energy
- Financial Services
- Healthcare
- Manufacturing
- Public Safety/First Responder
- Water/Wastewater

By Status

- Defining Scope
- Seeking Collaborators
- Preparing Draft
- Soliciting Comments
- Reviewing Comments
- Finalized Guidance
- Archived

Hardware Security Programs at ITL



Trust and Provenance in the Supply Chain Workshop

- Took place on April 15’25, Trust and Provenance in the Semiconductor Supply Chain Workshop | CSRC
- It was attended primarily by Semiconductor & EDA companies (AMD, Intel, Qualcomm, IBM, Rambus, Lattice, Cadence, etc.), Government and Academia.
- **Semiconductor traceability** emerged as the top short-term (<1 year) and long-term (2028-2029 timeframe) goal for the industry participants.
- In subsequent meetings with the industry participants, it was decided:
  - Have a workshop dedicated to semiconductor traceability.
  - Expand the discussion beyond chipmakers themselves to include the broader ecosystem that consumes and integrates semiconductors, i.e.,
    - Hyperscalers, personal computer, auto companies and government agencies.

Semiconductor Traceability and Provenance Workshop

- Took place on Jan 27’26, Semiconductor Traceability and Provenance Workshop | CSRC
- Presenters:
  - Google, Microsoft, IBM (Hyperscalers)
  - HP Inc. (Personal Computing)
  - Bosch, Stellantis, VW (Auto industry)
  - DHS, DoW (Government)
  - SEMI, USPAE (Industry bodies)
- Panel discussion participants:
  - AMD, Intel, Micron, Qualcomm (Semi companies)
  - Synopsys, Siemens EDA (EDA companies)

Semiconductor Traceability and Provenance Workshop

- Key takeaways:
  - Participants broadly agreed that the problem of semiconductor traceability is too large for any single company to solve alone.
  - At the same time, few expressed interest in abandoning their current internal systems in favor of a universal, top-down solution.
  - Companies see traceability as strategically important, but also as an area where competitive sensitivities remain high.
  - Industry is willing to align on standards, interoperability mechanisms, and shared terminology, but reluctant to expose proprietary data or redesign core processes that provide a competitive advantage.
  - The rise of advanced packaging and heterogeneous integration adds a new layer of urgency to the problem.
    - Modern systems increasingly combine chiplets from multiple vendors into a single package. In heterogenous integration the problem is not just a matter of tracking a single supplier, but of verifying the trustworthiness of an entire network of contributors.
  - Cost was another factor that surfaced repeatedly. Although the traceability infrastructure carries a price, there was no clear consensus on how those costs should be allocated.
    - Over time it will most likely be absorbed by end consumers, regardless of application sector.

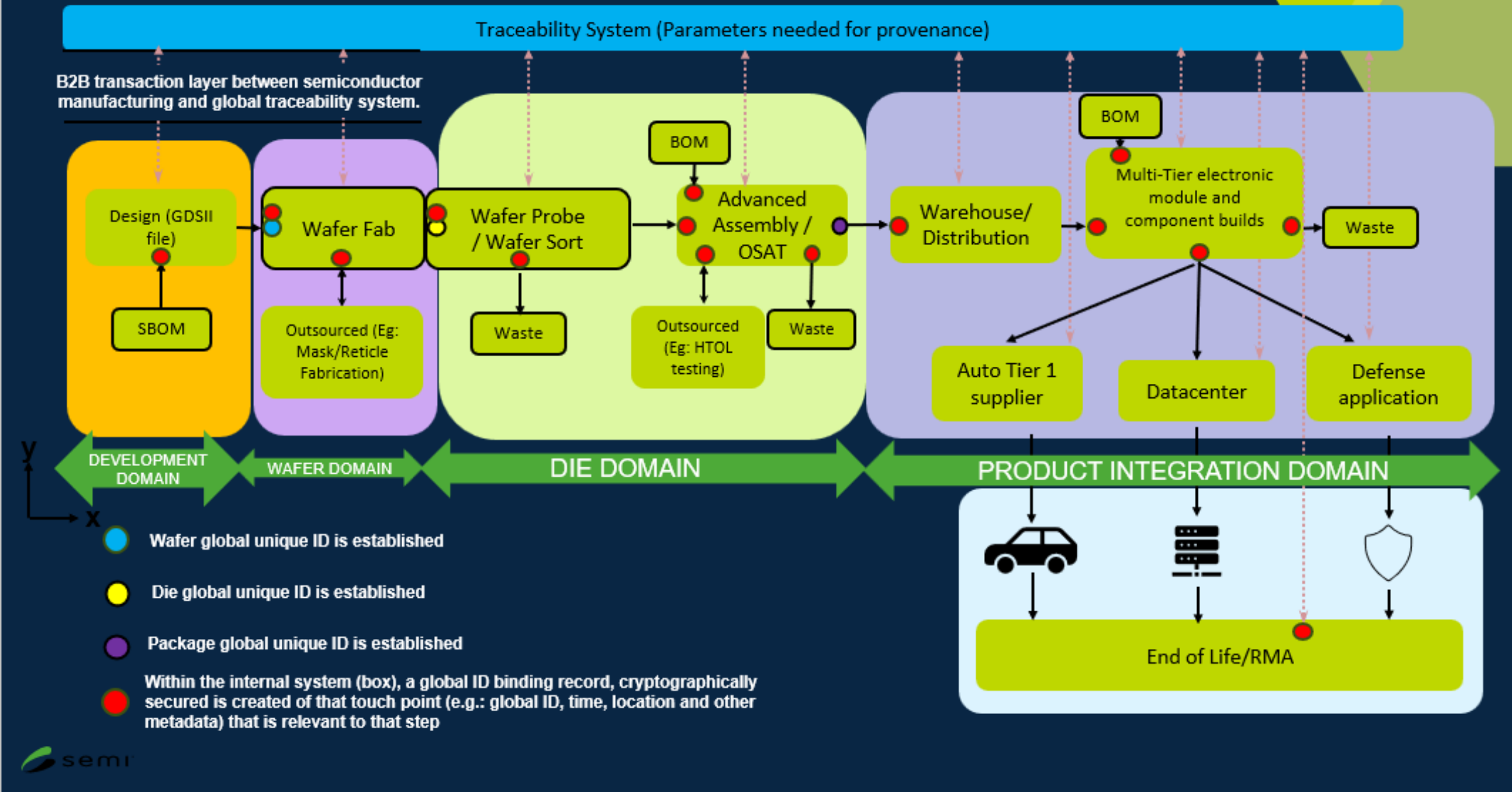
Semiconductor Traceability and Provenance Workshop -- Short-Term (<1 year) Goals

Breakout Session	Goal	Comments
Hyperscalers -- Semi/EDA	Agree on a minimum set of traceability attributes (data model) needed to facilitate automated auditabilty. Look at already existing and upcoming standards. Gather use cases in one place. Solution space also.	6 months
Auto -- Semi/EDA	Define data and establish ontology standards for data required by OEMs and Regulatory Entities.	Possible examples include expanding SBOM and similar details from ISO/SAE 21434, J3101-5, Euro 7.
	Define the use cases that the traceability information is designed to support.	Some may have time/response requirements, some maybe more regulatory requirements; Establish agreement on the need for verifiable data/information to support the use cases; How do we verify data from different sources (e.g., Foreign Sources).
	Define limitations on information that represents business intelligence (intellectual property) data.	Share explicit decisions based on contractual/access controls.
Government -- Semi/EDA	Implement regulations to force microelectronic supply chain to identify themselves via organization identifiers GS1 DUNS GLEIF.	
	IP/EDA compliance for establishing provenance throughout the supply chain.	
	Identify minimal amount of data necessary for customers to determine trust.	

Semiconductor Traceability and Provenance Workshop -- Long-Term (2028-2029) Goals

Breakout Session	Goals	Comments
Hyperscalers -- Semi/EDA	Execute a POC using the data model (see Hyperscalers - Semi/EDA short-term), include as an outcome making the data available to demonstrate different trust model approaches. Estimate added costs when executing the POC.	1 year (6 months after Hyperscalers - Semi/EDA short-term).
	Automate Traceability information.	After item above.
Auto -- Semi/EDA	Architect data repository/repositories (may include auto-related vulnerabilities tracking).	Vulnerability/Threat information building on AUTO-ISAC. Tier 1/2 concerns related to enabling access must be considered/captured in contractual requirements. Constraining access.
Government -- Semi/EDA	Further development/deployment of HBOM initiative.	
	Further development/testing/deployment of DHS S&T Supply Chain Traceability Initiative across the supply chain.	
	Government must prove they are willing to enforce/incentivize industry towards adoption.	

SEMI Phase 0 Chip Traceability: Journey from design to application



Next Steps

- Will start work on a traceability prototype during the next couple of months.
  - Receiving inputs from various stakeholders.
  - Examining whether to cover a particular segment of the traceability system shown in the previous slide, or the whole system.
- Most probably will organize a workshop during the spring of 2027 on traceability prototype development status.
  - Various companies have made proposals to CHIPS for funding for that purpose.

Semiconductor Supply Chain & Traceability Effort at NIST

follow-up: *hwsec@nist.gov*