

Global Semiconductor Alliance

Trusted IoT Ecosystem Security (TIES)

Reply to NIST RFI on Evaluating and Improving Cybersecurity Resources, the Cybersecurity Framework and

Combining CSF with Cybersecurity Supply Chain Risk Management prioritization of supply chain-related cybersecurity needs across sectors with a strategy to create a Digital Supply Chain Business Ecosystem

Version 1.0
April, 2022

Overview

We live in a world that is connected through IoT through complex technology and supply chains that are distributed globally. Modern life and our economic and security foundations are becoming dependent on these IoT devices, their supply chains, and critical infrastructure, all being in great risk due to lack of awareness, nation-state, and environmental disruptions, and lack of a coordinated plan to protect.

The Global Semiconductor Alliance Trusted IoT Ecosystem Security (GSA TIES) is providing this reply to the NIST "Request for Information about Evaluating and Improving Cybersecurity Resources including, the CSF, Cybersecurity Supply Chain Risk Management and prioritization of supply chain-related cybersecurity needs across sectors". The challenges are far greater than can be met with the existing CSF framework that place the burden of supply chain management on individual customers of microelectronics producers. In order to deliver assured microelectronics supply chains, we must understand and incentivize the microelectronics producers and suppliers, and their customers through market access and regulations.

The main challenge with microelectronics supply chain security and risk management is how to create business incentives for all vertical markets and the infrastructure that motivates both suppliers and buyers to adopt. Neither the individual customers in the microelectronic supply chain nor the collective ability of Big Tech and DoD commands adequate market share or enough economic power to sway the global supply chains to adopt an improved CSF just for risk management purposes. Well-regulated markets, driven by standards, are also needed to solve this problem. As part of a combined CSF, Governments must promote market incentives and standards for critical infrastructure for better visibility, traceability, and monetization from the supply chain through an ecosystem platform that is applicable to multiple industries and markets.

An orchestrated strategy is necessary in order to accelerate adoption of security solutions in the supply chain. This includes a strong business ecosystem platform, NIST's global core competencies on CSF guidelines, the Cybersecurity Supply Chain Risk Management framework, as well as pervasive supply chain security standards and interoperability guidelines with other standards bodies. In response to the Federal Register Cybersecurity Framework and Cybersecurity Supply Chain Risk Management articles 11, 12, 13, and 14, the GSA TIES proposes to include key considerations for the realization of next generation CSF, combined with an ecosystem strategy to improve supply chain traceability, and facilitate market access.

Key Considerations

The supply chain needs deployment of principles such as those outlined in CSF, but also in both NIST SP-800-161 and NIST SP 800-171:

- **"161" latest content addresses**: "Organizations are concerned about the risks associated with products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain. These risks are associated with an enterprise's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the security, resilience, reliability, safety, integrity, and quality of the products and services.

  "This publication provides guidance to organizations on identifying, assessing, and mitigating cyber supply chain risks at all levels of their organizations. The publication integrates cyber supply chain risk management (C-SCRM) into risk management activities by applying a multi-level, C-SCRM-

specific approach, including guidance on development of C-SCRM strategy implementation plans, C-SCRM policies, C-SCRM plans, and C-SCRM risk assessments for products and services."

- **"171" and associated DFARS clauses call for adequate protection of USG "controlled unclassified information (CUI),** and provides for proper security "hygiene" is practiced in key elements of the supply chain, specifically in the areas that control, handle, and manipulate design IP into the physical chips that are marketed to industry. While these principles are published, a means for confidence that these principles have been employed (potentially CMMC) in any particular organization is currently lacking.

There is a need for these capabilities:

- **Unique and immutable identification** methods on various levels on the physical chip marketed are needed in order to properly identify an authentic part from the source having this "hygiene."

- **Digital certificates (or other securely communicable data) linked to this physical ID** (these physical IDs) that provides key information important to the supply chain for validation of the physical item.

- **Traceability of the physical item Identity** through a ledger or data structure will provide information on the use and location of the item for Response and Recovery.

These capabilities are needed to help NIST to identify and prioritize supply chain-related cybersecurity needs across sectors, inform a public-private partnership and information on the technology and supply chain challenges organizations are facing and provide guidance on methods, practices and tools required.

In 2021, EO 14017, on America's Supply Chains, called for both 100-day & 1-year reviews in a variety of areas. All those reviews are complete and have published reports with recommendations. Departments of Commerce and Homeland Security Report makes ICT manufacturing and supply chain(s) recommendations:

"To develop a resilient ICT industrial base, DOC and DHS issue several recommendations, including:

- build resilience through secure and transparent supply chains;
- collaborate with international partners to improve U.S. and ally/partner supply chain resiliency and enhance participation in international standards development;
- increase engagement with industry stakeholders; and
- continue to study the ICT industrial base to monitor industry developments"

GSA TIES is a non-profit organization that has several initiatives supporting the above recommendations.

GSA TIES Initiatives

Increasing Global Supply Chain Visibility. The lack of visibility on how chips propagate in the supply chain through unregulated distribution channels and chip assembly houses in China and Taiwan, results into broader geopolitical risks. GSA TIES focuses on promoting secure & trusted digitalization solutions through connected chips, devices, systems, and applications, by leveraging a broad ecosystem in the industrial base to accelerate deployment, growth and field use of end-to-end solutions and services that enable higher supply chain visibility, faster adoption rate, and economies of scale across the supply chain ecosystem.

Creating Supply Chain Incentives. The lack of economic incentive among supply chain participants to invest in secure & trusted Chips, PCBs, Devices and Systems creates cybersecurity vulnerabilities. While the CSF provides guidance for Response and Recovery, without forensics, mitigations, and recovery plans it will be difficult and expensive to deploy. GSA TIES is uniquely focused on promoting a digital thread linking secure digital assets with trusted physical assets and the cloud, in a way that data producers and data consumers are incentivized to create new service revenue streams.

Improving Ecosystem-level Traceability. Lack of standards and systems that do not have dependency on any one or two nations, companies, or services to function for proofs of authenticity and traceability for Response and Recovery, causes major risks. GSA TIES proposes a strategy to collaborate with NIST for a business ecosystem traceability platform designed to accelerate standards development, scale adoption of CSF guidelines, and streamline operating methods of all enterprises participating in the value chain.

Creating Value through Digitalization. Digitalization is the use of technologies that impact how work gets done, enabled by IoT devices that connect people, suppliers, consumers, services providers and users to smart infrastructure, create new services and applications that provide new conveniences and become integral to the safety and prosperity of society. There are fantastic possibilities ahead beyond our current imagination. This connectivity and dependence on the global supply chain ecosystem also creates vulnerabilities and security risks that must be addressed in a broader strategy for Digitalization.

Collaborating on Strategy for Supply Chain Ecosystem. The following proposal discusses a collaborative ecosystem strategy for supply chain traceability carried out by GSA TIES and NIST that has the potential to address supply chain cybersecurity risks and incentivize adoption of security & trust through the creation of economic value and the infrastructure to facilitate market access while limiting adversaries.

Supply Chain Opportunities and Risks

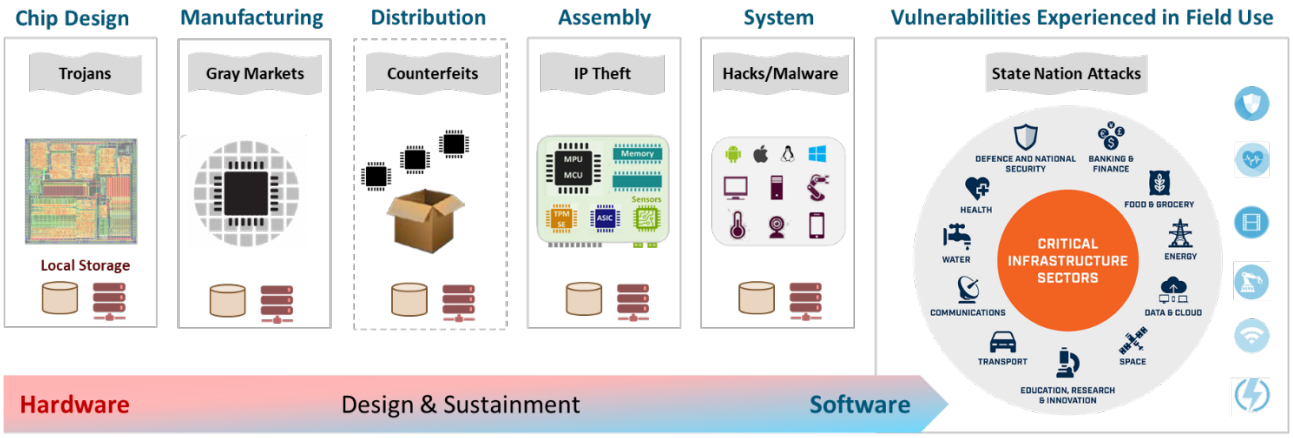
Global Opportunity. IoT, 5G, Cloud Computing, and AI will create $20 trillion for the global economy according to McKinsey & Company, by creating connected ecosystems of suppliers with infrastructure and applications for in aerospace-defense, automotive, industrial, networking, communications, healthcare, smart cities, agriculture, and other critical infrastructure enabling high growth markets. Billions of electronic devices are fueling a digital transformation of supply chains connecting IoT microelectronics suppliers to their customers and the broader infrastructure. This is opening up service-oriented market opportunities that will require new strategies to manage cybersecurity risks while enabling market access, commerce, and a plethora of connected IoT supplier services together with the smart infrastructure.

Cybersecurity Risks. With increased connectivity, attacker sophistication outpacing defender capabilities will exceed $3 trillion. Geopolitical risks coupled with the disaggregation of the hardware and software supply chains introduce vulnerabilities related to quality, reliability, and cybersecurity. These vulnerabilities start from the chip supply chain and propagate through the microelectronics products into the software infrastructure before they are experienced in end markets as IPR infringements, malware, DDoS outbreaks, and state nation attacks. As more intellectual property is misappropriated by China, the western world is facing major challenges in outcompeting on innovation and protecting against cybersecurity risks.

Lack of Supply Chain Visibility. The US $52 billion CHIPS Act in plus the EU €43 billion CHIPS Act will drive advancements in chip innovation and production capacity giving birth to billions of chips. However, the lack of visibility on how chips propagate in the supply chain through unregulated distribution channels and chip assembly houses mostly in China and Taiwan, results into broader geopolitical and geotechnical risks.

Hardware and Software intrusions, counterfeits, and tampering in the supply chain, affect confidentiality, integrity, safety, and the security of critical infrastructure.

Lack of supply chain visibility prevents: 1) the understanding and mitigation of supply chain vulnerabilities, 2) the creation of market place preference and differentiation based on supply practices and quality, and 3) the ability for governments to incentivize a more secure supply chain for critical infrastructure. A trusted supply chain traceability strategy can address these issues by improving visibility, measurement, and management and enabling hardware & software assurance to minimize risks and facilitate market access.



Lack of supply chain visibility threatens economic prosperity, privacy, national security and critical infrastructure

Proposed Strategy. The US and EU CHIPS Acts present a historic geopolitical opportunity to cooperate with international partners and allies in developing visibility and resiliency in microelectronics supply chains.

NIST has an opportunity to advance the current NIST "Framework for Improving Critical Infrastructure Cybersecurity" and for supply chain risk cybersecurity management by orchestrating an ecosystem strategy for public-private partnerships together with the GSA TIES. Such strategy must support the National Initiative for Improving Cybersecurity in Supply Chains by increasing supply chain visibility to facilitate market access, prevent unauthorized use, and develop a sustainable competitive advantage.

Supply Chain Executive Order

The POTUS Executive Order 14017 of February 24, 2021 on America's Supply Chains, captures key objectives related to the microelectronics supply chain:

- The US needs resilient, diverse, and secure supply chains to ensure economic prosperity and national security thought domestic production of microelectronics among other industries.
- Cooperation on resilient supply chains with allies and partners will foster collective economic and national security and strengthen the capacity to respond to emergencies.
- Agencies should, consult with outside stakeholders in the industry, academia, non-governmental organizations, etc. in order to fulfill the policy of this order.

DOC NIST and GSA TIES have similar mission and goals in line with the POTUS executive order and the potential to align on a strategy that support its objectives.

DOC and NIST Mission

The Department of Commerce's mission is to create the conditions for economic growth through Equity, Innovation, and Resilience as stated in the strategy for Strengthening American Competitiveness in the 21st Century. A key objective is to drive U.S. innovation and global competitiveness by investing in resilient supply chains, bolstering technological leadership, and engaging in strategic partnerships with our allies.

The strategic plan states that certain key initiatives that are to be led by NIST include:

- Revitalizing U.S. manufacturing and strengthening domestic supply chains;
- Accelerating the development, commercialization, and deployment of critical technologies;
- Strengthening U.S. participation in technical standards development; and
- Improving the security and integrity of the technology supply chain.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurements, science, standards, and technology and by leading in ways that enhance economic security and improve our quality of life. The NIST Cybersecurity Framework (CSF) has been a core part of its mission.

NIST CSF Evolution

In February 2013, Executive Order 13636 called for "Improving Critical Infrastructure Cybersecurity" and tasked DOC/NIST to establish a Cybersecurity Framework (CSF), which among other things focused on identifying cross-sector security standards and guidelines applicable to critical infrastructure and proposing areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations. Supply chain cybersecurity risk management one of those future areas needed today that requires broader collaboration to for visibility and traceability of Hardware & Software.

The global influence of NIST CSF enabled interagency and public-private collaboration and synergies with ISO and other standards bodies. However IoT connectivity and supply chain complexity grew at a faster pace than NIST's ability to expand CSF and support more standards for multiple markets. Several standards for the Hardware & Software supply chains evolved from SEMI, JEDEC, IPC, TCG, FIDO, SAE etc. This resulted into fragmentation and limited supply chain traceability which led to increased Hardware and Software vulnerabilities, as well as barriers to CSF adoption for IoT designers, end-users, and applications.

The rapidly growing IoT connectivity coupled with the lack of visibility in fragmented supply chains created opportunities and challenges which cannot be addressed by a single company. A collaborative, platform-based product design, delivery, and business ecosystem is needed in order to evolve an interoperable infrastructure for improving visibility among supply chains, market places, and end uses. Such platform can enable NIST to accelerate development of metrics and standards driven by the growth of data and analytics as a result of the increased visibility of the connected supply chain for microelectronics and IoT devices.

Supply chain traceability and security is a key starting point that establishes the foundation for visibility and control across, chips, electronics, software, IoT marketplaces, and connected ecosystems.

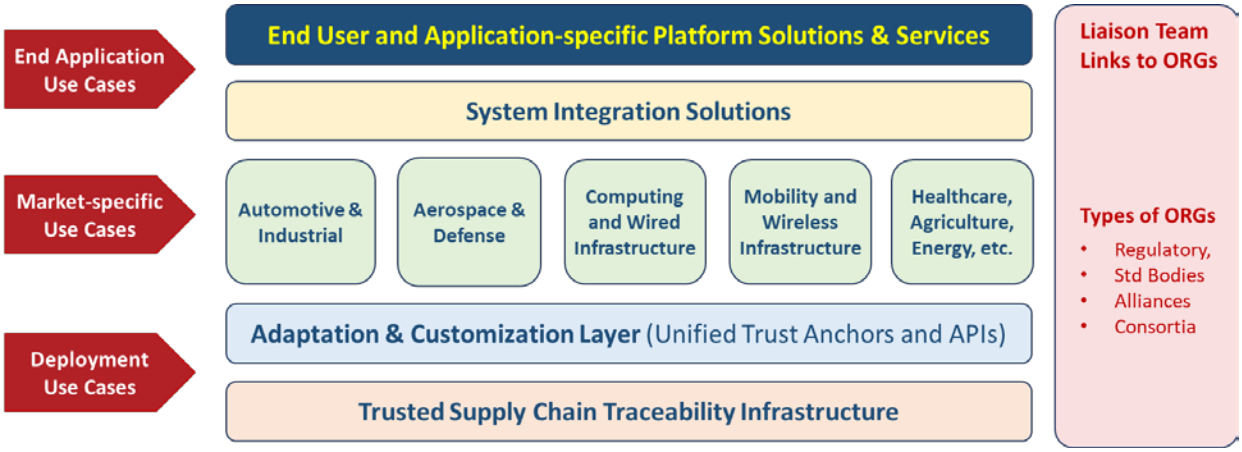
GSA TIES Mission

The Global Semiconductor Alliance (GSA) has over 300 members representing $500 billion in revenues in semiconductors and electronics. Members include chip suppliers, foundries, system companies, enterprise

software, cloud service providers, and OEMs. The GSA IoT is a collaboration platform where executives and experts meet with peers, partners, suppliers, and customers to address industry challenges and opportunities in areas of interest, including 5G, AI, edge applications, and Supply Chain Security (GSA TIES).

The GSA TIES is platform-based business ecosystem of companies and liaison organizations in the IoT value chain including chips, devices, systems, and software. GSA TIES members leverage the collective ecosystem IQ to network, collaborate on use cases and promote end-to-end solutions that minimize risk and maximize economic value. The goal of GSA TIES is to collaborate on secure and trusted solutions that accelerate adoption, growth, and field use of trusted electronic parts and data systems, enabled through traceability of connected chips, devices, systems, and applications in the IoT supply chain by promoting new revenue streams and business models and by facilitating public-private partnerships outside of GSA.

GSA TIES consists of several solutions working groups including, secure-connected SoC applications, secure silicon-to-cloud services for automotive markets, scaling trusted services from chip-to-cloud for IT & OT and Trusted Supply Chain Traceability and Digitalization from silicon to cloud. The goal of Trusted Supply Chain Traceability is to define use cases and promote end-to-end solutions that ensure the Hardware & Software products are trusted, secure, and assured to function as intended based on metrics and analytics.



A use case provides description of a problem plus steps and actions as experienced in a market or application by end users which can be addressed with end-to-end solution among stakeholders in order to create economic value. Use cases provide a basis for GSA TIES liaison relationships with regulatory agencies, standards bodies, and consortia.

NIST & GSA TIES Strategic Alignment

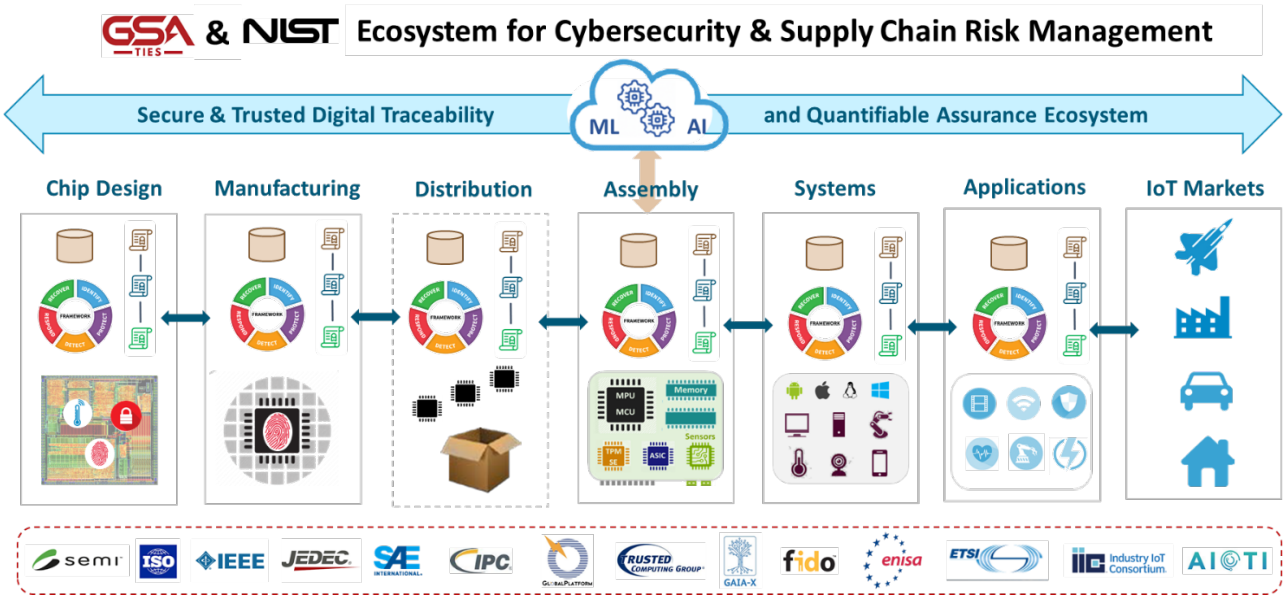
The US needs resilient, diverse, and secure supply chains to ensure economic prosperity and national security through increased production of microelectronics among all industries. Supply chain traceability tied to market preference and access is a key starting point that establishes the foundation for visibility and control across chips, electronics, software, IoT marketplaces, and connected ecosystems.

The GSA TIES is developing a platform-based business ecosystem for enabling supply chain visibility and market access where NIST can assume a leading role in driving interoperability and security guidelines in several standards bodies. As such, GSA TIES recommends strong collaboration between National Initiative for Improving Cybersecurity in Supply Chains in conjunction with NIST CSF related guidelines. 11, 12, 13, 14.

Numerous Executive Orders and strategic planning documents call for more and better Public-Private Partnerships, between the USG, the private sector, and academia. As the defense community started to embrace the idea of working closer with the commercial sector there were major barriers to accelerate innovation driven by legacy infrastructure and the disaggregation of the value chain.

The goal of GSA TIES is to collapse these barriers and accelerate growth of public-private partnerships by creating a collaborative, secure, and trusted business ecosystem that utilizes the collective IQ from chip-to-cloud in order to accelerate the adoption of IoT and monetization of IoT services for all vertical markets. This is attainable by leveraging the collective core competencies of NIST and GSA TIES on a strategy to evolve a traceable digital supply chain ecosystem utilizing consistent interoperability and cybersecurity guidelines for the digital transformation of participating stakeholders in the IoT value chain.

A strategic collaboration between NIST and GSA TIES has the potential to advance the connected supply chain and IoT infrastructure, accelerate business ecosystems tied to market access, incentives, preferences, and ultimately limit access to adversaries. Such strategy bridging private and public sectors can fuel economic growth, reduce adversaries' ability to misappropriate IP and enable a sustainable competitive advantage by acerating innovation, adoption, deployment, commercialization, and market access for secure IoT products and services offered by smart-connected IoT suppliers in various application markets.



In parallel, GSA TIES can promote use cases, end-to-end solutions, and operating methods in support of the NIST CSF guidelines. Both parties can leverage their global reach to collaborate with other standards bodies.

Traceable Digital Supply Chain Ecosystem

Background

Lack of supply chain visibility and compromise of vital supply chain elements are increasing, thereby impacting critical product safety, financial performance, and global political initiatives. The SolarWinds, Mirai Botnet, and the Big Hack Supermicro attack revealed that lack of visibility and economic incentives by fixed cost hardware suppliers to add security leads to substantial supply chain vulnerabilities and risks. With limited or no supply chain visibility, sanctions, and export controls for chips and materials used in IoT and electronics devices are not effective in keeping Western semiconductors out of Russian weapons.

The propagation and use of microelectronics and IoT devices needs to be securely monitored, managed, on a national and global basis, while protecting the privacy and intellectual property of participants. GSA TIES proposes a strategy toward a Secure & Trusted Digital Supply Chain Ecosystem that is capable of providing assurance and provenance of electronics systems, products, modules, and materials down to the individual unit, providing the level of control needed to secure our critical supply-chains while enabling market access.

Supply Chain Problem

The disaggregation of Integrated Device Manufacturers (IDMs) created economies of scale through specialization, but also led to fragmented supply chains creating an enormous attack surface. Supply chain vulnerabilities provide opportunities for adversaries to compromise hardware, software information, and material flows with coordinated cyberattacks, counterfeiting, rogue actors, fictitious or fraudulent distributors, phony OEM Suppliers, and smuggling operations.

There is little economic incentive among all parties in the supply chain to deliver trusted Chips, PCBs, Devices, and Systems. Supply chain complexity, legacy infrastructure, multiple standards, and limited knowledge base in tracing parts, result into field failures and nation state attacks whose root cause is hard to trace. That can adversely impact enterprises in the hardware and software value chain and cause vulnerabilities that can have devasting effects in smart infrastructure and national security.

While individual company or sector-based solutions exist across industries for specific remedies within a supply chain, there is no ecosystem-wide visibility, nor standardized mechanism to facilitate information exchange and data for a traceable business ecosystem. Such data includes market access for connected IoT products and services, while providing the evidence and proof needed for effective deterrents, precision control, and to reliably seek prosecution for those who intrude and compromise supply chains.

Digital Supply Chain Ecosystem

A collaborative platform-based business ecosystem that utilizes consistent cybersecurity guidelines, operating methodologies, and commercial technologies among all stakeholders in the value chain, must rapidly evolve sustainable solutions on top of the existing supply chain infrastructure.

The platform should provide ability to register and record data on materials, devices, integrated products, and processes; to include transactions, identification of associations, transfer of ownership, change of geographic location, and authentication, together across a single interoperable platform; to enable secure communication of data between entities within the design and sustainment supply chains; and to support a digital thread among smart-connected suppliers in the value chain that ensures interoperability and security across all participating companies and organizations, by using technologies that allow facts and data to be shared and be monetized, without compromise of privacy or intellectual property.

Vertically within each supply chain node, unique identities, and associated transactions are recorded, communicated and stored in a simple, yet highly secure environment, with minimal impact to existing operational and control paradigms. The use of tamper-evident (e.g. cryptographic keys, permission based blockchain) storage at the platform level, ensures data integrity throughout the entire lifecycle of materials and products. The resulting traceability data can be used for analytics to drive standards and metrics which are utilized, extended or created as applicable, within each supply chain node.

Some key capabilities that must be supported by the platform include:

- Secure provisioning and onboarding products to facilitate or regulate market access
- Creation of marketplace of digital data and asset authentication early in the supply chain
- Elimination of counterfeit materials or products entering the manufacturing supply chain
- Identification of any potentially compromised assets (materials, chips, products, enterprises)
- Root cause analysis of compromise, following the discovery of a cybersecurity incident
- Precise control of product transfers across geographical and political borders
- Prevention of use of devices that contain non-authenticated key materials
- Creation of digital thread that enables data producers to license their data to consumers

Benefits and Economic Value

The Digital Supply Chain Ecosystem affords all material manufacturers and product assemblers, the opportunity of protection of intellectual property, while simultaneously exchanging and accessing the necessary data for the control of their incoming and outgoing materials and products, in a way that minimizes additional cost and maximizes inclusivity within the industry in a sustainable way.

Specific benefits for smart-connected suppliers in the value chain are expected to include:

- Better visibility on product field use and remote lifecycle management
- Lower OPEX, higher differentiation, and reduced support costs and RMAs
- Evolution of digital thread and data that enable new IoT services and business models
- Prevention and elimination of unexpected product failure due to vulnerabilities
- Inhibition of unauthorized functionality introduced by third parties into products
- Heightened quality, safety, and security in the use of critical products in their intended use
- Deterrence of key intellectual property crossing unauthorized borders
- Prevention of ingress of counterfeit materials or devices directed to gray markets

Supply chain traceability and monitoring helps improve operating efficiencies, reduce OPEX, cost or risk, shorten time to market, and improve quality of results. Trusted supply chain provenance and traceability will provide economic incentives for stakeholders to participate in trusted ecosystems, become smart-connected suppliers and share the value and growth of IoT services for various application markets.

Collaborative Ecosystem Structure

Considering the disaggregation of the supply chain the variety of vertical markets, use cases, applications, and standards, end-to-end (chip-to-cloud) solutions and services needs to be sub-divided into domains. This can maximize collaboration among regulatory agencies, business enterprises, and standards bodies.

The development of the infrastructure for traceability of processes and assets can be accelerated by dividing the supply chain into domains of expertise that follow consistent cybersecurity guidelines, operating methodologies, digitalization workflows, and hand-offs across domains, including:

- IC Design to Packaged Chip Delivery: Internal traceability of IC design, manufacturing, assembly, and test. External traceability of chip delivery to ODMs, OEMs, and/or contract manufacturers.

- PCB Design and Assembly: Internal traceability of PCB design and provenance of Bill of Materials (BoM) for PCB/System Assembly. External traceability of device delivery to OEMs and integrators.

- Embedded System Delivery: Internal traceability of embedded system and external traceability of device/system delivered, at end-customer site, attested and securely onboarded to the cloud.

- Device Lifecycle Management: External (in-field) traceability of connected device, updates, internal status, real time application data, and internal traceability of (AI-based) applications and services.

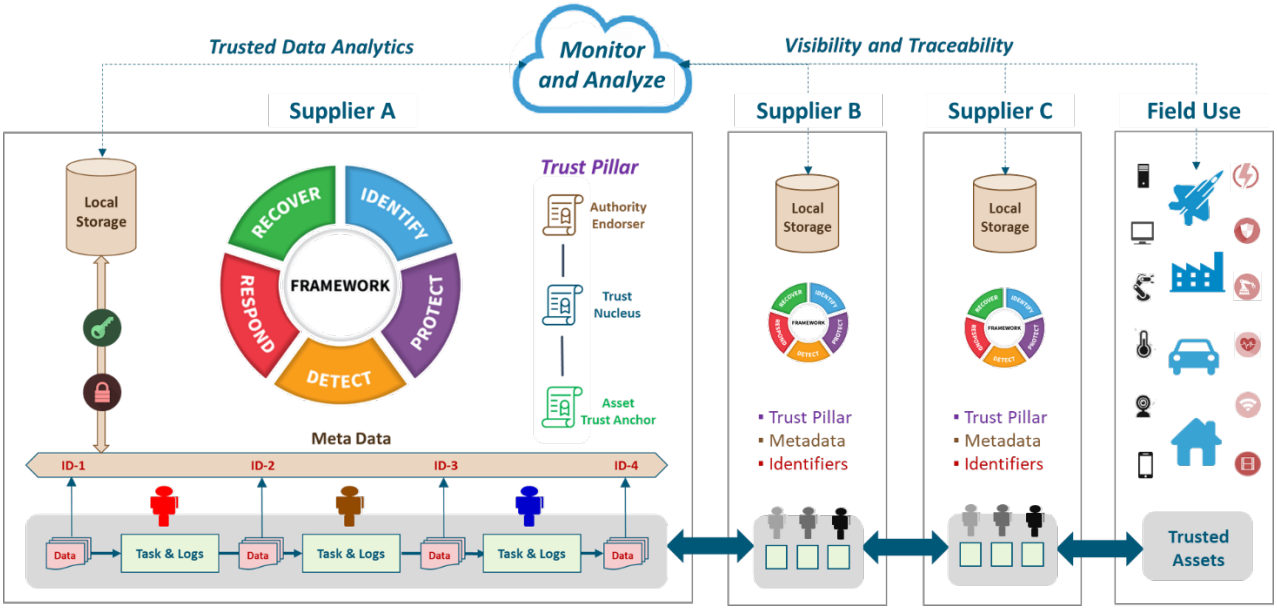
- Application Lifecycle Management: Internal & external traceability of software development, integrity, and software supply chain delivery, plus traceability of the data produced by edge apps.

- Recycling or Decommissioning: Internal & external traceability "catch all" of hardware for any markets. Recycled components must be reset and EOL components must be flagged as retired.

Collaboration among multiple parties in the value chain should be orchestrated in a way that it provides economic incentive to participating stakeholders. Consistent guidelines and digitalization of workflows for design, manufacturing, and delivery drives economies of scale and a digital thread for monetization of data.

Operational Guidelines & Methods

An end-to-end trusted platform ecosystem must enable a trusted operating model for all enterprises in the value chain that facilitates market access while enabling to monitor, measure and control unauthorized use.



Enterprises, must consistently support NIST CSF guidelines and interoperability standards and GSA TIES operating methodologies in order to be trusted value-add entities. As a result, delivery and distribution of microelectronics can be accelerated though a suitable mix of self-governance and parallel development.

An orchestration of a secure and trusted supply chain ecosystem is possible if all enterprises adopt a ***Trust Pillar*** as part of the investment in their digital transformation roadmap. This includes three components:

1. ***The Trust Nucleus*** which implements the details of the trust pillar. The approach might include but not limited to application of choice technologies or standardization on conventions, best practices, and interoperability standards that follow the NIST CSF guidelines.

2. ***An Asset Trust Anchor*** linked to the integrity of operation's deliverables such as physical assets (e.g. Chips, PCBs, devices, or systems) or a digital assets (e.g. Firmware, OS, Apps, or Digital Twins). Each entity cryptographically encodes details for verifying provenance and establishing chain of trust.

3. **An *Authority Root or Endorser*** as an objective source of truth on which relying parties depend to cryptographically attest the integrity of an asset through third-party endorser platforms such as consortia or certificate authorities, or distributed ledger technologies like blockchains.

Guidelines for cryptographically-backed composability at the Authority/Endorser end coupled with trust-chaining among producers and consumers that can be facilitated with Trust Pillars that can enable parallel development among self-governing enterprises across supply chain domains and scale trusted ecosystems.

In order for organizations to become trusted entities in the digital supply chain ecosystem, they need to accelerate their roadmap for the digital transformation of their enterprise. Some key capabilities that should be considered as part of the investment for digital transformation of the enterprise include:

- **Digitalization of Workflows** for provenance of process traceability including inputs, tasks, outputs, and deliverables among people, tools, and machines without compromising users' proprietary data.

- **Workflow Metadata Indexing** for traceable analytics of which data was produced when/how with ability for data consumers downstream to request and receive encrypted workflow data for a fee.

- **Cryptographic Traceability** including public-private ledgers of metadata indices with permissioned access for visibility and assurance of provenance and that workflows were not tampered or altered.

- **Asset Identifiers and Certificates** for Wafers, Dies, Chips, PCBs, Systems, Applications, used for provenance of product, authentication, and attestation of assets downstream in the supply chain.

- **Digitalized Market Access** whereby asset deliverables are tied to standards for monetization, enablement of scalable business models, new services, and data-driven revenue streams.

- **Secure Connectivity Protocols** across hardware, firmware, OS, Edge, cloud and smart infrastructure driven by devices Root of Trust based provisioning, onboarding, monitoring, reporting and updates.

- **Authentication and Attestation** methods to ensure that products do not contain counterfeit parts and are trusted via provenance and quantifiable assurance that they operate as originally intended.

- **Traceability & Lifecyle Standards** for internal and external traceability of digital and physical assets as well as product lifecycle security and risk management from manufacturing to recycling or EOL.

Investing in the above capabilities as part the digital transformation of enterprises in the IoT value chain, enables clear benefits with a compelling ROI. Pursuing these at an ecosystem-level with public-private

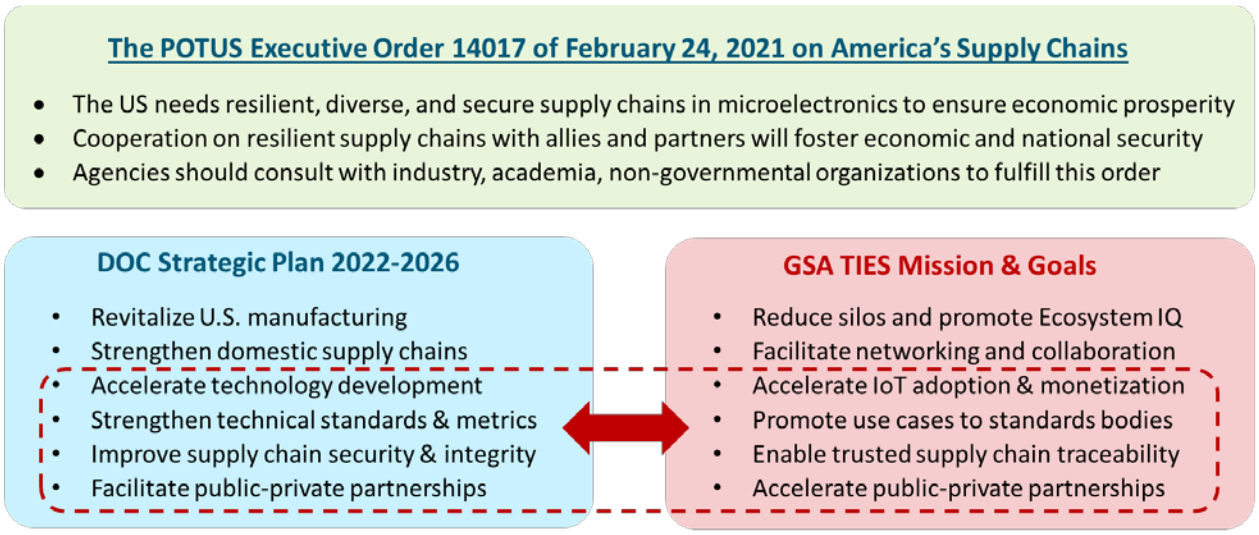
partnerships can accelerate adoption, drive economies of scale and enable the creation of a digital thread, growth of trusted data, and evolution of digital market places creating opportunities to monetize data with analytics used for ML/AI that will fuel a plethora of applications and digital twins.

NIST & GSA TIES Collaboration

The CHIPS Acts of the US and EU will create a unique opportunity for the Western partners and allies to leverage their design innovation core competencies, cultivate new talent, grow manufacturing capacity and produce high volumes of chips that must delivered globally through a secure & trusted digital supply chain ecosystem. Supply chain monitoring and traceability can facilitate market access for microelectronics while limiting adversaries' ability to misappropriate intellectual property or compromise critical infrastructure.

Through their global reach, DOC NIST and GSA TIES can play key role in collaborating to evolve the digital supply chain ecosystem including regulatory agencies, business enterprises, standards bodies, etc. Such evolution will require collaboration at multiple levels, strategic, industry, operational, and technical.

A collaboration between NIST and GSA TIES requires an understanding the core competencies of each party. At a high level, there is alignment on goals and objectives for developing a resilient microelectronics supply chain as stated in POTUS Executive Order, the DOC strategic plan, the initiatives being led by NIST.



DOC/NIST & GSA TIES can collaborate through a public-private partnership process to orchestrate an ecosystem platform that can improve supply chain traceability and market access for microelectronics and IoT products

At a high level, GSA TIES may drive the orchestration of the business ecosystem to accelerate public-private partnerships to develop supply chain solutions based on use cases for various application markets. NIST may drive supply chain interoperability guidelines in collaboration with other standards bodies. NIST and GSA TIES can collaborate to promote jointly the CSF cybersecurity and risk management guidelines and enterprise digitalization methods for better traceability, monitoring, and control in the supply chain.

Use Case Approach

GSA TIES has developed an initial repository of use cases in the supply continuum including chip, PCB, system, software, cloud, edge applications, and digital twins. Participating stakeholders, team-up to

collaborate on content that promotes end-to-end solutions to accelerate adoption of secure & trusted IoT applications that minimize risk and facilitate offering new services based on data, ML/AI and digital twins.

GSA TIES aim is to define supply chain use cases from an end user experience perspective and to encourage a "shift left" mentality for promoting end-to-end solutions. For example, a field failure that threatens safety, may be a vulnerability originating from rogue actor intruding into a software application at the edge, or a vulnerability originating from an unintentional error during chip design or manufacturing. Both require forward and backward supply chain traceability with quantifiable assurance on quality & security. Such assurances can be achieved though digitalization of enterprises in the value chain.

GSA TIES is currently orchestrating a series of connected domain-specific use cases and end-to-end solutions trusted supply chain traceability from chip design, manufacturing, distribution, PCB design & assembly, embedded system, secure device onboarding, over-the-air updates, edge applications, data analytics, and feedback loop back to the hardware supply chain to develop trusted digital twins. The aim to evolve trusted and traceable supply chain solutions for IoT in aerospace-defense, automotive, industrial, communications, networking, smart cities, etc.

A sample of the use case topics that are connected in the electronics value chain continuum from chip to IoT edge is shown below:

- Trusted Semiconductor IP Compliance with Digitalization of IP Design Process and Delivery
- Trusted Supply Chain Traceability with Zero Touch Chip Enrollment during test (at Birth)
- Manufacturing Integrity, Authenticity, and Quantifiable Assurance for Microelectronics
- Digitalization of Advanced Packaging Flow for Product Provenance and Traceability
- Trusted Traceability Procurement Logistics from Chip Supplier to PCB/System Consumers
- Using Virtual Identifier Threads for Reliability and Traceability of Parts Used in PCB
- Adding Blockchain for Trusted Traceability from PCB to Systems and Applications
- Root of Trust driven Zero Touch Secure Device Onboarding and OTA Applications
- Secure IC and IT Infrastructure for Functional Safety and Silicon Lifecycle Management

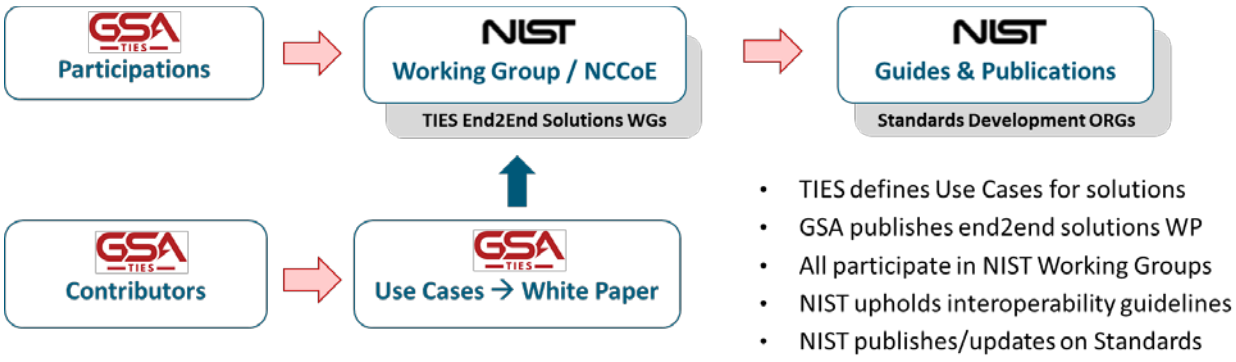
GSA TIES publications that reference standards will be shared the relevant standards bodies for their review, feedback and a request to provide notice for updates to forward to the GSA ecosystem. GSA TIES is forming liaison relationships with various standards bodies in order to increase visibility and collaboration on use cases driven by market needs. Use cases provide a vehicle for ecosystem collaboration where GSA TIES focuses on industry, business, and operational guidelines, while NIST and standards bodies focus on regulatory, interoperability, and best practices guidelines.

The scope of GSA TIES liaison relationships may vary by organization. For NIST, the GSA TIES liaison team believes that a more focused collaboration is needed, considering NIST's global reach in promoting CSF guidelines and the breadth of standards and metrics needed for supply chain quantifiable assurance.

Potential Collaboration with NIST

Certain GSA TIES Contributors who have experience and working relationships with NIST have identified an initial list of NIST guidelines and standards which are applicable for supply chain security and traceability, and are likely to be relevant for collaboration between NIST and GSA TIES. These are:

- NIST Cyber Security Framework (CSF)
- NIST Rick Management Framework (RMF)
- NIST Cybersecurity WP on Consumer IoT Products
- NIST SP 800-160 on Systems Security Engineering (SSE)
- NIST SP 800-161 on Supply Chain Risk Management (SCRM)
- NIST SP 800-171 / 172 on Securing (CUI)
- NIST SP 800-53 (rev5) on Security Controls
- NIST 800.175 Cryptographic Standards Guide
- NIST IR 8419 Blockchain for Mfg Traceability
- NIST SP 1800-34 on Validating the Integrity of Computing Devices



A potential liaison collaboration may start with GSA TIES Contributors participating in NIST working groups by sharing use cases and content that describes end-to-end solutions. Subsequently, the NIST working group may develop guidelines, share them with SDOs. Subsequently the SDOs may evolve standards and best practices and notify NIST and GSA TIES to raise awareness to their respective ecosystems.

With this strategy, use cases, guidelines, and standards may evolve in parallel in the ecosystem which can accelerate adoption supply chain traceability. As more liaison relationships are being formed, this strategy can help fill gaps in the supply chain continuum, fuel the growth of data and metrics, and therefore enable NIST accelerate the evolution of guidelines, standards, and security maturity models.

Security Maturity Models & Testbeds

The global awareness about CSF and the Security Maturity Model (SMM), has prompted several parties to develop application-specific methods for evolving SMMs. Some notable commercial references include, a Guide to Assessing Security Maturity by VMware and an industrial guide for Achieving NIST CSF Maturity with Verve Security Center. However, it is unclear how applicable these are for supply chain traceability.

One of the main challenges for evolving a supply chain traceability SMM is that the attack surface is large which makes it harder to determine the root cause vulnerabilities which may linked to quality, reliability or security issues that may occur anywhere in the supply chain. The evolution of metrics and simulation based digital twins may help evolve SMM for supply chain traceability, that can be augmented with practical guides for IoT such as the Industry Internet Consortium SMM as well as testbeds that can provide data from real life attacks.

Since supply chain traceability SMM is a relatively new concept, we may need to develop a strategy which may be another area of collaboration with NIST.

Summary and Recommendations

The challenge with the global microelectronics supply chain is that Big Tech and DoD collectively do not have sufficient infrastructure and economic power to sway fragmented supply chains to adopt an improved CSF just for risk management purposes. Along with an improved CSF, Governments must promote market incentives and standards for better visibility, traceability, and data monetization from the supply chain, in order to accelerate adoption and regulate market access for multiple industries.

What is needed is an orchestrated strategy for a strong business ecosystem that facilitates public-private partnerships that leverage NIST CSF, the Cybersecurity Supply Chain Risk Management framework, as well as supply chain security standards and interoperability guidelines together with other standards bodies. NIST and GSA TIES have an opportunity to lead globally such an ecosystem platform with our allies and develop a resilient, diverse, and secure supply chains to ensure economic prosperity and national security.

Recommendations:

- Incentivize adoption of risk-based capabilities, guidelines and standards for supply chain visibility.
- Catalogue existing standards for supply chain visibility and develop new standards where needed.
- Develop use cases for various secure & trusted applications that enable new IoT revenue streams.

All through public-private partnership and cooperation between NIST and GSA-TIES.

As of April 2022, GSA TIES participants include 40+ Companies and 100+ Contributors.