R01 - Encourage the use of Global Identifier Standards for supply chain traceability: The federal government should collaborate with international allies to create programs that incentivize suppliers to establish unique corporate IDs, product IDs, asset IDs and part IDs by using global standards such as GS1. Identifiers for tracking & tracing assets from design to manufacturing to field use, this will help enhance national security, protect public health and safety, promote environmental sustainability, and address consumer demand for transparency and accountability.

Justification

- Improve national security and supply chain transparency and reduce the risk of counterfeit or tampered goods used in critical sectors and by ensuring the authenticity and integrity of goods.
- Increase public health and safety by enabling faster identification and recall of products that may pose a functional safety, cybersecurity, or privacy concerns.
- Promote environmental sustainability by enabling greater visibility into the entire supply chain, from raw materials to recycling or disposal by facilitating tracking of materials and reducing waste.
- Address market needs and meet consumer demand for greater visibility, transparency and accountability by providing detailed information on the origin and journey of products.
- Enable the creation of a digital thread of data through digitalization of enterprise workflows and linking of workflow IDs to the product and asset IDs delivered by such workflows.

Implementation

- Collaborate with international allies to develop programs and guidelines that incentivize suppliers to adopt global identifier methods based on standards such as GS1.
- Encourage suppliers to establish unique corporate IDs, product IDs, asset IDs, and part IDs to drive consistency, interoperability, and trustworthiness in any supply chains.
- Facilitate the adoption of identifiers through incentives, education and outreach programs.
- Provide resources and guidance to suppliers to help them implement the new standards.
- Create incentives to upgrade existing supply chain management systems to include global identifier standards that ensure seamless tracking and tracing.
- Promote linking Global Identifiers for IoT devices to IoT cybersecurity labeling programs

Potential Implementation Barriers

- Resistance from suppliers who may view the implementation of ID infrastructure as burdensome and expensive and may be reluctant to invest time and money into adopting new standards.
- Technical challenges in implementing methodologies using identifier standards, especially for small suppliers who may lack the resources and expertise.
- The need for collaboration and coordination between different stakeholders in the supply chain, including suppliers, manufacturers, and distributors.
- The need for harmonizing identifier standards and systems used by different countries or regions and creating a secure and reliable database to store and manage the IDs and related information.

Federal Agencies Involved

- The Department of Commerce (DOC)
- The Department of Homeland Security (DHS)
- The Department of Defense (DOD)
- The Food and Drug Administration (FDA)
- The Federal Trade Commission (FTC)
- Small Business Administration (SBA)

Examples: These agencies can collaborate to establish programs and incentives for the use of Global Identifier Standards in their respective domains and require them procurement contracts and regulatory frameworks.

1. Department of Commerce (DOC) can collaborate with international standards organizations to promote the use of standards such as GS1 and create programs to incentivize suppliers to adopt them.

2. Department of Homeland Security (DHS) customs control unit can implement traceability standards for supply chain security, customs controls and tracking the products provenance and chain of custody.

3. Food and Drug Administration (FDA) can promote the adoption of global identifier standards to improve drug and medical device traceability, ensure product safety, and prevent counterfeiting.

Federal Considerations

- The federal government should collaborate with international allies to ensure that the implementation of global identifier standards is consistent with U.S. trade policy goals.
- The federal government should work to harmonize U.S. standards with international standards to facilitate interoperability.
- The federal government should prioritize the protection of sensitive information and ensure the security and reliability of databases used to manage the identifiers and related information.
- The federal government should ensure that agencies can collaborate to establish programs and incentives for the use of Global Identifier Standards in their respective domains.
- Agencies can also require the use of Global Identifier Standards in procurement contracts and regulatory frameworks and balance the costs benefits and challenges of implementing new standards

R02 - Promote trusted architectures for supply chain provenance and traceability: The federal government should incentivize hardware suppliers to develop trusted architectures for supply chain provenance, traceability chain of custody and IoT lifecycle management. By cryptographically linking SBOM to trusted HBOM in any IoT device or system, industries can help mitigate the risks associated with compromised components and ensure the security of critical systems. This will provide benefits for national security, public safety, and economic stability, making it a worthwhile investment for the government and society.

Justification

- The use of trusted architectures for supply chain provenance and traceability can help mitigate the risks associated with vulnerabilities or compromised components.
- Trusted architectures for supply chain provenance and traceability can increase the trustworthiness of critical IoT systems, which is key for national security, public safety, and economic stability.
- These architectures can increase consumer confidence in the products they purchase, and prevent supply chain attacks and data breaches leading to greater economic benefits for businesses.
- Cryptographic linking of SBOM to trusted HBOM enhances supply chain security, visibility, chain of custody and IoT lifecycle management.

Implementation Considerations

- Educate stakeholders in the value chain on the benefits of using trusted architectures for supply chain provenance and traceability.
- Promote industry adoption of trusted architectures through education and outreach. Incentivize hardware suppliers to develop trusted architectures for supply chain provenance and traceability.
- Develop guidelines for how the trusted architectures should be implemented by linking of HBOM and SBOM for provenance and traceability and encourage the adoption of standards and best practices.
- Encourage collaboration between government agencies and industry stakeholders (Private-Public Partnerships) to develop and promote trusted and traceable architectures.

Potential Implementation Barriers

- Lack of awareness or understanding of the benefits of trusted architectures.
- Resistance from industry stakeholders who are not interested in investing in new technologies.
- Implementation costs associated with developing and deploying new systems.
- Technical challenges associated with integrating new systems with existing infrastructure.
- Complexities involved in developing and deploying trusted architectures at scale.

Federal Agencies Involved

- National Institute of Standards and Technology (NIST)
- Department of Homeland Security (DHS)
- Department of Defense (DOD)
- Department of Commerce (DOC)
- Federal Trade Commission (FTC)
- Federal Energy Regulatory Commission (FERC)
- Cybersecurity Infrastructure Security Agency (CISA)
- General Services Administration (GSA)
- Industry stakeholders such as hardware suppliers and manufacturers

Examples: The DOD and CISA may require the use of trusted architectures for supply chain provenance and traceability in defense and critical infrastructure. The (GSA) may promote them in government procurement.

1. The National Institute of Standards and Technology (NIST) may develop guidelines and tools for implementing trusted architectures for supply chain provenance and traceability.

2. The Federal Energy Regulatory Commission (FERC): Promote the use of secure hardware and software components in the energy sector to ensure the reliability of critical infrastructure.

3. The Federal Trade Commission (FTC): Enforce regulations on deceptive trade practices that may compromise the security of supply chains.

Federal Considerations

- Funding and budget allocations for incentivizing hardware suppliers to develop trusted architectures for supply chain provenance and traceability.
- Developing and implementing policies and regulations related to the use of trusted architectures.
- Coordinating efforts between federal agencies and the commercial sector, to ensure a unified approach to implementing trusted architectures.
- Funding and resource allocation to support the development and implementation of trusted architectures.
- Promoting regulatory and policy changes to incentivize industry adoption of trusted architectures.
- Collaboration and coordination with industry stakeholders to develop and deploy trusted architectures at scale.

R03 - Incentivize IoT Systems Supply Chain to accelerate adoption of trusted traceability. Ensuring the security and integrity of the connected Electronics and IoT Systems supply chain is key to accelerate IT/OT convergence and prevent cyber-attacks in critical infrastructure that could result in serious human and economic losses. Unlike classic supply chains focusing on Availability of goods, IoT Systems also require Confidentiality and Integrity (CIA)

for data protection and assurance. The term "trusted" in this context refers to whether the IoT System and its parts operate as intended and whether the data it produces is trusted and not compromised.

Justification

- Ensure the confidentiality and integrity of IoT electronics supply chains to prevent cyber-attacks in critical infrastructure and protect against human and economic losses.
- Accelerate IT/OT convergence with adoption of trusted traceability methods for the electronics supply chain that enhance the efficiency & effectiveness in the delivery of critical infrastructure services.
- Enable companies and businesses to foster innovation, create a competitive advantage with smart-secure-connected electronics IoT Systems and ultimately become smart-connected-secure suppliers.
- Enable the creation of trusted connected ecosystems that accelerate end-to-end innovation, monetization and growth of IoT economies.

Implementation Considerations

- Offer tax credits, grants, or other financial incentives to companies that market electronics products with traceable parts country of origin, provenance, and journey in the supply chain.
- Require contractors and suppliers to adhere to specific security and traceability standards when bidding on government contracts, particularly for critical infrastructure.
- Establish a certification process for connected electronics products that meet security and traceability standards to enhance trust in the supply chain.
- Partner with industry associations and other stakeholders to develop best practices and guidelines for secure connected electronics product development and supply chain management.

Barriers

- Lack of awareness: Some companies may not be aware of the benefits of traceability or the risks associated with untraceable components in their supply chain.
- Lack of expertise: SMEs may lack the expertise and resources to implement traceability methods effectively.
- Limited supply chain visibility: In some cases, it may be difficult to trace components back to their original source due to limited visibility into the supply chain.
- Complexity: Implementing traceability methods in a complex supply chain can be challenging and time-consuming.
- Data confidentiality concerns: Collecting and storing data for traceability purposes may raise concerns about data trust and potential risks of using it for various applications.
- Cost of implementation: Companies may be resistant to investing in trusted traceability methods due to limited budgets, or lack of expertise or lack of standardized security and traceability protocols.

Federal Agencies Involved

- Department of Homeland Security (DHS)
- Department of Defense (DOD)
- National Institute of Standards and Technology (NIST)
- Federal Energy Regulatory Commission (FERC)
- Federal Communications Commission (FCC)
- Department of Energy (DOE)
- Cybersecurity Infrastructure Security Agency (CISA)

- Environmental Protection Agency (EPA)
- Small Business Administration (SBA)

Examples: Some federal agencies such as the DHS may require adoption of trusted traceability methods in critical infrastructure systems. Others such as NIST may develop and promote guidelines for adoption of such methods.

1. The Department of Energy (DOE) can establish incentives for utilities to adopt secure IoT systems in order to protect critical infrastructure from cyber-attacks.

2. The Cybersecurity Infrastructure Security Agency (CISA) can provide education and training to businesses and organizations on how to implement secure IoT supply chain processes and offer resources to assess and mitigate supply chain risk.

3. The Federal Communications Commission (FCC) can require manufacturers of connected devices to implement secure supply chain processes and ensure the security and integrity of IoT systems.

Federal Considerations

- The federal government should provide financial incentives to companies to encourage the adoption of trusted traceability methods that are aligned with executive orders and broader government priorities.
- The federal government should work with industry stakeholders offer tax credits, grants, or other financial incentives to companies that offer traceable connected electronics products.
- The federal government should require contractors and suppliers to adhere to specific security and traceability standards when bidding on government contracts for critical infrastructure.
- The federal government should promote partnerships of industry associations and stakeholders to identify potential gaps in the connected electronics supply chain and develop targeted solutions to address them.

R04 - Promote the Creation of Traceable and Trusted IoT Network Ecosystems: Drive awareness and interoperability programs on how trust is established among devices, networks, and personas operating in connected IoT environments, in ways that enable secure and reliable data exchanges and protect against malicious attacks, data breaches, and other security threats. By promoting a framework of trust, the government can have a significant impact on the security and resilience of critical infrastructure, information sharing, innovation, data protection, international cooperation and international trade.

Justification

- Trusted network ecosystems facilitate information sharing, innovation, data protection, international cooperation, and international trade.
- They improve the security and resilience of critical infrastructure with information sharing, analytics and feedback for digital twins
- They enable trusted data exchanges, and protect against malicious attacks and data breaches
- Manage threats and mitigate risks and consequences, economic, reputational and loss of life

Implementation Considerations

- Drive awareness on how security and trust is established among in IoT networks among devices, personas and applications operating in connected IoT environments.

- Work with industry stakeholders to develop and promote standards, guidelines, and interoperability programs to ensure that devices and networks can communicate securely and reliably.
- Encourage the development and adoption of secure and trusted IoT technologies and solutions.
- Work with industry, academia, and other stakeholders to promote innovation and research in the area of IoT security.

Potential Implementation Barriers

- Implementing trusted IoT network ecosystems may require significant upgrade to existing legacy systems and supply chain processes. Lack of standards and best practices is a key barrier.
- Companies may be resistant to investing in trusted IoT network ecosystems due to the costs involved.
- Lack of awareness and understanding of the importance of IoT security and trust.
- Limited interoperability between IoT devices and networks.
- Challenges in securing legacy systems that may not have been designed with security in mind.
- Resistance to change and the adoption of new technologies and approaches.

Federal Agencies Involved

- Department of Homeland Security (DHS)
- National Institute of Standards and Technology (NIST)
- The Federal Trade Commission (FTC)
- Department of Energy (DOE)
- Environmental Protection Agency (EPA)
- Federal Communications Commission (FCC)
- Environmental Protection Agency (EPA)
- Small Business Administration (SBA)

Examples: Some agencies such as DHS can promote the adoption of trusted IoT network ecosystems in critical infrastructure systems while DOC/NIST may work international allies to harmonize of guidelines and standards.

1. The FCC can promote the development of secure and reliable IoT networks by allocating and managing spectrum resources for IoT communications and promoting the use of secure network protocols.

2. The EPA can promote the use of IoT sensors and networks to monitor and manage environmental quality and promote sustainability.

3. Small Business Administration (SBA): The SBA can provide resources and assistance to small businesses seeking to implement secure and reliable IoT networks and devices.

Federal Considerations

- The federal government should work with industry stakeholders to develop guidelines for trusted IoT network ecosystems and provide financial incentives to companies to encourage their adoption.
- The federal government should promote the adoption of workflow processes that improve the security and resilience of critical infrastructure.
- The federal government should develop a comprehensive strategy for promoting the security of IoT devices and networks and invest in infrastructure to accelerate adoption of secure IoT solutions.
- The federal government should work with international partners to promote and harmonize global standards and best practices for securing IoT devices and networks.

- The federal government should encourage the use of secure IoT technologies and solutions in federal agencies and critical infrastructure sectors and encourage the creation of networked ecosystems

R05 - Accelerate evolution of trusted digital threads across value chains: The government should support the development of digital threads across value chains by incentivizing companies to digitalize their workflows, link their internal data IDs and holistic Bills of Materials (DBOM, HBOM, SBOM) to data market toward trusted digital threads that will enable marketplaces of data producers and data consumers platforms. Such platforms can have a significant impact on supply chain traceability, innovation, efficiency, security and economic growth.

Justification

- Increase end-to-end visibility of a product's lifecycle, and enable better supply chain visibility and security, to reduce risk of cyberattacks, product counterfeiting, and product recalls.
- Companies the adopt a digital thread can improve supply chain efficiency, reduce costs, manage vulnerabilities, increase differentiation, and promote innovation & data monetization.
- Digital threads can enable marketplaces of data producers and data consumers, creating new business opportunities for innovation and revenue stream that will fuel the future digital economies.
- Accelerate adoption by linking digital threads (DBOM, HBOM, SBOM) across value chains in ways protect proprietary IP but enable data marketplaces.

Implementation Considerations

- Develop educational and training programs to help businesses implement digital threads. Establish guidelines for creating a digital thread, including standards for data sharing and security.
- Incentivize companies to digitalize their workflows by offering tax credits, grants, or subsidies for investing in digital technologies.
- Encourage collaboration between industry leaders and government agencies to raise awareness on best practices and develop interoperable digital thread methods.
- Leverage the Cybersecurity labeling program to create a digital trail of IoT systems Bills of Materials (DBOM, HBOM, SBOM, Security keys, etc.) that will vary by vertical market.
- Provide funding for research and development of digital thread guidelines, methods and standards to facilitate development of best practices and guidelines for implementing digital threads.

Potential Implementation Barriers

- Resistance from businesses to adopt new digital technologies and workflows. The upfront costs of digitalization may be prohibitive for some companies, even thought the ROI may justify them.
- Some companies may be hesitant to share data due to concerns about intellectual property and competitive advantage. The digital thread should allow sharing of data at the producer’s discretion.
- Different industries may have varying requirements for digital threads, making it challenging to establish common standards and overcome concerns around data privacy and security and interoperability.

Federal Agencies Involved

- National Institute of Standards and Technology (NIST)
- Department of Commerce (DOE)
- Department of Homeland Security (DHS)
- Department of Defense (DOD)

- Food and Drug Administration (FDA)
- Environmental Protection Agency (EPA)
- Cybersecurity Infrastructure Security Agency (CISA)
- Department of Energy (DOE)
- Federal Trade Commission (FTC)
- Small Business Administration (SBA)

Examples: NIST may develop standards and guidelines for the creation of a trusted digital thread, while the DOC may promote the adoption of digitalization and the Cybersecurity labeling program linking to corporate Identifiers.

1. The FTC can encourage companies to adopt digital threads to improve transparency and accountability in supply chains and prevent fraud.

2. CISA can provide guidance on cybersecurity best practices for digital thread adoption to protect against cyberattacks.

3. The EPA can encourage the adoption of digital threads in the environmental sector to improve monitoring and reduce waste.

Federal Considerations

- The federal government should provide financial incentives to companies to encourage the adoption of digitalization and the creation of a digital thread for both SMBs as well as large enterprises.
- The federal government should work with industry stakeholders to develop guidelines for creating a trusted digital thread and how to comply with regulatory requirements for data privacy and security.
- The federal government should promote the adoption of a digital thread in government procurement processes to improve supply chain traceability and security.
- The federal government should foster public-private partnerships to promote innovation and collaboration in creating trusted digital threads that comply with relevant federal regulations and standards.

R06 - Incentivize the creation and growth of trusted data marketplaces: The government should incentivize the creation and growth of trusted data marketplaces where data producers and data consumers query and share information about data, enabling better visibility, traceability, and monetization while protecting proprietary IP. Trusted data marketplaces can drive incentives for market preference, regulated market access & use of goods as well as tax credits or subsidies. Platforms that facilitate adoption of marketplaces can help data producers and consumers reduce costs, improve efficiency by streamlining processes and eliminate redundancies, especially in complex supply chains where information flows are often fragmented or disconnected.

Justification

- Establish market preference and market access with better supply chain visibility and traceability
- Reduce costs of data sharing and licensing among data producers and consumers
- Improve efficiency by streamlining supply chain processes to locate and license relevant data
- Reduce redundancies and simplify logistics in complex supply chains for access and use of goods
- Increase data visibility in value chains to enable growth of market places that will fuel digital economies

Implementation Considerations

- Identify suitable marketplaces to incentivize and support
- Develop guidelines and regulations for access and use of data in the marketplace
- Provide tax credits and subsidies to encourage participation
- Promote the benefits of the marketplace to potential participants
- Ensure data security and confidentiality measures are in place
- Monitor and evaluate the effectiveness of the marketplace
- Use analytics to improve visibility, traceability, efficiency, and cost

Potential Implementation Barriers

- Lack of awareness about the benefits of marketplace platforms
- Concerns and resistance over data security and confidentiality
- Difficulty in regulating and monitoring access and use of data in the marketplace
- Unwillingness to share proprietary data without a license
- Lack of open and participatory platforms for data marketplaces

Federal Agencies Involved

- Department of Commerce (DOC)
- Small Business Administration (SBA)
- Department of Agriculture (USDA)
- Department of Homeland Security (DHS)
- Food and Drug Administration (FDA)
- Federal Trade Commission (FTC)
- National Science Foundation (NSF)
- General Services Administration (GSA)
- National Institute of Standards and Technology (NIST)
- Federal Trade Commission (FTC)

Examples: While NIST may develop standards and guidelines for data sharing and security, the DOC and DHS may promote data sharing initiatives among domestic and international supply chains.

1. The Food and Drug Administration (FDA) could collaborate with trusted data marketplaces to improve the safety and efficacy of drugs and medical devices.

2. The Federal Trade Commission (FTC) could develop guidelines for data marketplaces to ensure that they protect consumer privacy and prevent data breaches.

3. The General Services Administration (GSA) could promote the use of trusted data marketplaces in government procurement.

Federal Considerations

- Implement data privacy and confidentiality regulations based on experience (GDPR, CDPP, etc.)
- Develop policies to prevent monopolies in the data marketplace
- Provide education and resources to help organizations participate in data marketplaces. Ensure that the marketplace is accessible to small businesses and not just large corporations
- Balance incentives for participation with data security and privacy concerns
- Coordinate with other federal agencies and international allies to ensure a cohesive approach.

- Align with broader government efforts to promote open innovation platforms

R07 - Subsidize digitalization of enterprises in the IoT value chain: The digitalization of all business functions (design, production, marketing, procurement, distribution, etc.) enables more efficient management, greater visibility and traceability over supply chains to track products, monitor quality, and fix issues or defects. By using cryptographic methods, digitalization can have a major impart in the security, reliability, and integrity of the data for the digital economy. By providing incentives for businesses to adopt digital tools, the federal government can help promote ecosystems that create opportunities for businesses and workers and drive economic growth.

Justification

- Digitalization of business functions leads to greater management, efficiency and visibility in supply chains
- Cryptographic methods improve security, reliability, and integrity of digital data, especially in hand-offs
- Digitalization enables secure ecosystems, opportunities for businesses & workers and economic growth
- Subsidizing digitalization can lead to increased adoption of digital technologies and tools by businesses
- Digitalization of value chains enhances security, reliability, and integrity of data for the digital economy.

Implementation Considerations

- Develop and communicate clear guidelines and criteria for eligibility for the subsidies
- Create a streamlined application and approval process for businesses to apply for the subsidies
- Ensure that the subsidies are accessible to businesses of all sizes and types in the IoT value chain
- Monitor the effectiveness of the subsidies to ensure that they are achieving the intended outcomes
- Provide incentives for businesses to invest in digitalization and adopt digital technologies and tools.
- Encourage collaboration and knowledge sharing among businesses to promote best practices.

Potential Implementation Barriers

- SMBs lack the resources or expertise to effectively implement digital technologies and tools
- The initial cost of implementing digital technologies and tools may be a barrier for some businesses
- Resistance to change or adoption of new technologies, or lack of technical expertise and resources.
- Concerns over the security and confidentiality of digital data may discourage some businesses from adopting digital technologies and tools

Federal Agencies Involved

- Department of Commerce (DOC)
- Department of Energy (DOC)
- Department of Homeland Security (DHS)
- Environmental Protection Agency (EPA)
- National Science Foundation (NSF)
- Department of Transportation (DOT)
- National Institute of Standards and Technology (NIST)
- Cybersecurity Infrastructure Security Agency (CISA)
- Small Business Administration (SBA)

Examples: NIST can provide guidance on cybersecurity best practices for digitalization. SBA can offer subsidies, resources, and support for small businesses to adopt digital technologies based on subsidies from the DOC.

1. The Environmental Protection Agency (EPA) may provide technical assistance and funding to businesses that are looking to adopt IoT technologies to improve environmental monitoring and sustainability efforts.

2. The National Science Foundation (NSF) may provide funding for research and development of new IoT technologies and digitalization tools that can drive innovation and economic growth.

3. The Department of Transportation (DOT) may work with industry groups to develop standards for the use of IoT technologies in transportation and logistics, to ensure the efficient and secure movement of goods.

Federal Considerations

- Ensure that the subsidies align with broader federal priorities and goals, such as promoting economic growth and national security and that digitalization efforts prioritize security and privacy protections.
- Coordinate with other federal agencies to ensure that the subsidies do not conflict with other federal programs or initiatives to promote consistency and avoid redundancy.
- Monitor and evaluate the impact of the subsidies in IoT value chains and the economy
- Encourage equitable access to digital technologies and tools across different regions and industries and ensure that digitalization efforts prioritize security and privacy protections.

R08 - Promote creation and orchestration of trusted value chains: Promote orchestration of networks of entities, such as manufacturers, service providers, and regulatory bodies, that interact to establish and maintain Trust through collaboration and accountability to ensure that the IoT value chains and infrastructure are secure, transparent, trustworthy. By providing incentives for businesses to adopt transparent workflow practices, the federal government can help drive economic growth and social responsibility while protecting against supply chain attacks, device vulnerabilities and critical infrastructure risks.

Justification

- Maintain transparency, trust and accountability throughout the supply chain
- Grow economic value collaboration and accountability among enterprises in the value chain
- Protect against supply chain risks of vulnerabilities, intrusions, and adversaries
- Ensure that IoT supply chain infrastructure is secure, transparent, trustworthy
- Drive shared monetization among stakeholders in the value chain and scalable economics

Implementation Considerations

- The federal government can provide incentives for businesses to adopt transparent workflow practices.
- Networks of entities can be orchestrated to maintain trust through collaboration and accountability.
- Establish regulations, guidelines, standards for the creation and maintenance of trusted value chains.
- Provide incentives for businesses for collaboration and adoption of transparent workflow practices

Potential Implementation Barriers

- Competitiveness and lack of collaboration and accountability between entities within the value chain.
- Resistance to change and adoption of transparent workflow practices and open ecosystems.
- Cost of implementing and maintaining secure practices and trustworthy value chains.
- Lack of awareness about the importance of trustworthy and secure supply chains.
- Difficulty in orchestrating and coordinating multiple stakeholders across fragmented supply chains

Federal Agencies Involved

- National Institute of Standards and Technology (NIST)
- Department of Commerce (DOC)
- Federal Trade Commission (FTC)
- Department of Homeland Security (DHS)
- Food and Drug Administration (FDA)
- Small Business Administration (SBA)
- Cybersecurity Infrastructure Security Agency (CISA)

Examples: NIST may develop and promote standards and best practices, the DOC may provide guidance and resources for businesses, CISA may drive R&D for secure systems, and DHS promote trust in global value chains.

1. The Department of Energy can promote the adoption of transparent workflow practices among energy companies and work with them to maintain a secure and trustworthy infrastructure.

2. The Food and Drug Administration can collaborate with regulatory bodies and service providers to ensure a secure and trustworthy medical IoT infrastructure.

3. The Federal Trade Commission can provide guidance and incentives for businesses to adopt transparent workflow practices and collaborate to maintain a secure IoT infrastructure.

Federal Considerations

- The federal government should ensure that any incentives provided align with established guidelines and standards for trusted value chains.
- Foster collaboration among federal agencies, industries and value chains to accelerate adoption with a unified approach to IoT supply chain security and transparency.
- Develop continuous monitoring and updating of regulations and standards are necessary to keep up with emerging threats and technologies.
- Ensure that incentives and regulations are not overly burdensome for businesses

R09 - Subsidize orchestrated Public-Private Partnerships across value chains: The federal government can accelerate the creation of traceable supply chains by subsidizing orchestration of connected Private-Public Partnerships across complex value chains which digitalize portions of supply chains piecemeal using consistent methods of “receivables-process-deliverables”. This can help supply chain stakeholders to collaborate in parallel and accelerate adoption of the digital thread, and be more efficient which will help businesses to grow new data revenue streams on top of IoT products and services which will fuel economic growth.

Justification

- Subsidizing orchestrated value chain partnerships can accelerate the adoption of end-to-end digital thread and traceability in complex supply chains.
- Digitalizing portions of supply chains piecemeal using consistent methods can help stakeholders collaborate in parallel and accelerate adoption of traceability.
- Creating resilient and secure supply chains can help businesses drive economic growth.
- Improve supply chain traceability can help businesses reduce risk and increase resilience, which can lead to business and economic growth.

Implementation Considerations

- Subsidize the orchestration of connected Private-Public Partnerships across complex value chains.
- Promote consistent digitalization methods for "receivables-process-deliverables" across supply chains by digitalizing portions of supply chains piecemeal to facilitate collaboration among stakeholders.
- Fund the development of digital infrastructure, training programs, and other resources necessary for successful partnership implementation.

Potential Implementation Barriers

- Resistance to change from supply chain stakeholders who are accustomed to traditional methods.
- Lack of technical expertise and infrastructure to implement digitalization across the supply chain.
- Costs associated with implementing digitalization across the supply chain.
- Resistance from supply chain stakeholders who may be hesitant to share data or work with competitors.
- Resource constraints for smaller businesses that may not have the capacity to participate in partnerships.

Federal Agencies Involved

- Department of Commerce (DOC)
- Department of Agriculture (USDA)
- Environmental Protection Agency (EPA)
- Food and Drug Administration (FDA)
- Department of Homeland Security (DHS)
- Federal Trade Commission (FTC)
- Federal Communications Commission (FCC)
- Small Business Administration (SBA)

Examples: The DOC can provide funding for PPP supply chain digitalization initiatives, NIST may develop and promote best practices and SBA may provide resources and support for smaller businesses to participate in PPPs.

1. The Department of Homeland Security can provide security certifications and audits for the digital components of the supply chains to build trust among PPP participants.

2. The Federal Trade Commission can enforce antitrust regulations to prevent PPP monopolies from forming in digital marketplaces and incentivize PPPs to include small and innovative businesses in the mix.

3. The Federal Communications Commission can work with private sector partners to improve connectivity and communication across supply chain networks.

Federal Considerations

- The federal government should prioritize partnerships that promote transparency, efficiency, and security.
- The federal government should ensure that partnerships do not unfairly disadvantage smaller businesses or create monopolies.
- The federal government should be prepared to address potential security and confidentiality concerns associated with increased data sharing in supply chains.
- The federal government should consider the potential impact on domestic and international trade policies and importance of ensuring that the subsidies are distributed equitably across various stakeholders.

R10 - Establish data policies that drive economic growth: Monetization of data will require infrastructure for Security, Privacy, Data Sharing, Ownership and Control Frameworks, Identity and Access management (IAM), Data Protection, Sharing and Exchange, plus Data Analytics with AI to minimize supply chain risk and maximize economic value. Policies related to data can have a major impact on privacy, security, interoperability, transparency, accountability, innovation, and monetization, as it can fuel synergistic ecosystems and the future digital economies.

Justification

- Data policies can have a major impact on privacy, security, interoperability, transparency, accountability, innovation, and monetization.
- A lack of clear and consistent data policies can create uncertainty and hinder the growth of digital economies.
- The monetization of data can drive business growth and fuel synergistic ecosystems, but it requires infrastructure for security, privacy, data sharing, ownership and control frameworks, identity and access management (IAM), data protection, sharing, licensing, and data analytics with AI to minimize supply chain risk and maximize economic value.

Implementation Considerations

- Promote infrastructure for security and privacy, data sharing, ownership and control frameworks, identity and access management (IAM), data protection, sharing and exchange, and data analytics
- Establish policies related to data need to be established and enforced to ensure compliance with regulatory requirements.
- Evolve policies in consultation with industry, academia, civil society, and government agencies and keep them up-to-date with changing technologies and business models.

Potential Implementation Barriers

- Lack of knowledge about data policies, resistance to change and implementation of new policies. Lack of clarity on how data policies will impact stakeholders, particularly on privacy and security.
- The lack of clear and consistent data policies can create uncertainty and hinder the growth of digital economies.
- The cost of establishing infrastructure for data security, privacy, sharing, and exchange, as well as data analytics with AI, could be significant.
- Developing data policies that balance privacy and security concerns with innovation and economic growth can be challenging.

Federal Agencies Involved

- Department of Commerce (DOC)
- Federal Trade Commission (FTC)
- Department of Homeland Security (DHS)
- National Institute of Standards and Technology (NIST)
- Department of Justice (DOJ)
- Department of Homeland Security (DHS)

Examples: NIST may provide guidance on data security and privacy, DOC may promote data sharing and exchange, FTC may enforce data protection laws, and DOJ can investigate and prosecute data breaches and cybercrimes.

1. The Department of Homeland Security (DHS) may develop data confiddentiality and security regulations that protect sensitive information while promoting innovation and economic growth.

2. The Food and Drug Administration (FDA) may establish data sharing policies that promote innovation in medical research and development while ensuring patient privacy and safety.

3. The Cybersecurity Infrastructure Security Agency (CISA) may establish data security standards and policies that protect critical infrastructure and reduce cyber threats.

Federal Considerations

- The federal government should consider potential impact of data policies on privacy, security, transparency, accountability, and monetization and develop policies that prioritize privacy and security to build trust with consumers and encourage innovation by providing clear guidelines for data use.
- The federal government policies should promote interoperability to enable data sharing across different systems and consider the impact on SMBs.
- The government should promote collaboration and information sharing among federal agencies and industry partners to improve data policies and infrastructure.

R11 - Facilitate the Creation of Data-driven business ecosystems: The federal government should raise awareness about the *New Gold*, Data Monetization Strategies, Data Analytics for Insights, Trusted Data Marketplaces, Platform-based Business Ecosystems, Network effects, Digital Thread of Data in connected value chains, Data Regulations, and tools for Monitoring and Managing Data Marketplaces. Data-driven networks of interconnected businesses, technologies, and platforms can leverage synergies to enhance existing products and services, create new revenue streams and enable digital twins.

Justification

- Data-driven ecosystems can create new revenue streams and enhance existing products and services among Interconnected businesses, technologies, and platforms can leverage synergies in the value chain.
- Data analytics can provide insights that drive innovation, improve decision-making and enable data monetization strategies can lead to significant benefits and economic growth
- Trusted data marketplaces can promote data sharing and collaboration. Data-driven business ecosystems can lead to new revenue streams and enhanced products and services.
- Platform-based ecosystems can enable businesses to collaborate and innovate more effectively and scale rapidly through network effects can create a virtuous cycle of growth for businesses.
- Data regulations can provide a framework for businesses to manage and use data responsibly and use tools for monitoring and managing data marketplaces can ensure transparency and accountability

Implementation Considerations

- Develop educational programs for businesses and individuals. Raise awareness about data-driven business ecosystems among through public campaigns, conferences, and workshops.
- Provide funding and incentives for data-driven ecosystem and solutions PPPs with industry leaders, innovative startups and academic institutions
- Foster the development of platform-based ecosystems by providing incentives and resources to businesses.

- Encourage collaboration and innovation among businesses by promoting network effects. Provide tools and resources for monitoring and managing data marketplaces.

Potential Implementation Barriers

- Lack of awareness and understanding about data-driven business ecosystems.
- Difficulty in developing and implementing data monetization strategies
- Limited resources and expertise for implementing data monetization strategies and data analytics.
- Lack of national strategy to create platform-based ecosystems.
- Balancing the benefits of data-driven business ecosystems with data privacy and security concerns.

Federal Agencies Involved

- Department of Commerce (DOC)
- National Institute of Standards and Technology (NIST)
- National Science Foundation (NSF)
- Department of Energy (DOE)
- Department of Transportation (DOT)
- Department of Agriculture (DOA)
- Federal Trade Commission (FTC)

Examples: The DOC may raise awareness about data-driven business ecosystems, provide resources and train businesses. NIST may develop guidelines for best practices for the digital thread of data in connected value chains.

1. The Department of Energy (DOE) can promote the use of data analytics in the energy sector to optimize energy production and reduce costs.

2. The Department of Transportation (DOT) can leverage data from connected vehicles and infrastructure to improve traffic flow, reduce congestion, and increase safety.

3. The Department of Agriculture (USDA) can create data-driven initiatives to optimize agriculture production, reduce waste, and improve food security.

Federal Considerations

- Ensure fair competition and preventing monopolies. Balance data sharing with privacy and security. Develop guidelines and standards for data management and sharing
- Encouraging private sector to invest in data-driven economic growth. Promote collaboration between government, industry, and academia
- Balance the need for data privacy and security with the benefits and value of data-driven business ecosystems. Promote collaboration businesses while ensuring fair competition.
- Ensure transparency and visibility in data marketplaces by encouraging the use of data analytics to improve government operations and services.
- Addressing the digital divide and ensuring that all businesses have access to the resources and tools needed to participate in data-driven business ecosystems.

R12 – Evaluate Opportunities, Risks and Regulations on Using AI for Supply Chains: The federal government should evaluate the potential impact of AI in accelerating adoption of supply chain resilience, security, and traceability. It should also evaluate the risks of malicious actors using AI to tamper with supply chains, as well as

consequences, potential remedies and regulatory actions needed to prevent state nation attacks, especially in legacy infrastructure.

Justification

- AI-powered supply chain traceability can help improve the accuracy and efficiency of tracking products and components throughout the supply chain.
- It can help prevent counterfeiting and improve supply chain transparency, which is increasingly important for businesses and consumers alike.
- AI can help companies quickly detect and respond to supply chain disruptions, reducing the risk of costly delays or shortages.
- The use of AI by malicious actors to intrude the supply chain of critical infrastructure could have serious consequences, such as data breaches, system disruptions, or physical damage.
- The increasing use of AI in critical infrastructure makes it a potential target for attackers seeking to exploit vulnerabilities in AI systems.
- AI-powered attacks could be more sophisticated and harder to detect than traditional attacks, making them more difficult to defend against.

Implementation

- Promote how to leverage AI and IoT technologies to create end-to-end supply chain visibility and traceability.
- Encourage the use of AI algorithms for analyzing vast amounts of supply chain data to identify patterns and anomalies, making it easier to identify potential vulnerabilities or areas for improvement.
- Companies can use AI-powered predictive analytics to anticipate supply chain disruptions and take proactive measures to mitigate them.
- The government can work with industry stakeholders to develop AI-specific security standards and best practices for critical infrastructure.
- AI systems used in critical infrastructure should be subject to rigorous testing and evaluation to identify potential vulnerabilities and ensure they are secure.
- The government should provide funding and resources for research into AI security and develop tools to detect and respond to AI-powered attacks.

Barriers

- The rapid evolution of AI technology makes it difficult to keep pace with emerging threats and vulnerabilities.
- Lack of data quality: The accuracy and completeness of supply chain data can be a challenge, making it difficult for AI algorithms to provide reliable insights.
- Data privacy concerns: Sharing supply chain data with third-party AI vendors can raise concerns about data privacy and security.
- Technical expertise: Implementing AI-powered supply chain traceability requires significant technical expertise and resources and there are challenges associated with securing AI systems.
- The cost of implementing AI security measures could be significant, especially for smaller companies that may lack the resources to invest in advanced cybersecurity measures.

Federal commercial and civilian agencies involved

- Department of Commerce (DOC)

- National Institute of Standards and Technology (NIST)
- Federal Trade Commission (FTC)
- Department of Homeland Security (DHS)
- Federal Bureau of Investigation (FBI)
- Department of Defense (DOD)
- Food and Drug Administration (FDA)
- Federal Energy Regulatory Commission (FERC)
- Cybersecurity Infrastructure Security Agency (CISA)

Examples: The DOC may evaluate the use of AI in supply chains and consider new regulations about the use of AI, while NIST may raise awareness about good and bad uses of AI and develop guidelines for best practices.

1. The Food and Drug Administration can evaluate the use of AI in pharmaceutical supply chains and assess the impact on public health.

2. The Cybersecurity Infrastructure Security Agency can assess the cybersecurity risks of AI in supply chains and develop best practices for mitigation.

3. The Federal Energy Regulatory Commission can evaluate the impact of AI on energy supply chains and assess regulatory implications.

Federal considerations

- The government should evaluate the potential risks and benefits of AI-powered supply chain traceability and work with industry stakeholders to develop regulations and guidelines as needed.
- The government should ensure that any regulations or guidelines related to AI-powered supply chain traceability are consistent with existing data privacy and security laws.
- The government should work to promote international collaboration on AI-powered supply chain traceability to help establish global standards and best practices.
- The government should work with industry stakeholders to develop standards and best practices for securing AI systems used in critical infrastructure.
- The government should promote collaboration and information sharing among federal agencies and industry partners to improve AI security.