Status of Standards for Microelectronics Assurance & Traceability

February 2024
Bottom Line Up Front

Current State: Issues/Challenges/Security concerns

• Huge risk of supply disruption
• No market preference for assured supply¹
• Insufficient funding for infrastructure, standards, and process development

¹Assured Supply refers to availability, confidentiality & integrity of the product

Desired State

• Significant increase in production tied to assured supply preference for critical infrastructure
• Critical Infrastructure and consumers both value and benefit from assured efficient supply
• Public/private partnership to build traceability and provenance of assured supply

What’s needed:

• Accelerate targeted funding to build traceability and provenance for assured supply
• Market preference/policy for assured supply
• Fund increased government/industry participation in standards development of assured supply and traceability

Next Steps (TBD):

• Support and fund engagement in standards activity
• Build funding program and RFS for traceability and provenance of assured ME supply in targeted pilots
• Policy focused to build market preference to assured supply for critical infrastructure
Our View of Microelectronic Needs

Commercial Foundation

- **Advanced Technology** is needed across all lithographic nodes for dual use
- **Market incentives and assurance tied to standards** can drive demand to support the business model of at scale fabs, to develop and sustain the IP ecosystems, foundry capacity, and packaging ecosystem

Technology to Capability

- To address security and economic interests, R&D investments must result in **assured production**
- To accomplish this, **R&D must be done in close collaboration with at-scale foundries**
- **ME assurance processes and data with end-to-end traceability** can result in technology investments that increase market leadership and security

Building Assured Supply

- **Leverage assured supply** chain partners and geographic locations to expand production
- **Coordinate investments** to accelerate development & technology transition into assured supply chains
- **Strength in standards and market preferences** can drive demand for assured supply and supply chain sustainability

Strength in standards and market preferences can fortify ME Security & Demand
Elements Needed for Market Adoption

**Policy and Market Behavior**

- **Drive demand** tied to assurance to increase production capacity
- **Establish market incentives, policies and standards** that reduce risk of supply disruption
- **Promote the monetization of security** through traceability that can be valued by end users and consumers

**Trusted Digitization Solutions**

- **Illuminate supply chain** through provenance (e.g., trusted certificates, blockchain, etc.)
- **Model market risks** including non-market forces
- **Create the infrastructure** to monetize assured supply and security
- **Measure the impact of assured supply** to end-markets through market-level traceability and preference

**Physical Traceability & Supply Chain**

- **Implement immutable physical traceability** and validation infrastructure industry-wide
- **Standardize and validate root of trust** and hardware as a service to deliver differentiated technology through assured supply chain
- **Promote consumer level traceability tools** and marketplace
Assurance & Preferred Supply through Provenance & Traceability
Digitalization of Value Chain Enables Data Marketplaces

Trust Analytics & Monitor

Visibility & Traceability

Field Use

Local Storage

Cryptographic Linking

Meta Data

ID-1

ID-2

ID-3

ID-4

Task & Logs

Data

Task & Logs

Data

Task & Logs

Data

Cryptographic Linking

Trust Anchor

Trust Nucleus

Authority Endorser

*Source: GSA TIES reply to NIST RFI on Cybersecurity Framework and Supply Chain Risk Management
Observe, Orient, Decide, Act to Manage Parts & Supply Chains

Observe:
- Global Supply Disruption
- National Security Incident
- Merger & Acquisition
- End of Life notice
- Vulnerability Notice
- Part Update

Orient & Decide:
- Trade/Market Policy Analysis
- National Security Policy Analysis
- System Impact Assessment
- System block modernization
- Supplier Assessments
- Program Impact Assessment
- Part spec. & roadmap
- Part Buys or Migration

Act:
- Commerce Policy Update
- Deploy Industrial Policy (Title III, etc.)
- Commerce/Trade Controls (CFIUS, Wassiner, etc.)
- Long term Agreement
- System block modernization
- Part Buys or Migration

Enterprise Parts Management System

World Model
- National Sec. Policies
- Commercial Policies
- Enterprise Systems Models
- Supply Chain Models
- Actor Models & Stakeholder Map
- Supplier Models
- Parts Models

Raw Data Sources
- Design & IP Ecosystem
- Wafer Fab Ecosystem
- Packaging & Distribution
- Network Manager
- Engine Manager

Policy Engine

Simulation Engine

Block Chain API

Mitigation Engine

Alerts & Pub/Sub

Data Integrity & Confidentiality

Provenance & Traceability

System Integration

USG Critical Infrastructure

Global Supply Chain
## Status of Standards Activity

<table>
<thead>
<tr>
<th>Cyber Physical Systems Security</th>
<th>Packaging &amp; Distribution</th>
<th>JA7496 - Cyber-Physical Systems Security Engineering Plan&lt;sup&gt;2&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Note - Rev. A in progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>References 100's of cross-sector standards not uniformly adopted and used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JA7496 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td>SwA</td>
<td></td>
<td>JA6678 - Cyber Physical Systems Security Software Assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JA6678 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JA6678/1 Config &amp; SW/Integration SwA Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JA6678/1 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1791 Trusted Electronic Designer, Fabricator, and Assembler Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1791 Certification Scheme offered by IPC</td>
</tr>
<tr>
<td>HwA</td>
<td></td>
<td>JA6801 - Cyber Physical Systems Security Hardware Assurance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1782 - Standard for Manufacturing / Supply Chain Traceability of Electronic Products</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note - Supply chain elements in revision (currently in ballot)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1782 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td>Traceability</td>
<td></td>
<td>SEMI E142 Specificaton for Substrate Mapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SEMI 6504 - Specification for External Device Traceability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SEMI 6504 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1783 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1783 - International Standard for Component-Level Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IPC-1783 Compliance Standard or Guide (includes Audit Checklist)</td>
</tr>
<tr>
<td>Counterfeit Avoidance &amp; Det.</td>
<td></td>
<td>Anti-Counterfeit (premotive controls) for Design &amp; Verify</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JESD243 - COUNTERFEIT ELECTRONIC PARTS: NON-PROLIFERATION FOR MANUFACTURERS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Anti-Counterfeit Mechanisms for Packaging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AS6171 - Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts and specific test method slash sheets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AS6496 - Fraudulent/Counterfeit Electronic Parts…</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AS6553 - Counterfeit Electronic Parts; Avoidance, Detection, Authorized/Franchis Mitigation, and Disposition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AS6174 - Counterfeit</td>
</tr>
</tbody>
</table>

### Significant Gaps in Early Design and Manufacturing of ME Hardware and Supply Chain

- Significant gaps exist in early design and manufacturing of ME hardware and supply chain processes.
- GAP PRODUCTION OF ME DISTRIBUTORS
Modern Supply Chain Security

Industry and consumers adopt and USG values traceability and supply chain assurance.
Next Steps/Recommendations

- **Promote standards** - Accelerate and support standards for Microelectronics Assurance, Provenance, and Traceability

- **Inclusion of funding for standards participation and development** - Support development of technology to deliver Assurance, Provenance, and Traceability along with requirements and funding for standards participation of the stakeholders

- **Robust funding for pilot** - Encourage industry and government to robustly implement and require market preference for Assurance, Provenance, and Traceability