NDIA Electronics Division

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • NDIA.org

Assured and Preferred Supply of Microelectronics through Provenance, Traceability, and Market Preferences

White Paper

March 2024

Contributors

Below is a list of the contributors to this paper:

Eustace Asanghanwa,
Microsoft

Brett Attaway,
Siemens

Bert Clements,
Army DEVCOM

Zachary A. Collier,
Radford University

Dave Chesebrough,
Defined Business Solutions

Donald Davidson,
Synopsys

Daniel DiMase,
Aerocyonics, Inc.

Tom Katsioulas,
Archon Design Solutions, Inc.

Tom Dodson,
Intel

Michael Durkan,
Siemens

Larry Gurule,
I-Infusion

Joel Heebink,
Aerocyonics, Inc.

Dave Huntley,
PDF Solutions

Kirsten Koepsel,
Aerocyonics, Inc.

Cesar Martinez,
Intel

Jeremy Muldavin,
GlobalFoundries

Eli Munson,
Maxar Technologies

Harvey Reed,
MITRE

Simha Sethumadhavan,
Columbia University

Kevin Sink,
TTI, Inc.

Christopher Sundberg,
Woodward, Inc.

Ezra Hall,
GlobalFoundries

Members of the Electronics Division reviewed this paper prior to its publication. For more information about the Electronics Division, including a list of upcoming events, please visit **NDIA.org/Divisions/Electronics.**

DISCLAIMER: The ideas and findings in this report should not be construed as official positions of any organizations listed as contributors or the membership of NDIA. It is published in the interest of an information exchange between government and industry, pursuant to the mission of NDIA.

Executive Summary

The Department of Defense, through numerous service programs and other activities, develops and purchases a wide range of microelectronics. These range from unique, state-of-the-art devices to modified commercial microelectronics, commodity commercial microelectronics, and even legacy microelectronics with limited commercial use. To ensure a secure and reliable supply of these devices, the Department of Defense utilizes a network of trusted suppliers and invests in technical activities designed to build in or verify security in these critical devices.

To support Departmental efforts to increase the security of microelectronics, this paper explores the need to develop a preference for assured[1] and traceable microelectronics with initial emphasis on national and economic security, defense, and critical infrastructure. This approach could act as a complement to the use of the network of trusted foundries and other current security measures. Support for assured and traceable microelectronics by manufacturers will ensure that reliable and secure products are available for supply to customers in the United States and allied nations. The white paper also explores guaranteed access to trusted and assured microelectronics by increasing design and manufacturing in the U.S. and allied nations and the establishment of market preferences for assured supply and actions that are critical for achieving the national security and economic growth objectives set forth by Congress, including through recent Chips and Science Act[2] legislation.

Market preferences for supply chain assurance and traceability can be accomplished through incentives, standards, and legislative requirements. An outcome of these actions will be to build a level, competitive, and secure playing field for microelectronics supply chains, along with assuring the delivery of secure components and systems to support the U.S. and allied nations, with initial emphasis on national security, defense, and critical infrastructure. Additionally, creating a trusted digital thread across the supply chain will enable the establishment of marketplaces of data for producers and consumers that can have a significant positive impact on supply chain resilience, logistics, innovation, efficiency, and security and ultimately lead to economic prosperity. We can reference this as a "supply value chain."

The Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act funding[3] was a critical first step in providing incentives to advance secure domestic and allied semiconductor supply. However, the Act only addresses the supply side of the ecosystem. For example, it does not create new demand for microelectronic chips. At the same time, other Congressional requirements have been mandated for microelectronics: Fiscal Year 2020 National Defense Authorization Act Section 224, "Requiring Defense microelectronics products and services meet trusted supply chain and operational security standards,"[4] and Fiscal Year 2023 National Defense Authorization Act Section 5949 "Prohibition on certain semiconductor products and services"[5] (including supply chain traceability and assurance aspects). To successfully achieve the goals mentioned above, it is imperative that the participants in the global microelectronics supply chain establish an infrastructure for measuring assurance, tracking provenance,[6] enabling supply chain traceability, and establishing a strategy for market preference for assured supply, market access, and end market use.

As we have seen in recent years, the problem of managing the demand versus supply imbalance for microelectronic-based products has been exacerbated by supply chain issues caused by natural, pandemic, and geopolitical issues. These issues, combined with the parallel expansion of counterfeiter exploitation, significantly increase the risks of maliciously modified parts or cybersecurity issues entering the supply chain. Microelectronics have become important elements in growing geopolitical conflicts as they enable electronic warfare systems, the proliferation of satellite-based observations, and other related systems key to hot and cold warfare, to name a few. Warfare, in this context, includes not only traditional methods implemented with armaments but also increasingly through geopolitical, economic, cyber, and trade attacks and attacks to supply chains, communications, and critical infrastructure.

The Value

We must create a system that links evidence of assured supply to end service providers and end users and delivers market value and remuneration for the assurance of the supply chain and services infrastructure.

Today, consumers can scan a code and understand where they get their coffee or chocolate bar, which village, and how it is produced (see Figure 1). This allows the consumer to reward the producer for the quality and eliminate layers of costly supply chain middlemen to deliver better value to the consumer. In the same way, we must create a system that rewards the producers of microelectronics for how and where they produce the goods that deliver our home conveniences, move us around in the world, safeguard our money, and connect us to our loved ones and the rest of the world.

[1] Assurance – "Grounds for justified confidence that a claim has been or will be achieved." SAE International, SAE JA7496, Cyber-Physical Systems Security Engineering Plan (CPSSEP), June 2022. Retrieved from SAE International: https://www.sae.org/standards/content/ja7496_202206/.

[2] https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf

[3] Hayashi, Y. (2022, December 5). U.S., EU Agree to Coordinate Semiconductor Subsidy Programs. Retrieved from WSJ: https://www.wsj.com/articles/u-s-eu-agree-to-coordinate-semiconductor-subsidy-programs-11670284917.

[4] National Defense Authorization Act for Fiscal Year 2020, 10 U.S.C. § 2302 (2020). https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.

[5] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, 41 U.S.C. § 4713 (20220. https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

[6] The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data at each step. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.

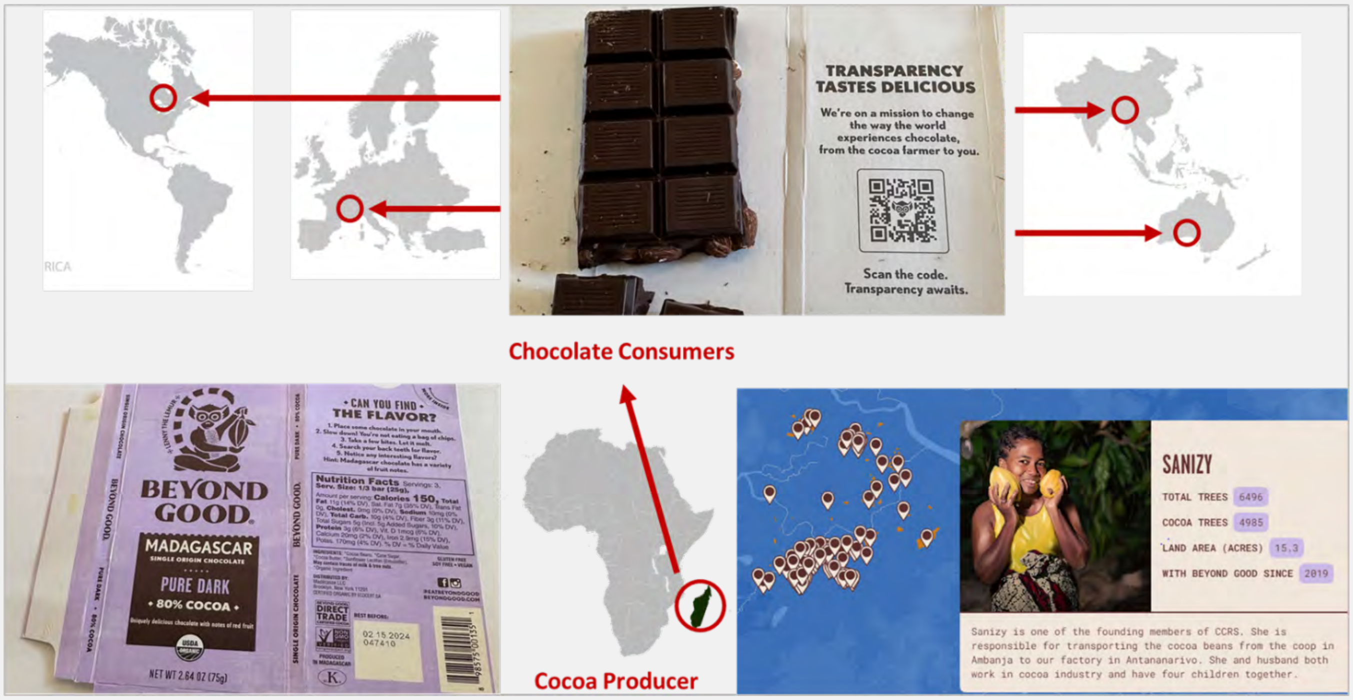
TRANSPARENCY TASTES DELICIOUS
We're on a mission to change the way the world experiences chocolate, from the cocoa farmer to you.
Scan the code. Transparency awaits.
Chocolate Consumers
BEYOND GOOD
MADAGASCAR
SINGLE ORIGIN CHOCOLATE
PURE DARK
• 80% COCOA •
NET WT 2.64 OZ (75g)
• CAN YOU FIND • THE FLAVOR?
Nutrition Facts
DIRECT TRADE
02.15.2024
047410
Cocoa Producer
SANIZY
TOTAL TREES 6496
COCOA TREES 4985
LAND AREA (ACRES) 15.3
WITH BEYOND GOOD SINCE 2019
Sanizy is one of the founding members of CCRS. She is responsible for transporting the cocoa beans from the coop in Ambanja to our factory in Antananarivo. She and husband both work in cocoa industry and have four children together.

Figure 1: Traceability and Associated Value, Chocolate Example[7]

This evidence will be delivered through provenance and traceability using a digital thread to provide the framework for trust-as-assurance case data to become verifiable and linked to specific products (see Figure 2). An end-to-end digital thread is thereby created through the digitalization of workflows of enterprises participating in the value chain. Information about data can be provided in its entirety or via metadata indices delivered through a data marketplace. Cryptography implemented in digital certificates, communicated through a digital thread through the supply chain, can provide intellectual property protection as needed.

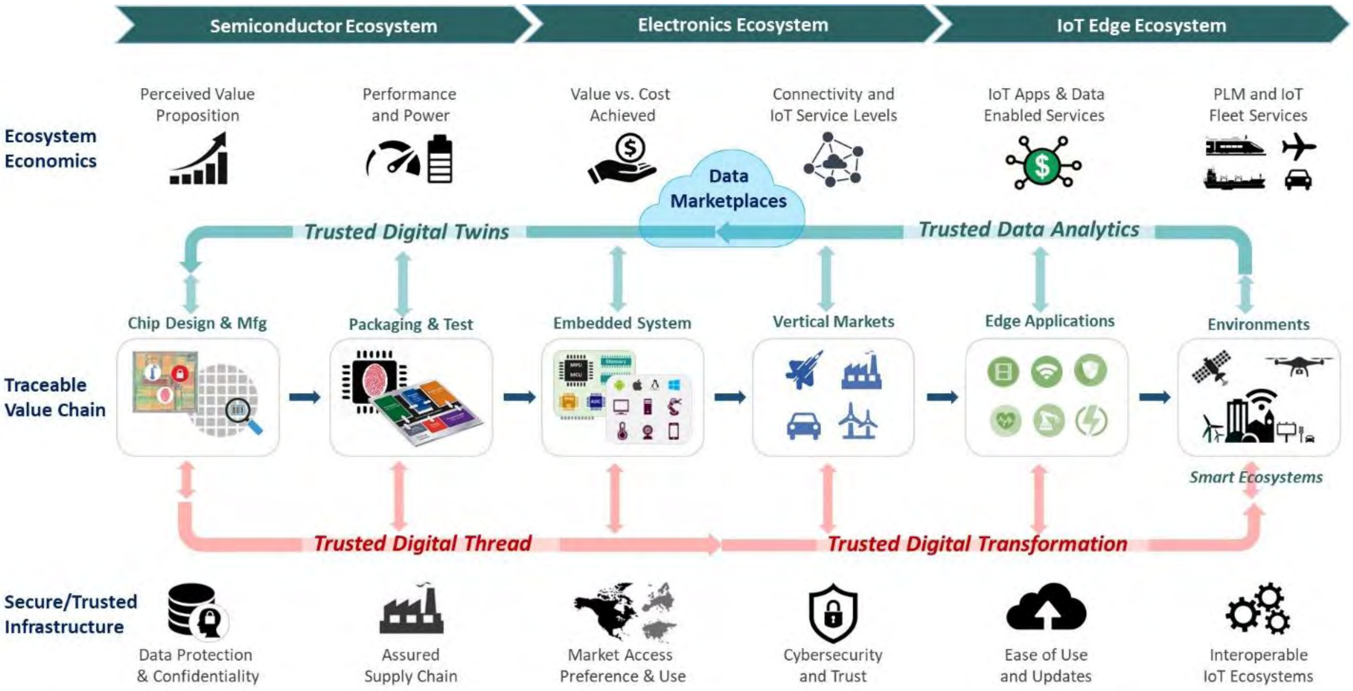

Figure 2: Assurance & Preferred Supply through Provenance & Traceability

[7] Beyond Good. (2023, June). Derived from Beyond Good: https://farmers.beyondgood.com/.

A secure and trusted infrastructure provides the foundation to create digital threads across the value chain. A digital thread linking data producers and consumers enables them to establish market preference. Through market access and by using a digitally transformed environment, enterprises can become smart-connected suppliers in the value chain. Connected enterprises enable networks of data producers and consumers. As the data available in this value chain expands, analytics and AI-based applications can be leveraged to enable digital twin models[8] and other derivative works. Increasingly improving virtual models, or digital twins, fed with real marketplace data through analytics, can be used to make better, more reliable, higher quality products from the start and to better inform decisions.

All of this enables additional opportunities for producers to improve customer value and monetize that value. These opportunities include IoT and data-enabled services, such as fleet management and control, product lifecycle management through subscription, business models, hardware as a service, and a variety of data-enabled applications.

From a national perspective, supply chain availability can be monitored much faster and more accurately, allowing the ability for more precise risk identification and mitigation. This includes risks such as geopolitically and naturally caused supply chain gaps. Also enabled through this means will be the ability to track the illegal distribution of critical and proprietary technologies to prohibited entities or competitors and the ability to disable them if such distribution occurs.

The Approach

The approach includes three elements: digital solutions, physical traceability, and market behavior. These approaches are all aimed at providing a secure and available supply of microelectronics from a robust and diverse supply chain. This requires the following:

Provenance and Supply chain traceability: Utilization of physical identifiers linked to a digital thread that connects devices as they travel through the supply chain. This will include linkages (a relationship) to provenance (includes assurance claims linked to data) while protecting proprietary information. Without supply chain traceability, there is no ability to provide accountability for risk mitigation and assurance or to maximize economic value.

- **Provenance** - The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data at each step. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data.
- **Traceability** - A domain of consideration encompassing the process for determining the provenance of an item (also referred to as tracking).
- **Pedigree** - The validation of the composition of technologies, products, and services at each step.
- **Non-repudiation** - The assurance that someone cannot deny the validity of something or refute responsibility.

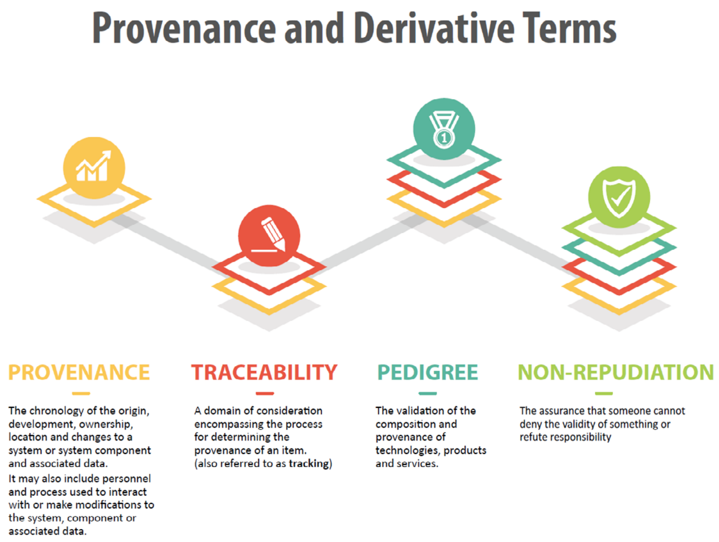
Provenance and Derivative Terms
PROVENANCE
The chronology of the origin, development, ownership, location and changes to a system or system component and associated data.
It may also include personnel and process used to interact with or make modifications to the system, component or associated data.
TRACEABILITY
A domain of consideration encompassing the process for determining the provenance of an item. (also referred to as tracking)
PEDIGREE
The validation of the composition and provenance of technologies, products and services.
NON-REPUDIATION
The assurance that someone cannot deny the validity of something or refute responsibility

Figure 3: Provenance and Derivative Terms[9]

Market Preference: Consumer behavior today places an overwhelming value on performance and price with related demand that drives 98% of global semiconductor production (supply). As the scale of commercial demand drives supply investments, altering the commercial buying behavior model to include valuing assured supply will then provide economic incentives, or demand, for industry adoption, truly establishing a dual-use demand business case for secure supply compliant with the standard(s)[10,11]. Regulations and requirements applied to both defense and non-defense market segments can also help value the standard(s) and further tip the scales. Market preferences will reduce challenges and favorably influence opportunities to achieve national economic and security objectives.

[8] Digital twin – "A set of virtual information constructs that mimics the structure, context and behavior of an individual / unique physical asset, or a group of physical assets, is dynamically updated with data from its physical twin throughout its life cycle and informs decisions that realize value." AIAA Digital Engineering Integration Committee and AIA Technical Operations Council, Digital Twin: Definition & Value, December 2020. Retrieved from AIAA: https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/policy-papers/digital-twin-institute-position-paper-(december-2020).pdf.

[9] SAE International, SAE JA7496, Cyber-Physical Systems Security Engineering Plan (CPSSEP), June 2022. Retrieved from SAE International: https://www.sae.org/standards/content/ja7496_202206/

[10] Adam Hastings & Simha Sethumadhavan, ***A New Doctrine for Hardware Security***, 2020. Retrieved from ArXiv.org: https://arxiv.org/pdf/2007.09537.pdf.

[11] Simha Sethumadhavan & Tim Sherwood, ***Mechanism Design for Improving***, 2022. Retrieved from Computing Community Consortium: https://cra.org/ccc/wp-content/uploads/sites/2/2023/04/01378-Mechanism-Design-Workshop-Report.pdf.

Market Access and Usage: Developing microelectronics architectures to securely link embedded identities in the hardware will enable physical asset traceability through trusted digital threads. Stakeholders in the microelectronics value chain can use this new tool to regulate market access and usage and to enable new "anything as a service" business models, such as pay-as-you-go and chip-use leases.

Supply chain traceability of microelectronics components and the supporting infrastructure of requirements and standards can create the level of supply chain transparency needed to accelerate the creation of smart value chains and digital marketplaces for microelectronics and market preference. All this can be jump-started by policy to demand adoption and corresponding incentives for reward that adoption. Key benefits include enabling new market opportunities and efficiencies. Other benefits include managing system-level risks by mitigating them through the assurance of authenticity and, most importantly, the enablement of U.S. and allied nations' leadership in microelectronics to ensure supply continues uninterrupted.

Recommended Next Steps

Figure 4 shows a high-level overview of the recommendations, beginning with three main works (in block 1) recommended to further detail the primary elements introduced in this white paper. Blocks 2-4 contain elements that should be inserted, as appropriate, into those three work areas to produce the desired result.

1. Further Standards Development	**Established industry consensus standards in three work areas:** • Physical traceability • Assurance standards with market preferences • Data marketplaces, including traceability & IP compliance Use cases & exemplar illustration for these areas
2. USG Efforts:	• Acquisition regulations requiring electronics supply in accordance with industry consensus standards • USG funding to facilitate above
3. Drive Market Adoption	• Policy driving market behavior for defense and critical infrastructure (preference for domestic & allied manufacturing
4. Supporting Recommendations	• Education and workforce development • Scientific work that combines incentives and technology • Make security accountable and explainable • Co-develop emerging technologies • Prioritize human impacts of hardware security

Figure 4: Overview of Recommendations

The three new work areas recommended to further develop matters discussed in this paper are briefly introduced below. Additionally, use cases and an exemplar illustration for context are desired.

1. **Physical traceability** of parts across the supply chain tied to digital traceability that enables validation and remediation of quality, reliability, safety, and security concerns across the entire supply chain (to include provenance and assurance).
2. Establish **assurance standards and market preferences** requiring those standards that drive the United States Government/ Department of Defense (USG/DoD), critical infrastructure, and consumer demand to U.S. supply to drive capabilities, capacity, and sustainable profitability domestically. Internationally developed standards with Allied nations can facilitate the benefit of establishing complementary supply from allied nations. These standards should take into consideration existing standards (such as IPC traceability standards) and programs (such as the DMEA Trusted IC Program and RAMP-C) and address gaps where appropriate.
3. Digital/virtual modeling and traceability of the microelectronics supply chain and establishment of **data marketplaces and apps** that drive value to consumers, industry, the USG, and their allies.
4. Use Cases – suggestions: 1) Intellectual Property (IP) compliance and traceability, and 2) physical traceability and provenance.
5. Exemplar or story illustrating at least one use case.

This Page Intentionally Blank

NDIA

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION
AFFILIATED ORGANIZATIONS

ETI EMERGING TECHNOLOGIES INSTITUTE NTSA WID WOMEN IN DEFENSE

The National Defense Industrial Association is the trusted leader in defense and national security associations. As a 501(c)(3) corporate and individual membership association, NDIA engages thoughtful and innovative leaders to exchange ideas, information, and capabilities that lead to the development of the best policies, practices, products, and technologies to ensure the safety and security of our nation. NDIA's membership embodies the full spectrum of corporate, government, academic, and individual stakeholders who form a vigorous, responsive, and collaborative community in support of defense and national security. For more than 100 years, NDIA and its predecessor organizations have been at the heart of the mission by dedicating their time, expertise, and energy to ensuring our warfighters have the best training, equipment, and support. For more information, visit **NDIA.org**