Sub Working Group Outline on
Augmented Logistics and Smart Supply Chains

Sub-Group Members
Robby Moss,
Tom Katsioulas
Steve Griffith
Mike Bergman
Ann Mehra

Sub Working Group Outline on
Augmented Supply Chain Logistics

Summary of Recommendations on Supply Chain Logistics

R01 - National IoT Strategy for adoption of IoT in supply chain logistics

R02 - Promote standards and protocols for IoT in supply chain logistics

R03 - Provide financial incentives to encourage adoption of IoT in supply chain logistics

R04 - Foster PPPs focused on adoption of IoT in supply chain logistics

R05 - Invest in workforce development focused on IoT in supply chain logistics

R06 - Strengthen cybersecurity measures focused on IoT in supply chain logistics

R07 - Promote international collaboration on adoption of IoT in supply chain logistics

R08 - Monitor and evaluate progress of adoption of IoT in supply chain logistics

R09 - Select mix of policies, incentives and requirements to support sustainable, scalable growth in domestic IoT manufacturing supply chain

National IoT Strategy for adoption of IoT in supply chain logistics

Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.

Justification

- Drive economic growth and competitiveness
- Provide guidance and support for businesses to adopt and integrate IoT solutions within supply chains
- Job creation and workforce development
- Help establish guidelines, standards and best practices for IoT security and data protection
- Provide guidelines and assurance that benefits are distributed equitably

Implementation

- Stakeholder engagement
- Focus on key areas where IoT can provide the greatest benefit
- Support innovation and research and development (R&D)

Barriers

- Interagency coordination
- Resistance to change
- Cybersecurity and data privacy concerns
- Legal and regulatory barriers
- Balancing innovation and regulation

Agencies

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

Federal considerations

- Aligning strategy with broader national priorities and policies
- Engaging with industry associations and international organizations
- Coordinating efforts and resources across federal agencies
- Address concerns and needs of all stakeholders

Promote standards and protocols for IoT in supply chain logistics

Promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across various IoT systems and devices.

Justification

- Interoperability
- Scalability
- Innovation and competition
- Cybersecurity and data privacy
- Simplified integration and maintenance
- Cost savings
- Regulatory compliance

Implementation

- Include diverse range of stakeholders – businesses, technology providers, academia, government agencies
- Prioritize critical areas – data exchange, device interoperability, security
- Build on existing standards

Barriers

- Resistance to standardization
- Fragmentation
- Cost and resource constraints
- Rapid technological advancements

Agencies

- NIST
- FTC
- Department of Commerce
- Federal Communications Commission (FCC)

Federal considerations

- Provide regulatory framework supporting standardization efforts
- Collaborate with international organizations and foreign governments
- Offer financial and technical support to businesses, particularly SMB to assist with adoption and compliance
- Monitor and evaluate effectiveness

Provide financial incentives to encourage adoption of IoT in supply chain logistics

Establish and provide financial incentives aims to encourage adoption of IoT technologies in supply chain operations by reducing initial investment costs and perceived risks associated with implementation of IoT solutions.

Justification

- Encourage investment
- Stimulate innovation
- Enhance competitiveness
- Create jobs and economic growth
- Promote sustainability

Implementation

- Identify appropriate incentives
- Define eligibility criteria
- Coordinate across federal agencies
- Monitor and evaluate
- Raise awareness and provide technical assistance

Barriers

- Budget constraints
- Political opposition
- Bureaucratic hurdles
- Inefficient allocation of resources
- Market distortion
- Difficulty measuring impact
- Lack of awareness

Agencies

- DOC
- DOT
- DOE
- Small Business Administration (SBA)
- National Science Foundation (NSF)
- Department of Agriculture (USDA)
- Environmental Protection Agency (EPA)
- Department of Defense (DoD)
- Department of Labor (DOL)

Federal considerations

- Targeting the right recipients
- Balancing public and private investment
- Providing assurance of fairness and transparency
- Encouraging innovation
- Collaboration with industry and academia

Foster PPPs focused on adoption of IoT in supply chain logistics

Establish and foster public-private partnerships (PPPs) focused on IoT adoption to facilitate collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia.

Justification

- Leveraging resources and expertise
- Risk sharing
- Accelerating technology adoption
- Addressing regulatory challenges
- Fostering innovation
- Enhancing global competitiveness
- Building trust and cooperation

Implementation

- Identify key stakeholders
- Establish collaborative framework
- Define clear goals and objectives
- Develop joint projects and initiatives
- Effective communication and coordination

Agencies

- DOC
- DOT
- DOE
- SBA

Barriers

- Misalignment between public and private sectors
- Differing priorities and objectives
- Intellectual property (IP) and data privacy concerns
- Limited resources

Federal considerations

- Address alignment and communication issues
- Align priorities and objectives
- Protect IP and data
- Allocate resources efficiently

Invest in workforce development focused on IoT in supply chain logistics

Invest in and promote education and workforce development focused on IoT to address growing demand for skilled professionals capable of designing, implementing, and managing IoT systems in supply chain operations.

Justification

- Addressing skills gap
- Enhancing competitiveness
- Fostering innovation
- Supporting digital transformation
- Encouraging job creation
- Promoting social inclusion
- Long-term sustainability

Implementation

- Identify skill requirements
- Develop targeted curricula
- Expand access to education and training
- Encourage industry-academia partnerships
- Focus on reskilling and upskilling
- Promote STEM education
- Establish performance metrics

Agencies

- Department of Education
- Department of Labor
- National Science Foundation
- Department of Commerce

Barriers

- Insufficient funding
- Resistance to change
- Difficulty in identifying skill requirements
- Skills mismatch

Federal considerations

- Allocate sufficient resources
- Foster collaboration between industry and academia
- Continuously evaluate performance and improve effectiveness of training and education

Strengthen cybersecurity measures focused on IoT in supply chain logistics

Strengthen cybersecurity measures focused on IoT across supply chain networks to address concerns around data privacy, security, and potential risks associated with increased connectivity and interdependence of IoT systems.

Justification

- Protecting sensitive data
- Providing assurance of operational
- Maintaining trust
- Compliance with regulations
- Enhancing competitiveness
- Addressing evolving threats
- Fostering innovation

Implementation

- Develop comprehensive cybersecurity framework for IoT in supply chain
- Promote adoption of best practices and standards
- Encourage information sharing
- Invest in security technologies
- Promote security-by-design principles
- Raise awareness and provide training

Barriers

- Limited resources
- Complexity of supply chains
- Resistance to information sharing
- Evolving threats

Agencies

- Department of Homeland Security (DHS)
- NIST
- DOC
- FTC

Federal considerations

- Support research and development
- Allocate resources to facilitate training and awareness
- Encourage collaboration among industry stakeholders and government agencies
- Monitor and update cybersecurity policies, regulations and best practices adapting to evolving threat landscape

Promote international collaboration on adoption of IoT in supply chain logistics

Promote international collaboration in IoT adoption across global supply chains to facilitate sharing knowledge, best practices, and resources between countries and regions, driving innovation and accelerating widespread adoption of IoT technologies in supply chain operations worldwide.

Justification

- Global nature of supply chains
- Harmonization of standards and regulations
- Addressing global cyber threats
- Leveraging global expertise
- Fostering innovation
- Building trust
- Addressing social and environmental challenges

Implementation

- Establish bilateral and multilateral agreements
- Participate in international forums and organizations
- Share information and best practices
- Collaborate on research and development
- Promote capacity building
- Identify key international partners
- Leveraging existing diplomatic channels
- Coordinate with relevant federal agencies

Agencies

- Department of State
- DOC
- DHS
- NIST
- FTC

Barriers

- Differing priorities and interests
- Trust and data privacy concerns
- Regulatory and legal barriers

Federal considerations

- Align collaboration efforts with national priorities
- Respect priorities of partner countries
- Develop clear objectives and mutually beneficial goals
- Effective communication and coordination among federal agencies and international partners
- Remain adaptable to evolving global landscape

Monitor and evaluate progress of adoption of IoT in supply chain logistics

Monitor and evaluate progress to provide assurance that IoT adoption efforts in supply chain logistics are on track, effectively addressing identified challenges and opportunities, and delivering desired outcomes.

Justification

- Assess effectiveness and measure impact
- Identify areas for improvement
- Allocate resources efficiently
- Enhance accountability
- Facilitate knowledge sharing
- Inform future strategies

Implementation

- Establish clear goals and objectives
- Develop relevant performance indicators
- Implement data collection and reporting mechanisms
- Conduct periodic assessments
- Culture of continuous improvement
- Collaborate with stakeholders and assign responsibility
- Develop a monitoring and evaluation plan
- Allocate resources

Agencies

- DOC
- DOT
- DHS
- NIST
- FTC

Barriers

- Potential for lack of clear goals and objectives
- Inadequate data collection and reporting mechanisms
- Resource constraints
- Resistance to change

Federal considerations

- Clear communication of goals, objectives, and expectations
- Collaborate with relevant stakeholders
- Be transparent in sharing results, fostering trust and accountability
- Be adaptable and responsive to new information and insights

Select mix of policies, incentives and requirements to support sustainable, scalable growth in domestic IoT manufacturing supply chain

The recommended policies, incentives and requirements are relevant to the transportation sector as it becomes increasingly connected, integrated, and ultimately autonomous. Rapid technological advances are further augmented by communication and IT, including IoT.

Justification

- Tighter domestic preference requirements could create supply constraints and prevent the manufacturers from meeting even modest deployment goals.
- May be difficult for U.S. manufacturing capacity to meet increased demand that would be sparked by anticipated federal investment/incentives.
- May be no domestic alternatives for components and subcomponents, limiting the ability of equipment providers to control domestic content.
- Burden related to federal domestic preference requirements will increase as subcomponents become smaller, more integrated.

Implementation

- Phase in domestic contact requirements.
- Accelerate domestic manufacturing with investment tax credit for capital costs.
- Provide clear rules on domestic content requirements.
- Avoid rules that require determining the country of origin of subcomponents.
- Component test should include all costs associated with the manufacturing of a product.
- Allow 100% of manufacture value added (MVA) or substantial transformation to be classified as domestic content in component tests.
- Designate countries outside US for allowed procurement of components.

Barriers

- Current Supply Chain constraints meeting domestic content requirements.
- Funding constraints: huge initial capital cost investment to build up new domestic manufacturing plants.
- Resource constraints: need to be an influx of skilled engineers, technicians to support domestic buildup.

Agencies

- DOC
- DOT
- NIST
- Federal Highway Administration (FHWA)
- National Highway Traffic Safety Administration (NHTSA)

Federal considerations

- Extended phase in period necessary to avoid supply shortages and provide domestic manufacturers and their suppliers with sufficient time to develop domestic manufacturing capabilities.
- For domestic content requirement, guidelines on how they apply across all funding and procurement programs.
- Provide guidance to implementing state agencies.

Sub Working Group Outline on
Smart Supply Chain Traceability

Summary of Recommendations on Supply Chain Traceability

R01 - Encourage Global Identifier Standards for Supply Chain Traceability

R02 - Promote Trusted Architectures for Provenance & Traceability

R03 - Incentivize IoT Systems Supply Chains to Adopt Trusted Traceability

R04 - Promote Creation of Traceable and Trusted IoT Network Ecosystems

R05 - Accelerate Evolution of Trusted Digital Threads Across Value Chains

R06 - Incentivize the Creation & Growth of Trusted Data Marketplaces

R07 - Subsidize Digitalization of Enterprises in the IoT Value Chain

R08 - Promote Creation and Orchestration of Trusted Value Chains

R09 - Subsidize Orchestrated Public-Private Partnerships Across Value Chains

R10 - Establish Data Policies that Stimulate Economic Growth

R11 - Facilitate Creation of Data-driven Business Ecosystems

R12 - Evaluate Opportunities, Risks of Using AI in Supply Chains

Encourage Global Identifier Standards for Supply Chain Traceability

R01

The Federal Government should encourage the use of Global Identifier Standards for supply chain traceability

Justification

- Improve security and supply chain transparency
- Reduce risk of counterfeit or tampered goods
- Increase public health, safety, security and privacy
- Promote environmental sustainability with greater visibility in product lifecycles
- Address market need for greater transparency and accountability, on origin and journey of products
- Enable creation of digital threads by tying workflow IDs to asset IDs

Implementation

- Incentivize suppliers to adopt global standards, such as GS1
- Encourage suppliers to use unique IDs for their corporation, products, parts, assets, etc.
- Provide resources and guidance to upgrade existing IT systems to support chain traceability IDs
- Facilitate adoption of IoT product IDs linked to cybersecurity labels

Agencies

- DOC
- NIST
- DHS
- CISA
- FDA
- SBA

Barriers

- Resistance from suppliers to invest in ID infrastructure
- Technical challenges for SMBs to implement methodologies for adopting identifier standards
- Need for collaboration among stakeholders in fragmented supply chains to cross-ref IDs
- Need for secure / interoperable databases for global ID handling

Federal considerations

- Collaborate with international allies on global ID standards in line with US trade policy goals.
- Harmonize global ID standards to facilitate interoperability.
- Ensure agencies' collaboration to incentivize use of Global IDs in their respective domains.
- Require the use of ID standards in all procurement contracts

Promote Trusted Architectures for Provenance & Traceability

R02

Promote development and use of trusted hardware/software architectures for supply chain provenance, traceability, chain of custody and lifecycle mgmt.

Justification

- Enhance supply chain security and mitigate risks relate to compromised components
- Increase trustworthiness of critical systems for security, safety, and economic stability.
- Increase consumer confidence, prevent supply chain attacks and data breaches
- Improve supply chain security, chain of custody and lifecycle management (SBOM-HBOM)

Implementation

- Educate stakeholders on the benefits of trusted architectures.
- Promote industry adoption of via education and outreach.
- Incentivize suppliers to develop systems with trusted parts
- Develop guidelines to speed adoption of industry standards
- Encourage collaboration PPPs

Agencies

- NIST
- DHS
- DOD
- DOC
- FTC
- CISA
- GSA

Barriers

- Lack of awareness of benefits of trusted architectures
- Resistance to invest or design due to implementation costs
- Technical challenges linking to legacy infrastructure.
- Complexities in deploying trusted architectures at scale.

Federal considerations

- Funding and budgets to incentivize industry suppliers
- Policies and regulations for use of trusted architectures.
- Coordinating efforts across Public-Private sectors
- Funding incentives to speed adoption and use at scale

Incentivize IoT Systems Supply Chains to Adopt Trusted Traceability

R03

Incentivize the Supply Chains to accelerate adoption of trusted traceability to ensuring security, integrity and trustworthiness of IoT devices and systems

Justification

- Improve confidentiality & integrity of IoT supply chain to prevent attacks, human/economic losses
- Accelerate IT/OT convergence, enhance efficiency in delivery of critical infrastructure services.
- Create a competitive advantage, foster innovation, enable SMBs and large companies to monetize
- Enable suppliers of IoT devices to become smart-connected-secure IoT suppliers and service providers
- Enable the creation of connected ecosystems for end-to-end monetization and IoT growth

Implementation

- Financial incentives to companies that market trusted products
- Require contractors and suppliers to follow traceability standards
- Establish a certification process for electronics products to meet trusted traceability standards
- Facilitate partnerships with industry associations develop guidelines and best practices

Agencies

- DHS
- DOD
- NIST
- FERC
- FCC
- DOE
- CISA
- EPA
- SBA

Barriers

- Lack of awareness on risks and trusted traceability benefits
- Lack of expertise and resources to develop traceability methods.
- Resistance due to complexity and cost of Confidentiality & Integrity
- Reluctance to invest due to IP protection and development cost

Federal considerations

- Develop financial incentives to offering traceable products/parts
- Promote methods for trusted traceability in line with executive orders and government priorities
- Require contractors & suppliers to follow traceability standards
- Promote orchestrated PPPs in to close value chain traceability gaps

Promote Creation of Traceable and Trusted IoT Network Ecosystems

R04

Promote traceable and trusted IoT network ecosystems made of devices, systems, networks, and personas operating in connected IoT environments

Justification

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

Implementation

- Drive awareness on how trust is established in IoT networks.
- Promote interoperability programs for networks to operate securely and reliably
- Encourage the development and adoption of secure, trusted and interoperable IoT solutions
- Work with industry, academia, promote innovation and R&D

Agencies

- DHS
- NIST
- FTC
- DOE
- FCC
- EPA
- SBA

Barriers

- Cost of upgrading legacy systems, and supply chain processes.
- Resistance to investing in trusted IoT network ecosystems
- Lack of awareness of importance of IoT security and trust.
- Limited interoperability between IoT devices and networks.
- Securing systems that were not designed with security in mind.

Federal considerations

- Develop guidelines for trusted IoT network ecosystems
- Provide financial incentives to encourage adoption.
- Promote processes that improve critical infrastructure resilience
- Invest in secure infrastructure among devices, networks, people
- Mandate secure solutions for federal agencies and key sectors

Accelerate Evolution of Trusted Digital Threads Across Value Chains

R05

Accelerate evolution of trusted digital threads across value chains by incentivizing companies to digitalize their workflows and link their data IDs to marketplaces

Justification

- Increase visibility of a product's lifecycle and reduce risk of cyber attacks, counterfeits, recalls.
- Improve efficiency, reduce costs, manage vulnerabilities, increase differentiation, and promote innovation & data monetization.
- Enable data marketplaces that create business opportunities and drive new revenue streams
- Speed adoption by linking digital threads (DBOM, HBOM, SBOM) to protect proprietary IP but enable value chains to monetize

Implementation

- Develop educational/training programs on digital threads
- Establish guidelines to create a digital thread data sharing.
- Incentivize companies to digitalize their workflows
- Promote collaboration PPPs for digital thread enabled apps
- Fund development of methods to ease digital thread evolution

Agencies

- NIST
- DOE
- DHS
- FDA
- EPA
- CISA
- DOE
- FTC
- SBA

Barriers

- Lack of education on how digital threads enable new business
- Resistance from businesses to adopt new digital solutions
- Hesitance to share data due to IP issues or competitive advantage.
- Varying requirements for digital threads, making it challenging to establish common standards

Federal considerations

- Promotion and guidelines to create trusted digital threads.
- Financial incentives to enable creation of digital threads
- Support processes to improve supply chain traceability.
- Promote PPPs that facilitate innovation and collaboration to create digital threads compliant to federal regulations/standards

Incentivize the Creation & Growth of Trusted Data Marketplaces

R06

Incentivize the creation of trusted data marketplaces where data producers and consumers share information about data enabling data exchange and monetization while protecting proprietary IP

Justification

- Regulate market access and use with better supply chain visibility
- Reduce costs of data sharing for producers and consumers
- Streamline supply chain processes to locate and license relevant data
- Reduce redundancies and simplify logistics in complex supply chains
- Increase data visibility and access in value chains to enable growth of marketplaces that will fuel the future digital economies

Implementation

- Develop guidelines & regulations for access and use of shared data
- Provide tax credits and subsidies to encourage participation
- Promote marketplace benefits to participants, suppliers, customers
- Drive data security-confidentiality metrics and monitor effectiveness
- Encourage use of analytics for better visibility, traceability, efficiency

Agencies

- DOC
- SBA
- DOA
- DHS
- EPA
- FDA
- NSF
- GSA
- NIST
- FTC

Barriers

- Lack of awareness on the value of the marketplace platforms
- Concerns and resistance over data security and confidentiality
- Challenge to regulate & monitor access, sharing and use of data
- Reluctance to share proprietary data without a license
- Lack of open and participatory platforms for data marketplaces

Federal considerations

- Implement regulations based on experience GDPR, CDPP, etc.
- Develop policies to prevent monopolies in the marketplace
- Provide education and resources to help SMBs join marketplaces
- Balance participation incentives with data security and privacy
- Align government efforts to drive open innovation platforms

Subsidize Digitalization of Enterprises in the IoT Value Chain

R07

Fund digitalization of key business functions of enterprises in the IoT value chain for better visibility and ability to track products, monitor use, fix defects, and offer services

Justification

- Improve management, efficiency and visibility in supply chains
- Increase security, reliability, and integrity of digital data
- Enable secure ecosystems, SMB opportunities, economic growth
- Accelerate creation of digital thread and IoT services growth
- Facilitate digital transformation over-the-air services & updates
- Enhance supply chain security, integrity of data which will the future digital economies.

Implementation

- Develop guidelines and criteria for eligibility for the subsidies
- Streamline application/approval process for business subsidies
- Ensure that the subsidies are accessible to all businesses
- Provide incentives for SMBs to invest in digitalization and tools
- Encourage collaboration and community knowledge sharing

Agencies

- DOC
- DOE
- DHS
- NIST
- CISA
- SBA

Barriers

- SMBs lack resources/expertise to implement digital technologies
- The cost of implementation may be a barrier for some businesses
- Resistance to change, or lack of technical expertise/resources.
- Concerns over the security and confidentiality of digital data may discourage some stakeholders

Federal considerations

- Ensure that subsidies that align with federal priorities and goals
- Coordinate with other federal agencies to avoid redundancy.
- Monitor and evaluate the impact of the subsidies on the economy
- Encourage equitable access to digital technologies and tools
- Prioritize digitalization efforts on security and confidentiality

Promote Creation and Orchestration of Trusted Value Chains

R08

Promote creation & orchestration of trusted value chains made of entities, manufacturers, service providers, that collaborate and drive trust and accountability

Justification

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

Implementation

- Provide incentives for businesses to adopt transparent practices.
- Orchestrate networks of entities to maintain trust through collaboration and accountability.
- Establish guidelines for creating & upkeeping trusted value chains.
- Provide incentives for businesses to collaborate and adopt best practices for transparency

Agencies

- NIST
- DOC
- DOE
- FTC
- DHS
- FDA
- SBA
- CISA

Barriers

- Competitiveness and lack of collaboration and accountability
- Resistance to change for adoption of transparent & open ecosystems
- Cost of implementing practices for trustworthy value chains.
- Difficulty in orchestrating and coordinating diverse stakeholders across fragmented supply chains

Federal considerations

- Ensure that incentives align with guidelines and standards
- Foster collaboration among agencies, industries and value chains to accelerate adoption
- Develop & monitor regulations and standards to keep up with new threats and technologies.
- Ensure that regulations are not burdensome for businesses

Subsidize Orchestrated Public-Private Partnerships Across Value Chains

R09

Subsidize orchestrated Public-Private Partnerships working in parallel to speed adoption of traceability with consistent workflow & hand-off methods

Justification

- Speed adoption of digital thread & complex supply chain traceability
- Digitalize supply chains rapidly via PPPs working piecemeal in parallel for slices of the supply chain
- Create resilient and secure supply chains can help businesses drive economic growth.
- Improve supply chain traceability to help businesses reduce risk and increase resilience, which can lead to business and economic growth.

Implementation

- Subsidize the orchestration of connected PPS across value chains.
- Promote consistent digitalization methods for "receivables-process-deliverables“ for digital threads
- Fund the development of digital infrastructure, training programs,
- Provide support necessary for successful PPP implementation.

Agencies

- DOC
- DOA
- EPA
- FDA
- DHS
- FTC
- FCC
- SBA

Barriers

- Resistance from supply chain stakeholders to change or share data or work with competitors.
- Cost and lack of expertise and digitalize the infrastructure.
- Costs related to implementing digitalization among enterprises
- Technical challenges related to integrating disparate systems and data formats.

Federal considerations

- Prioritize PPPs that promote transparency, efficiency, security.
- Ensure that partnerships do not unfairly disadvantage SMBs
- Address security & confidentiality concerns related to data sharing
- Consider the potential impact on domestic and international trade policies and subsidies

Establish Data Policies that Stimulate Economic Growth

R10

Establish data policies that drive economic growth via frameworks that facilitates Data Monetization Security, Privacy, Data Sharing, Ownership, Control, Licensing etc.

Justification

- Data policies can have a major impact on privacy, security, innovation, and monetization.
- Lack of data policies can create uncertainty and hinder the growth of digital economies.
- Monetization of data enables business growth and can fuel synergistic ecosystems
- Frameworks that facilitate data protection, sharing, licensing, and analytics can minimize risk and maximize economic value

Implementation

- Promote infrastructure for data security and privacy, sharing, ownership, analytics and control
- Establish policies related to data that ensure compliance with regulatory requirements.
- Evolve policies in consultation with industry, academia, and government agencies and keep up-to-date with changing tech

Agencies

- DOC
- FTC
- NIST
- DOJ
- DHS

Barriers

- Lack of knowledge about data policies and resistance to change
- Lack of clarity on how data policies on confidentiality and security will impact stakeholders
- Lack of data policy can hinder growth of digital economies.
- Cost of establishing infrastructure for data security, control, etc.

Federal considerations

- Consider potential impact of data policies and provide guidelines for data use and monetization.
- Promote interoperability for data sharing across different systems
- Encourage collaboration and info sharing among agencies and industry to improve data policies
- Promote collaboration and info sharing among agencies & industry

Facilitate Creation of Data-driven Business Ecosystems

R11

Facilitate the Creation of Data-driven business ecosystems by raising awareness about the *New Gold*, trusted data marketplaces, monetization strategies, platforms that maximize network effects

Justification

- Data-driven ecosystems enable new and scalable revenue streams
- Connected businesses, products and services fuel economic growth
- Data analytics provide insights to improve services and monetization
- Trusted data marketplaces promote data sharing and collaboration
- Platform-based ecosystems enable businesses to collaborate, innovate and scale with network effects
- Data regulations can ensure that businesses and marketplaces drive transparency and accountability

Implementation

- Develop educational programs for businesses and individuals.
- Raise awareness via campaigns, conferences, and workshops
- Fund incentives for data-driven ecosystems and solutions PPPs
- Foster development of platform-based business ecosystems
- Encourage collaboration and innovation via network effects

Agencies

- DOC
- NIST
- NSF
- DOE
- DOT
- DOA
- FTC

Barriers

- Lack of awareness about data-driven business ecosystems.
- Difficulty in developing data monetization strategies
- Limited resources and expertise to develop data analytics.
- Lack of national strategy to create business ecosystems
- Balancing benefits of business ecosystems with data privacy

Federal considerations

- Ensure ecosystem participation while preventing monopolies
- Develop guidelines for data management and sharing
- Encourage private sector to invest for economic growth
- Balance data trust with security and value of business ecosystems
- Ensure transparency and visibility in data marketplaces.

Evaluate Opportunities, Risks of Using AI in Supply Chains

R12

Evaluate opportunities, risks and regulations for using AI to accelerate supply chain security and resilience, or prevent bad actors from tampering

Justification

- AI-powered traceability can vastly improve supply chain security and resilience.
- AI can increase transparency and prevent counterfeits
- AI can detect supply chain disruptions and reduce risk
- AI used by bad actors in the supply chain can cause major disruptions and harm
- AI-powered attacks are more sophisticated and harder to detect than classic attacks. AI can target critical infrastructure

Implementation

- Promote AI with IoT for end-to-end supply chain traceability.
- Encourage use of AI to analyze supply chain data to create value.
- Promote predictive analytics to anticipate & handle disruptions,
- Provide funding to research AI security and build tools to detect & respond to AI-powered attacks.

Agencies

- DOC
- NIST
- FTC
- DHS
- FBI
- DOD
- FERC
- CISA
- FDA

Barriers

- Lack of data quality makes it hard for AI to provide reliable insights.
- Rapid evolution of AI makes it hard to keep pace with emerging threats and vulnerabilities
- Sharing supply chain data with third-party AI impacts privacy, security and attack surface.
- Technical challenges on securing trust of data used in AI systems

Federal considerations

- Evaluate the risks and benefits of AI-powered supply chains
- Work with industry stakeholders to develop guidelines needed.
- Ensure that guidelines on AI-powered supply chain are in line with data privacy & security laws.
- Promote global collaboration on AI-powered solution and develop best practices using AI systems