



# Work-in-Progress Draft Report of the Internet of Things (IoT) Advisory Board (IoTAB)

August 18, 2023 **Updated** Pre-Read Draft

## **IoT Advisory Board Members**

Benson M. Chan (IoT Advisory Board Chair), Chief Operating Officer, Strategy of Things Inc.

Daniel W. Caprio Jr. (IoT Advisory Board Vice Chair), Co-founder and Chair, The Providence Group

Michael J. Bergman, Vice President, Technology and Standards, Consumer Technology Association

Ranveer Chandra, Managing Director of Research for Industry and Chief Technology Officer of Agri-Food, Microsoft

Nicholas Emanuel, Head of Product U.S., CropX

Steven E. Griffith, Senior Industry Director, National Electrical Manufacturers Association

Tom Katsioulas, Chair, Global Semiconductor Alliance

Kevin T. Kornegay, Professor and IoT Security Endowed Chair, Morgan State University

Debra Lam, Managing Director of Smart Cities and Inclusive Innovation, Georgia Institute of Technology

Ann Mehra

Robby Moss, President and Principal Consultant, TGL Enterprises LLC

Nicole Raimundo, Chief Information Officer, Town of Cary, North Carolina

Maria Rerecich, Senior Director of Product Testing, Consumer Reports

Debbie A. Reynolds, Founder, Chief Executive Officer and Chief Data Privacy Officer, Debbie Reynolds Consulting

Arman Shehabi, Staff Scientist, Lawrence Berkeley National Laboratory

Peter Tseronis, Founder and Chief Executive Officer, Dots and Bridges LLC

## Contents

<b>IoT Advisory Board Members</b> .....	2
1. Executive Summary .....	5
2. Introduction .....	5
3. Background.....	5
3.1. Charter and Scope.....	6
4. Summary of Recommendations of the Advisory Board .....	7
5. Methodology .....	22
5.1. Approach .....	22
5.2. Description of IoT in the Context of this Report.....	22
6. Commentary and Discussion Topics Related to IoT Adoption .....	23
6.1. IoT Technology .....	23
6.2. Artificial Intelligence (AI) Considerations .....	23
6.3. Consumers (appliances, TVs, wearables, etc.) .....	23
6.4. Smart Homes (HVAC, security, lighting, etc.).....	23
6.5. Regulations.....	23
6.6. Standards .....	23
6.7. IoT Personas .....	23
7. Cross Market and Development Topic Areas .....	27
7.1.1. Overview.....	27
7.1.2. Opportunities and benefits of solving challenges for each theme (for personas) ..	27
7.1.3. Barriers to those opportunities (faced by personas) .....	27
8. Topic-specific Findings of the Advisory Board .....	28
8.1. Smart traffic and transit technologies .....	28
8.2. Augmented logistics and supply chains.....	29
8.3. Sustainable and critical infrastructure .....	29
8.4. Precision agriculture .....	29
8.5. Environmental monitoring .....	29
8.6. Public safety .....	29
8.7. Healthcare .....	29
9. Recommendations .....	30
Key Recommendation 1.0: National Data Protection Framework .....	32
Key Recommendation 2.0: Standardize IoT Implementation .....	37

Key Recommendation 3.0: IoT Cybersecurity (including Critical Infrastructure).....	43
Key Recommendation 4.0: IoT Connectivity Improvement and Expansion.....	51
Key Recommendation 5.0: Address Privacy Considerations for IoT.....	55
Key Recommendation 6.0: Sustainable Infrastructure.....	57
Key Recommendation 7.0: Workforce.....	65
Key Recommendation 8.0: Smart Traffic and Transit.....	71
Key Recommendation 9.0: Augmented Logistics and Supply Chains.....	73
Key Recommendation 10.0: Precision Agriculture.....	111
Key Recommendation 11.0: Environmental Monitoring.....	115
Key Recommendation 12.0: Public Safety.....	117
Key Recommendation 13.0: Health Care.....	118
Key Recommendation 14.0: International Considerations.....	119
10. Conclusion.....	120
11. References.....	121
12. Acknowledgements.....	121
13. Appendices.....	121
14. Compliance Matrix.....	122

## 1. Executive Summary

[this will be drafted after other sections are complete]

## 2. Introduction

[this will be a greeting and introduction from the IoT Chair and Vice-Chair]

## 3. Background

In January 2020, the Congress enacted the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law No. 116-283). Section 9204(b)(5) of this act established the Internet of Things Advisory Board (IoTAB) within the Department of Commerce. In accordance with the Federal Advisory Act, as amended, 5 U.S.C., App., the IoT Advisory Board (IoTAB) was chartered in December 2021.

The IoTAB is [chartered](#) to provide advice to the Internet of Things Federal Working Group (IoTFWG). In support of the working group charter to develop a report to congress, the IoTAB will assist with:

- the identification of any Federal regulations, statutes, grant practices, programs, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development of the Internet of Things;
- situations in which the use of the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States, including benefits from or to—
  - smart traffic and transit technologies;
  - augmented logistics and supply chains;
  - sustainable infrastructure;
  - precision agriculture;
  - environmental monitoring;
  - public safety; and
  - health care;
- whether adequate spectrum is available to support the growing Internet of Things and what legal or regulatory barriers may exist to providing any spectrum needed in the future;
- policies, programs, or multi-stakeholder activities that—
  - promote or are related to the privacy of individuals who use or are affected by the Internet of Things;
  - may enhance the security of the Internet of Things, including the security of critical infrastructure;
  - may protect users of the Internet of Things; and
  - may encourage coordination among Federal agencies with jurisdiction over the Internet of Things;

- the opportunities and challenges associated with the use of Internet of Things technology by small businesses; and
- any international proceeding, international negotiation, or other international matter affecting the Internet of Things to which the United States is or should be a party.
- The IoTAB shall submit to the IoTFWG a report that includes any findings and recommendations. The IoTFWG will be providing that report in its entirety to Congress.

The membership of the IoTAB consists of sixteen members and a chairperson (listed on the internal cover). The Secretary of Commerce appointed all members of the IoTAB and the Board has met on a regular schedule as necessary to complete the report .

[Additional text will share the objectives of the report, and what the Board foresees as the outcome after the conclusion of its efforts. (Mention that this report is intended to highlight ways that IoT can be expanded and strengthened in ways that will bring economic prosperity and other benefits to the Nation and the World with a focus on increasing competitiveness, economic prosperity, and national security. Also highlight topics for the federal working group including ongoing efforts).]

### 3.1. Charter and Scope

Federal Advisory Committee Act (FACA) description, charter and scope

Scope and objectives of this report, and what the Board foresees as the outcome after the conclusion of its efforts. (Mention that this report is intended to highlight ways that IoT can be expanded and strengthened in ways that will bring economic prosperity and other benefits to the Nation and the World with a focus on increasing competitiveness, economic prosperity, and national security. Also highlight topics for the federal working group and highlight ongoing efforts)].

Note: Not sure this and the background info are needed

#### 4. Summary of Recommendations of the Advisory Board

After the recommendations are compiled, this will be a text-based summary, at a high-level, of what the Board recommends.

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
<b>National Data Protection Framework</b>				
Key Recommendation 1.0	The U.S. should establish a framework or model by which data related to the Internet of Things may be protected and used to benefit all. The model would consider a schema for describing IoT-related data and methods for both use and protection.	--	Policy/Guidance R&D	
Supporting recommendation 1.1	The federal government should facilitate/support the development of a National Data/Privacy Framework that clearly delineates the different aspects of data (i.e., machine versus personal) and how they should or shouldn't be utilized in smart transportation technologies.	STT-R01	Policy/Guidance R&D	
Supporting recommendation 1.2	The government should develop an IoT Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices.	PRV-R03	Policy/Guidance R&D	
Supporting Recommendation 1.3	Conformance to any specific set of requirements should be voluntary. Adjusted from: Keep IoT Product Certification Programs Voluntary. Conformance to any specific set of requirements should be voluntary.	CYB-R02	Tech Transfer Outreach/Engagement Policy/Guidance	
Supporting recommendation 1.4	(Under review) The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations.	Status?	Policy/Guidance	
Supporting Recommendation 1.5	Federal agencies can establish templates for clear and robust policies regarding data sharing and data usage involving third parties in the IoT ecosystem. Where practical, agencies can help to foster voluntary, industry-led adoption of such policies to enhance transparency leading to improved user trust in IoT devices and services.	PRV-R02	Policy/Guidance R&D	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting recommendation 1.6	The government can encourage and foster data policies that drive economic growth, such as through this framework.	This may overlap with SSC-R19	Outreach/Engagement Policy/Guidance	
<b>Standardization / Interoperability</b>				
Key Recommendation 2.0	The Federal Government should establish methods to foster interoperability for IoT technology, including through the use of consistent models, protocols, and schemas.	--	R&D	
Supporting Recommendation 2.1	The government should 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.	SSC-R02	Outreach/Engagement Policy/Guidance	
Supporting Recommendation 2.2	Agencies can support research and industry-led standards in areas such as telematics and sensor technologies for autonomous vehicles. These standards should be based on high-level safety guidelines (perhaps as determined by the National Highway Traffic Safety Administration or another federal organization).	STT-R02	Outreach/Engagement Policy/Guidance	
Supporting Recommendation 2.3	The federal government should promote and adopt industry led standards for minimum baseline interoperability and cybersecurity requirements for smart transportation technologies and corresponding transportation infrastructure (i.e., sensors in roads, cameras at intersections).	STT-R04	R&D Coordination	
Supporting Recommendation 2.4	The federal government can facilitate and support the adoption of smart city and sustainable infrastructure standards. Issues: This recommendation has some overlap with SUS-R05	SUS-R07	Outreach/Engagement Policy/Guidance	
Supporting Recommendation 2.5	The federal government should promote the development and adoption of existing industry standards activities with respect to energy efficient, clean, and renewable energy technologies that are used in sustainable infrastructure.	Updated SUS-R13	Outreach/Engagement Policy/Guidance	



Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting Recommendation 2.6	<p>Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT.</p> <p>May Issues: The recommendation needs clarity on the scope of devices to be addressed. More broadly every Board recommendation may need clauses to clarify included and excluded scope; this is a topic for the chairs to address.</p>	PSF-R01	Outreach/Engagement Policy/Guidance	
Supporting Recommendation 2.7	<p>(Under Review) Agencies can promote and, if necessary, develop a protocol for data exchange standards for IoMT (Internet of Medical Things) for interoperability, and promote the adoption of these standards. Solutions might include protection for medical data in mobile apps and IoT devices that is similar to the current Health Insurance Portability and Accountability (HIPAA) Act provisions.</p> <p>Issues: Recommendation should focus on data interoperability as a goal, rather than data exchange standards as the means to that goal</p> <p>This was discussed in May but <b>not included herein</b>: HCR-R03 Enact HIPAA-like protection for users' medical data in mobile applications and IoT devices. Consider medical data as a category for defined data protections. Issues: Need to clarify the scope of applicability and examine the potential for unintended consequences.</p>	HCR-R02	R&D Coordination Policy/Guidance	
<b>Cybersecurity</b>				
Key Recommendation 3.0	<p>The Federal Government should provide specific and consistent guidance for providers and adopters to ensure secure operations. While not the exclusive source of cybersecurity guidance, federal entities should continue to support NIST as a developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.</p>	--	Outreach/Engagement Policy/Guidance	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting Recommendation 3.1	The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.	CYB-R05	Policy/Guidance Coordination Funding?	
Supporting Recommendation 3.2	The government should 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.	SSC-R06	Outreach/Engagement Policy/Guidance	
Supporting Recommendation 3.3	The government should prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices.	CYB-R01	Policy/Guidance Coordination Outreach/Engagement	
Supporting Recommendation 3.4	The federal government should continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.	CYB-R03	Policy/Guidance Coordination	
Supporting Recommendation 3.5	The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.	CYB-R04	Policy/Guidance Coordination	
Supporting Recommendation 3.6	<b>(Under Review)</b> The Federal Government should update Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience requiring a sector-specific Internet of Things (IoT) data strategy. <b>From May: Issues: More information is needed to resolve the relationship of sustainable infrastructure to critical infrastructure and smart cities.</b>	SUS-R09	Policy/Guidance Coordination	
Supporting Recommendation 3.7	<b>(Under Review?)</b> The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.	SUS-R10	Policy/Guidance Coordination	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
	Note: As SRMAs are associated with critical infrastructure sectors, the resolution of questions around the relationship of sustainable infrastructure to critical infrastructure is needed to resolve how this recommendation applies.			
Supporting Recommendation 3.8	(Proposed / Updated) The federal government should facilitate/promote and support the development of an overarching guideline framework developed in a multi-stakeholder process that more clearly distinguishes the major sectors of the IoT for use when dealing with concerns such as cybersecurity. This framework could include definitions for the major sectors of the IoT under which relevant overarching guidelines would apply.	NEW CYB-R06		
<b>Connectivity</b>				
Key Recommendation 4.0	The federal government should expand and improve programs that ensure reliable and sufficient connectivity among and between IoT devices in all areas of the country. The government should further promote accelerated innovation to ensure improved communications by ensuring the availability of suitable and sufficient spectrum resources, the development of wide-area networking technologies, and enhancing interoperability.	--	Policy/Guidance Coordination Outreach/Engagement Grants/funding	
Supporting Recommendation 4.x	(Proposed) To promote continued U.S. leadership on spectrum policy, the government should continue to free up spectrum for licensed and unlicensed use via spectrum sharing and repurposing underutilized federal spectrum.	NEW	Policy/Guidance Coordination Outreach/Engagement	
Supporting recommendation 4.1	The federal government should consider increasing funding and accelerating implementation of broadband deployment across rural America. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 3.	PRA-R03	Grants/funding	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting recommendation 4.2	<p>The federal government should actively promote and support the adoption of satellite narrowband IoT systems for agricultural IoT, with the aim of improving connectivity, data collection, and decision-making in rural and remote agricultural areas.</p> <p>Issues: Government doesn't usually play a role in harmonizing standards; possibly should be broader than satellite communications;</p> <p>Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 4.</p>	PRA-R04	Coordination Outreach/Engagement Grants/funding	
<b>Privacy</b>				
Key Recommendation 5.0	<p>The Federal Government should address privacy specific considerations for IoT. The successful adoption of IoT technology depends heavily on gaining the trust and confidence of the organizations, agencies, consumers, and others that will implement and expand its use.</p>	--	Coordination Outreach/Engagement	
Supporting recommendation 5.1	<p>Develop and implement a privacy transparency system for IoT devices, using the "U.S. Cyber Trust Mark" for business, government, and consumer data for Connected Devices and other transparency programs as a guide.</p>	PRV-R05	Coordination Outreach/Engagement Policy/Guidance	
Supporting recommendation 5.2	<p>Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.</p>	PRV-R07	Coordination Outreach/Engagement Policy/Guidance	
Supporting recommendation 5.3	<p>Use Plain Language in IoT Privacy Policies as part of the Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020.</p>	PRV-R01	Coordination Outreach/Engagement Policy/Guidance	
<b>Sustainable Infrastructure</b>				

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Key Recommendation 6.0	The Federal Government should lead in the adoption and integration of sustainable infrastructure and emerging technologies into the US economy and infrastructure.	--	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 6.1	The federal government should specify and utilize energy efficient and sustainable technologies into infrastructure and other projects that are funded in full, or partially, with federal funding. <b>Issues: May need to be reconciled or combined with 10.4.</b>	SUS-R12	Coordination Outreach/Engagement Policy/Guidance Funding?	
Supporting Recommendation 6.2	The federal government should consider new models for sustaining and support in considering project feasibility.	SUS-R03	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 6.3	The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.	<b>Updated</b> SUS-R08	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 6.4	The Federal Government should establish a national Emerging Technologies Program Office within the Executive office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage emerging technology initiatives across the United States.	<b>Updated</b> SUS-R11	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 6.5	The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).	SUS-R01 <b>Status?</b>	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 6.6	The federal government should consider the specification and utilization of IoT and “smart” technologies into infrastructure	SUS-R02	Coordination Outreach/Engagement Policy/Guidance	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
	and other projects that are funded in full, or partially, with federal funding. <b>Issues: May need to be reconciled or combined with 6.1.</b>		Funding	
Supporting Recommendation 6.7	The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility. <b>Maybe missing: SUS-R06: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.</b>	SUS-R03	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting Recommendation 6.8	The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models. <b>Issues: This recommendation has some overlap with Recommendation 2.4.</b>	SUS-R05	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting recommendation 6.9	The federal government should promote development and adoption procedures that accelerate and streamline planning, permitting, and interconnection aspects related to energy efficient technologies.	<b>Updated</b> SUS-R15	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting recommendation 6.10	Accelerate the promotion and adoption of procedures and methods to make the electric grid more reliable and resilient.	<b>Updated</b> SUS-R16	Coordination Outreach/Engagement Policy/Guidance Funding	
<b>Workforce / Education</b>				
Key Recommendation 7.0	The federal government should invest in and promote education and workforce. Workforce and education are broad topics. Specialized training programs could start as early as high school and include cybersecurity topics. Inclusion of yearly certifications is encouraged.	--	Coordination Outreach/Engagement Policy/Guidance Workforce Funding	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting Recommendation 7.1	The federal government should consider “student loan forgiveness” programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies.	SUS-R04	Coordination Policy/Guidance Workforce Funding	
Supporting Recommendation 7.2	<b>(Updated)</b> The federal government promote Continuing Education, Professional Development, and Vocational Training for IoT Integration in Supply Chain Management.	SSC-R05	Coordination Policy/Guidance Workforce Funding	
Supporting recommendation 7.3	<b>(proposed)</b> The federal government should invest and promote education and workforce development in smart transportation technologies.	STT-R05	Coordination Policy/Guidance Workforce Funding	
Supporting recommendation 7.4	Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.	PRV-R06	Coordination Policy/Guidance Workforce	
Supporting recommendation 7.5	The federal government should develop and facilitate programs and grants to reskill existing workers, train future workers across manufacturing, construction, and clean technology / renewable industries.	<b>Updated</b> SUS-R14	R&D Coordination Policy/Guidance Workforce	
<b>Smart Traffic / Transit</b>				
Key Recommendation 8.0	[Smart Traffic/Transit recommendation text is still being developed.]	--		
Supporting Recommendation 8.1	The federal government should consider developing programs and grants to allow underserved and less developed communities as well as rural areas to adopt smart transportation technologies.	STT-R03	Coordination R&D Outreach/Engagement Policy/Guidance Funding	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting Recommendation 8.2	The Federal Government should provide overarching regulatory guidance for the drone industry. The Federal Government should also provide funding for the drone industry for additional research in order that existing technical obstacles can be overcome.	STT-R06	Coordination R&D Outreach/Engagement Policy/Guidance Funding	
<b>Augmented Logistics and Supply Chains</b>				
Key Recommendation 9.0	[Full recommendation for supply chain still being developed.]	--		
Supporting Recommendation 9.1	Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.	SSC-R01	Coordination R&D Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.2	Establish and provide financial incentives to encourage businesses to adopt IoT technologies in their supply chain operations by reducing the initial investment costs and perceived risks associated with the implementation of IoT solutions.	SSC-R03	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting Recommendation 9.3	Federal entities can also help 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.	SSC-R04	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting Recommendation 9.4	Promote international collaboration in IoT adoption across global supply chains to share knowledge, best practices, and resources between countries & regions, driving innovation & accelerating widespread adoption of IoT technologies in supply chain operations worldwide.	SSC-R07	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.5	The government should provide an intentional process to monitor and evaluate progress to provide assurance that IoT adoption efforts in supply chain logistics are on track,	SSC-R08	Coordination Outreach/Engagement Policy/Guidance	



Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
	effectively addressing identified challenges and opportunities, and delivering desired outcomes.			
Supporting Recommendation 9.6	The federal government should select the most appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic IoT manufacturing supply chain.	SSC-R09	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.7	The government should promote the development and use of standards for supply chain logistics, traceability, and assurance.	Traceability R01	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.8	Agencies should support creation of cryptographically strong architectures and infrastructure that enable supply provenance, traceability, and lifecycle management by linking HBOM, SBOM to the design & manufacturing processes and data into a foundation of trust enabling IoT services.	Traceability R02	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.9	The government should establish incentives for industries to adopt capabilities for tracing design, manufacturing, and supply chain workflows that cryptographically link parts, personas, and data to deliver traceable products and IoT systems that function as originally intended.	Traceability R03	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting Recommendation 9.10	As foundations of trust evolve and IoT devices are deployed, get connected to networks, and used in the field, the government should promote traceable and interoperable IoT ecosystems across value chains amongst devices, personas, and infrastructure.	Traceability R04	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.11	Promote the use of digital threads among enterprises in disaggregated supply chains, to enable the creation of connected IoT value chains. Leverage digital threads of data across value chains to enable marketplaces of trusted data producers and data consumers.	Traceability R05	Coordination Outreach/Engagement Policy/Guidance	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
Supporting Recommendation 9.12	As digital threads and data platforms emerge, the government should incentivize the enablement and use of data marketplaces to increase visibility and economic growth with data enabled services while protecting proprietary IP and PII of stakeholders.	Traceability R06	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting Recommendation 9.13	The government should encourage Private-Public partnerships to finance a unified infrastructure for the digitalization of enterprise business processes including design, production, procurement, distribution, etc. to accelerate adoption of digital threads.	Traceability R07	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting Recommendation 9.14	To speed up the creation of connected value chains the government should promote PPPs that facilitate the adoption of end-to-end digital threads using consistent digitalization methods capturing receivables, processes, and certified deliverables.	Traceability R08	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.15	As digital threads drive growth of data among marketplaces, policies will be needed regarding data privacy, confidentiality, ownership, control, management, access, licensing, and trust for data use in applications, to minimize security risks and maximize economic value.	Traceability R09	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.16	As data produced in supply chains and during field use becomes the “new gold”, the government should raise awareness about the value of data marketplaces and incentivize the creation business ecosystems and data-driven networks of products, businesses, and value chains.	Traceability R10	Coordination Outreach/Engagement Policy/Guidance	
Supporting Recommendation 9.17	Considering the rapid growth of AI, the federal government should assess the supply chain risks of intrusions and attacks as well as opportunities to speed up adoption, as AI will have profound impact risk management, security, resilience, and economic growth.	Traceability R11	Coordination Outreach/Engagement Policy/Guidance	

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
<b>Precision Agriculture</b>				
Supporting Recommendation 10.0	<p>Develop a comprehensive national strategy for agricultural IoT to establish a clear vision and roadmap for the integration of IoT in agriculture, addressing current challenges, fostering innovation, and promoting long-term sustainability and competitiveness of the agricultural sector.</p> <p>Issues: This recommendation needs refinement. While it is too generic, it could perhaps be combined with similar recommendations from other subgroups;</p> <p>Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 6.</p>	PRA-R06	Coordination R&D Outreach/Engagement Policy/Guidance	
Supplemental Recommendation 10.1	<p>The federal government should consider subsidizing the use of IoT in farms.</p> <p>Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 1.</p>	PRA-R01	Coordination Outreach/Engagement Policy/Guidance Funding	
Supplemental Recommendation 10.2	<p>The federal government should consider fully funding the deployment of a “farm of the future” setup in every land grant university nationwide. This nationwide test-farm IoT network should span different forms of agriculture, including, but not limited to broadacre, horticulture, livestock, and aquaculture.</p> <p>Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 2.</p>	PRA-R02	Coordination Outreach/Engagement Policy/Guidance Funding	
Supporting recommendation 10.3	<p>The federal government should actively promote and support the adoption of Generative AI applications for agricultural IoT, with the aim of improving decision-making, optimizing resource utilization, and enhancing productivity in the agricultural sector through innovative and data-driven solutions.</p> <p>Issues: Concerns regarding privacy, maturity of the AI technology; premature for government to “promote” use of this technology</p>	PRA-R05	Coordination Outreach/Engagement Policy/Guidance	

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
	Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 5.			
<b>Environmental Monitoring</b>				
Key Recommendation 11.0	[Key recommendation text for environmental monitoring is still being developed.]	--		
Supplemental Recommendation 11.1	The federal government should establish or encourage IoT environmental data repositories in support of open, available data. Promoting the open availability of data would promote research, improve transparency, and encourage proactive improvement by industry participants.	ENV-R02	Coordination R&D Outreach/Engagement Policy/Guidance	
Supplemental Recommendation 11.2	The federal government should facilitate and support the research, development and deployment of low-cost air quality sensors. (Could we expand to additional types of monitoring?)	ENV-R01	Coordination R&D Outreach/Engagement Policy/Guidance	
<b>Public Safety</b>				
Key Recommendation 12.0	[Recommendation text for public safety is still being developed.]	--		
Supporting Recommendation 12.1	The federal government should create a stockpile of public safety IoT devices that is available for immediate access.	PSF-R02	Coordination R&D Outreach/Engagement Policy/Guidance	
<b>Health Care</b>				
Key Recommendation 13.0	[Recommendation text for health care is still being developed.]	--		
Supporting Recommendation 13.1	(Under Review) Raise Priority for IoMT to Healthcare Facilities' Executive Leadership Teams	HCR-R01	Coordination R&D Outreach/Engagement	

Working Draft IoT AB report

Recommendation #	Recommendation Description	Subteam #s	Legends	Personas (Future)
	May Issue: More research needs to be done on how establishing a Federal Chief IoT Officer would transfer to the desired outcome in healthcare organizations. Note: I think IoT officer references have been removed.		Policy/Guidance	
<b>International</b>				
Supporting Recommendation 14.1	(Proposed) The IoTAB strongly supports the voluntary public/private partnership that created the US Cyber Trust Mark.	NEW	Outreach/Engagement Coordination Policy / Guidance	
Supporting Recommendation 14.2	(Proposed) The government should create an international data minimization framework related to IoT devices, aligning with the NIST Privacy Framework principles.	NEW	Outreach/Engagement Coordination Policy/Guidance	

## 5. Methodology

### 5.1. Approach

Describe the approach taken – the regular meetings, sub-group approach, draft recommendations collected and discussed in the teams, the presentation to the Board for formal consideration and approval, integration into the report.

### 5.2. Description of IoT in the Context of this Report

Since there has been a great deal of discussion about defining IoT, we will simply describe what constitutes IoT for the purposes of this report and the recommendations. Observations and Commentary for Related Topics and Technology

## 6. Commentary and Discussion Topics Related to IoT Adoption

### 6.1. IoT Technology

#### **What is the current state**

- Discussion of free open-source designs (goes to ease of implementation, but “wild wild west” of cyber, Intellectual Property, etc.)
- Discussion of microcontrollers and microprocessors (goes to complexity, supply chain, etc.)
- Discussion of connectivity (Wi-Fi, BT, 5G, LoRa, Matter, etc.)
- Discussion of applications

#### **What is the future state**

- Examine the use of current and emerging technologies (inclusive of Artificial Intelligence and the way data could be aggregated and combined from different technologies)
- Identify as a Board what areas might also constitute a future state and how we might get there using possibly scenarios involving personas
- How we look at future proofing the Report, so that it's use extends beyond its initial release

### 6.2. Artificial Intelligence (AI) Considerations

### 6.3. Consumers (appliances, TVs, wearables, etc.)

### 6.4. Smart Homes (HVAC, security, lighting, etc.)

### 6.5. Regulations

### 6.6. Standards

### 6.7. IoT Personas

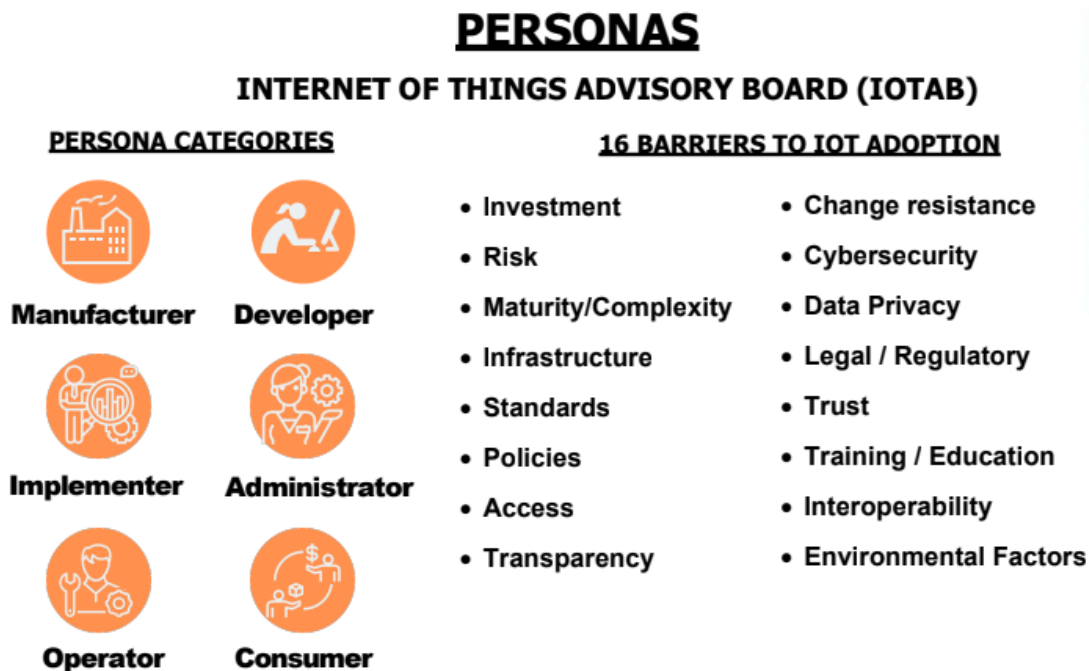
Brief background about the personas and their value in ensuring that the relevant and appropriate stakeholder groups are considered and, where applicable, included in the recommendations.

- End users (consumers, enterprise, government, etc.)
  - Brief description of what this persona is, their “involvement” with IoT
- Implementers (integrators, installers, etc.)
- Channel (resellers, distributors, retailers, etc.)
- OEMs (those who incorporate IoT into their products)
- Technology/solutions developers (technology, apps developers, telecommunications companies)

### Persona Categories

- **Manufacturer**
- **Developer**
- **Implementer**
- **Administrator**
- **Operator**
- **Consumer**

(Some slides are included in this initial version to illustrate content to be expanded on)





### IoTAB - Personas - Barriers to Adoption Set 1 of 4

Barriers	Manufacturer	Developer	Implementer	Administrator	Operator	Consumer
Investment	X					
Risk	X		X			
Maturity/Complexity				X		
Infrastructure			X			
Standards						

### IoTAB - Personas - Barriers to Adoption Set 2 of 4

Barriers	Manufacturer	Developer	Implementer	Administrator	Operator	Consumer
Policies		X	X			
Access						
Transparency				X	X	X
Change resistance			X	X	X	X
Cybersecurity	X	X	X	X	X	X

### IoTAB - Personas - Barriers to Adoption Set 3 of 4

Barriers	Manufacturer	Developer	Implementer	Administrator	Operator	Consumer
Data Privacy	X	X	X	X	X	X
Legal / Regulatory		X	X	X	X	X
Trust						X
Training			X	X	X	X
Interoperability	X					

### IoTAB - Personas - Barriers to Adoption Set 4 of 4

Barriers	Manufacturer	Developer	Implementer	Administrator	Operator	Consumer
Environmental Factors	X	X	X	X	X	X

## 7. Cross Market and Development Topic Areas

Introductory text explaining the importance of the cross market and development topic areas. (Section 8.1 serves as an example to be iterated throughout the remaining subsections)

- Enhance and modernize the infrastructure for IoT (this can be related to things like connectivity, computing, power, legacy infrastructure, etc.)
- Create trust in IoT (security, privacy, transparency, data ownership, etc.)
- Supply chain integrity and resilience (in this case, Tom's version of supply chain, and not Robby's. We can put Robby's into the industry-specific section).
- Develop, grow, and maintain a workforce to support the IoT economy.
- Address challenges of IoT in a global ecosystem and economy
- Develop government capability to support and sustain a IoT economy (this is where the emerging technology office recommendations come in. We could also put in the recommendations from sustainable infrastructure
  - about government procuring IoT for its own use in its facilities, etc.).
- Facilitate industry adoption (including govt, small business adoption and value realization of IoT. this theme can be moved to the topic specific section, if we think it is appropriate).
- Facilitate IoT technology leadership (R&D, etc.). This one could potentially be combined with 6 although 6 is about govt leadership. whereas this one is about facilitating industry R&D...

### 7.1.1. Overview

- Definition of this theme area
- Why is this important and why does this need to be addressed?

### 7.1.2. Opportunities and benefits of solving challenges for each theme (for personas)

- Description of opportunity/market characteristic, etc
- Examples of representative opportunities
- Summary of key representative ongoing industry/government/academia efforts in this area

### 7.1.3. Barriers to those opportunities (faced by personas)

- Description of barrier and examples
- Who is impacted
- Impact/significance of this barrier (descriptive, or quantitative)
- Summary of barriers

## 8. Topic-specific Findings of the Advisory Board

[This section will provide topical details on the work and findings of the Board. These are presented in the order they were listed in Section 9204 with additional topics added thereafter. Section 8.1 serves as an example to be iterated throughout the remaining subsections.]

The Advisory Board explored the many areas described in Section 5(B)(ii) to explore, discuss, and consider “situations in which the use of the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States. Discussions included presentations from speakers who brought a unique perspective in these areas, or who represented groups that are continuing research on similar topics.

### 8.1. Smart traffic and transit technologies

[text will be fleshed out – these are the bullets from Board meeting slides]

Systems- security, intelligence, monitoring, management

Hardware- traffic signals, cameras, sensors, off-road equipment, busses, trains, vehicles with varying levels of autonomy (drones, shuttles), Electric Vehicle (EV) charging equipment, micromobility

Software- route planning

Connectivity- Cellular Vehicle to Everything (C-V2X), 5G, autonomous navigation (edge and cloud)

Edge Computing (self driving vehicles)

Artificial Intelligence

Linkage to IoT AB Subgroup on Smart and Critical Infrastructure

Safety Applications

Improving Road Safety/Protecting Vulnerable Road Users

Use Cases

emergency vehicle traffic preemption

entering school or work zone

pedestrian crossing ahead;

Support Functions

Package, Food and Medicine Delivery

Congestion Mitigation/Environmental Benefits

Orderly flow of traffic

Less time idling

Increase Productivity

Less time stuck in traffic

8.2. Augmented logistics and supply chains

8.3. Sustainable and critical infrastructure

8.4. Precision agriculture

8.5. Environmental monitoring

8.6. Public safety

8.7. Healthcare

## 9. Recommendations

The global Internet has rapidly progressed from a simple interconnection among a few computing centers to a ubiquitous digital environment that touches every aspect of our lives. A key part of 21<sup>st</sup> Century digitization is the continued IoT implementation within public and private-sector organizations.

The IoTAB recommends that the IoTFWG consider (and where appropriate, act to implement) the findings and recommendations below. The Board remains in place until [date] to clarify any points for the IoTFWG or to answer any questions about these recommendations.

[describe the fact that some of these recommendations are broad and cross-sector in support of national adoption. Others are topic-specific and are more focused on particular technical considerations, including many of the areas specified in the NDAA legislation.]








[describe that the first (seven) are broad, cross-sector recommendations, while the remaining are topic-specific and address the sectors specifically called out in the legislation.]

The global Internet has rapidly progressed from a simple interconnection among a few computing centers to a ubiquitous digital environment that touches every aspect of our lives. A key part of 21<sup>st</sup> Century digitization is the continued IoT implementation within public and private-sector organizations.

The IoTAB recommends that the IoTFWG consider (and where appropriate, act to implement) the findings and recommendations below. The Board remains in place until [date] to clarify any points for the IoTFWG or to answer any questions about these recommendations.

During discussions, seven topics surfaced repeatedly as areas that affected a broad range of IoT topics. Because this initial set represents cross-sector needs, the Board has described recommendations on those topics first in the report. The remaining recommendations are topic-specific and follow those cross-cutting discussions.

[Note: the Board has suggested the addition of visual icons / legends to highlight the types of recommendations being made. These are a starter set of icons that might be included before each recommendation as a simple cue. ]

- Research & Development 
- Technology transfer 
- Outreach & engagement 
- Workforce/training 
- Coordination 
- Grants/funding 
- Policy/guidance 

## Key Recommendation 1.0: National Data Protection Framework

The U.S. should establish a framework or model by which data related to the Internet of Things may be protected and used to benefit all. The model would consider a schema for describing IoT-related data and methods for both use and protection.

### Summary of Supporting Recommendations:

Supporting recommendation 1.1	The federal government should facilitate/support the development of a National Data/Privacy Framework that clearly delineates the different aspects of data (i.e., machine versus personal) and how they should or shouldn't be utilized in smart transportation technologies.
Supporting recommendation 1.2	The government should develop an IoT Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices.
Supporting Recommendation 1.3	Conformance to any specific set of requirements should be voluntary.
Supporting recommendation 1.4	(Under review) The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations.
Supporting Recommendation 1.5	Federal agencies can establish templates for clear and robust policies regarding data sharing and data usage involving third parties in the IoT ecosystem. Where practical, agencies can help to foster voluntary, industry-led adoption of such policies to enhance transparency leading to improved user trust in IoT devices and services.
Supporting recommendation 1.6	The government can encourage and foster data policies that drive economic growth, such as through this framework.



An element of this IoT Data Protection Framework might include definition of specific information / data types, along with recommended starting considerations for protection. A similar model exists for federal information systems. NIST Special Publication (SP) 800-60, for example, describes several hundred types of information along with recommended considerations about the consequences of a loss of confidentiality, integrity, or availability of that information. A similar model could be used for IoT-related data.

The framework would also support privacy-related considerations. During IoTAB discussions, the Board heard that privacy concerns inhibit adoption of IoT by consumers, so resolving trust concerns from potential users is an important objective.

The framework might provide states and local jurisdictions the ability to specify criteria, such as data retention or destruction requirements, anonymization methods, and guidance for effective data applications.

**Supporting recommendation 1.1:** The federal government should facilitate/support the development of a National Data/Privacy Framework that clearly delineates the different aspects of data (i.e., machine versus personal) and how they should or shouldn't be utilized in smart transportation technologies.

Through engagement with key stakeholders (including vehicle manufacturers, infrastructure providers, and transportation agencies), the U.S. can lead by example in establishing practical use cases for data usage.

Example use cases include the following:

- Data from a Traffic Camera at an intersection could be used to determine who was responsible for an accident and allow for more efficient insurance claims.
- Data generated from a connected vehicle and its corresponding roadside infrastructure can be utilized to transmit basic safety information to the vehicle's driver such as entering a school or work zone.
- Emergency Vehicles and corresponding roadside infrastructure can generate data to preempt traffic signals so the vehicles can get to their destination sooner.

While the vast amount of data that would be provided will significantly improve safety and convenience, the criticality and sensitivity of such data requires adequate protection that can be specified through this new framework.

**Implementation considerations:** In conjunction with supporting a National Privacy Framework, the federal government should consider setting high-level policy guidelines for data ownership, retention and usage that includes specific guidance for data that has personal information. These guidelines should leverage existing legislative or regulatory language and provide incentives for state and local jurisdictions to adopt them. Creation of a model and guidelines for data ownership, retention and usage would provide states and local jurisdictions the ability to

develop criteria for how long data should be retained, how personal information should be stripped from any such data, and how to effectively utilize that data in their operations.

As the framework is implemented broadly, constituents could share lessons learned from pilot projects and successful case studies, further supporting training and education on proper data retention and usage procedures.

**Potential barriers:** Funding and resource constraints may hinder implementation of this recommendation since some state and local jurisdictions/agencies may not have funding or staff to effectively implement these programs. Coordination across multiple jurisdictions will be challenging, since each jurisdiction has unique and challenging circumstances, and many have existing or pending data protection and privacy legislation.

Notably, it may be challenging to consistently identify and separate data that has personal or private information.

**Supporting recommendation 1.2:** The government should develop an IoT Privacy Framework for Innovation and Data Protection specifically tailored to the unique challenges posed by IoT devices.

[Ed. Note: The above recommendation (1.1) focuses on data protection but is not IoT-specific. The board could tailor that framework to include specifics related to the unique challenges posed by IoT devices. The framework would need to balance the need for data privacy and security with fostering innovation in the IoT sector - that makes it both complementary and separate from above. Notably, the framework would still need to be used as a voluntary guideline across any sector that develops or implements IoT. Doing so would provide a consistent, unified approach to Data Privacy and security in the IoT sector, reducing confusion and fragmentation for business, government, and consumers. This consistency would encourage innovation by providing clear guidelines and expectations for IoT device manufacturers, fostering a competitive and growth-oriented environment.

**Implementation considerations:** Considerations for this IoT model would incorporate lessons learned from existing privacy regulations, such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), to create a more effective and efficient framework.

The team creating and maintaining the framework would need to implement safeguards to ensure that the resulting product remains adaptable and scalable to accommodate the rapidly evolving nature of IoT technology and the Data Privacy Landscape.

**Potential barriers:** The data protection needs of business, government, and consumers can vary greatly. The IoT Data Privacy Framework would need to achieve a careful balance among those considerations. The government would also need to identify the means of providing resources, guidance, and support to constituents for the adoption and implementation of the IoT Privacy Framework.

Those creating this IoT Privacy Framework would need to ensure the means by which the model would be continually reviewed and updated to ensure it remains relevant and effective in addressing emerging Data Privacy challenges and technological advancements.

**Supporting Recommendation 1.3:** Conformance to any specific set of requirements should be voluntary.

There is general consensus that conformance to any specific set of requirements should continue to be voluntary. Market incentives continue to grow, and there is increasing interest in this program based on the participation by industry, consumer advocates and academia. Further incentives from the U.S. Government will drive more participation. On the other hand, a pivot from voluntary cooperation to obligatory mandates may diminish support. Changing the focus in industry from one of supporting development to debate over authority. Such a debate will likely stall progress despite current momentum in industry.

**Implementation considerations:** None identified

**Potential barriers:** None identified

**Supporting recommendation 1.4:** (Under review) The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations.

Using the framework model, the nation could create a set of "data use" basics that could be included in privacy policies for IoT devices. These could, for example, be expressed in a similar way to how security considerations are listed in NIST SP 800-60 (as referenced above). Consistent understanding of the data produced by various technologies, including example use cases that describe the data implementation, could enhance consistency of data protection. That consistency may improve confidence in IoT products and foster adoption of more trustworthy technology since adopters will have a baseline of information on which to make decisions and comparisons.

**Implementation considerations:** None identified

**Potential barriers:** None identified

**Supporting Recommendation 1.5:** Federal agencies can establish templates for clear and robust policies regarding data sharing and data usage involving third parties in the IoT ecosystem. Where practical, agencies can help to foster voluntary, industry-led adoption of such policies to enhance transparency leading to improved user trust in IoT devices and services.

Such templates and policies are vital due to the significant privacy and data protection risks presented by IoT's increased interconnectivity and data sharing capabilities. Since these risks may discourage IoT adoption, clear policies that safeguard users' personal data and ensure transparency would foster trust and expanded IoT use.

**Implementation considerations:** The government should create guidelines on how to effectively communicate third-party data sharing and data use in privacy policies, in alignment with other recommendations from this report. Those guidelines and policies would be supported by public awareness campaigns to educate users about their data rights and to share information about how to properly share and protect IoT data.

**Potential barriers:** Some organizations, including those who rely on third-party data sharing for business operations, may not be fully supportive of restrictions on data sharing and data usage. There may also be challenges in aligning these policies with existing privacy regulations and international data protection standards. While such challenges are not insurmountable, privacy and data protection requirements vary greatly by region and can be difficult to reconcile across cultural and geographic boundaries.

**Supporting recommendation 1.6:** The government can encourage and foster data policies that drive economic growth, such as through this framework.

Data policies can have a major impact on privacy, security, innovation, and monetization. Importantly, the lack of data policies can create uncertainty and hinder the growth of digital economies. Identifying opportunities to monetize data further enables business growth and can fuel synergistic ecosystems.

The federal government can apply policies to facilitate data protection, sharing, licensing, and analytics can minimize risk and maximize economic value.

Specifically, agencies should consider the potential impact of data policies and provide guidelines for data use and monetization. Citizens will benefit from the promotion of interoperability for data sharing, and from improved collaboration and information sharing among agencies and industry.

**Implementation considerations:** Implementation of this recommendation would include programs to promote the necessary infrastructure for data security and privacy, including aspects of data sharing, ownership, analytics and control. Agencies would need to establish and maintain data policies that ensure compliance with regulatory requirements, in consultation with industry, academia, and government agencies.

**Potential barriers:** Lack of knowledge about the data policies and resistance to change will likely both hinder adoption. Lack of data policy would hinder growth of digital economies, and even where policies are created, any lack of clarity on how data policies on confidentiality and security will impact stakeholders might result in reduced trust or effectiveness. There may also be challenges from costs of establishing the administrative and technical infrastructure needed.

## Key Recommendation 2.0: Standardize IoT Implementation

The Federal Government should establish methods to foster interoperability for IoT technology, including through the use of consistent models, protocols, and schemas.

There exist many standards today and there may be a better method for determining which standards should be used under specific conditions. In some cases, formal standards may be needed, such as those from a standards development organization or from a technical engineering organization (e.g., Institute of Electrical and Electronics Engineers (IEEE)). It is likely that wholly new standards and models will not need to be created “from scratch” but rather, industry collaboration is likely to advance existing communications and interoperability protocols that can rapidly be encouraged and adopted. The board highly recommends not to mandate any formal or informal standard or protocol, but rather to encourage voluntary conformance in the interest of improved interoperability.

Discussions at board meetings indicated that concerns about getting “locked-in” to a particular vendor’s proprietary technology currently act as an impediment to IoT adoption. No company or agency wants to invest in infrastructure that will rapidly become obsolete. Quite the opposite is true – in many cases, IoT infrastructure may need to operate for many decades. Parallel examples such as Wi-Fi (supported through IEEE 802 series technical standards) and cellular industry consortium standards demonstrate that interoperability and standardization do not reduce a vendor’s ability to innovate. Quite the opposite seems to be true – the ability for products to work together has great possibilities for both established manufacturers and newcomers.

Before the government can foster specific standards, it may be helpful for one or more agencies to perform a survey of available and relevant standards, protocols, and models. Such a survey would be helpful, for example, if agencies wish to include open standards and consortium developed standards as part of the requirements for federal funded projects. Federal recommendations (or requirements) for a given set of standards will promote industry adoption and foster standardization.

**Supporting Recommendation 2.1:** The government should 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.

Doing so would foster innovation and competition among all parts of the supply chain, simplify integration and maintenance for supply chain partners, examine the cybersecurity and privacy risks, scalability over time, provide cost savings, and potentially meet regulatory compliance.

By establishing a set of common standards and protocols, businesses can seamlessly integrate IoT solutions into their existing supply chain operations, facilitating data exchange, and enabling more efficient and informed decision-making processes.

Developing industry standards and protocols involves collaboration between government agencies, industry stakeholders, technology providers, and researchers to identify the key requirements and specifications for IoT systems in supply chain management. This may include addressing issues such as data formats, communication protocols, security measures, and device compatibility, among others.

In addition, the government should promote the adoption of these standards and protocols through education and awareness campaigns, providing businesses with the necessary resources and guidance to successfully implement IoT solutions in their supply chain operations. By creating industry standards and protocols, the government can help to create a stable and unified foundation for IoT technology, driving its widespread adoption, and maximizing its potential benefits for businesses and consumers alike.

**Implementation considerations:** The range of stakeholders should be considered from diverse persona groups including businesses, technology providers, academia, government agencies. There should be a prioritization on critical areas first (e.g., exchanging data, device interoperability, security). There should be a focus on building on existing standards ahead of creation of new ones.

**Potential barriers:** There could be a resistance to standardization given the current landscape and multitude that exists. There could be fragmentation of existing standards and a resistance to creating more standards given the current landscape and multitude that exists. There could be cost and resource constraints and a considerably different landscape given rapid technological advancements.

**Supporting Recommendation 2.2:** Agencies can support research and industry-led standards in areas such as telematics and sensor technologies for autonomous vehicles. These standards should be based on high-level safety guidelines (perhaps as determined by the National Highway Traffic Safety Administration or another federal organization).

The autonomous vehicle (AVs) market in some respects is still emerging. AVs exist in states like California and Arizona, however in other areas of the country they are only found in designated geo-fenced areas like a university campus. It will be some time before these exist on current highways / streets that have vehicles with human drivers. Research is needed to determine how AVs will interact with these vehicles, with roadside infrastructure, and with pedestrians. In addition, research is needed to show how these interactions change in times of bad weather.

Adoption of vehicle-related standards would promote improved safety and reliability through better vehicle and infrastructure communications and interoperability. Consistent communications standards will promote innovation as vendors work (and compete) to develop products and services that will work together. This increased production and adoption is expected to drive cost savings, further advancing adoption and benefits.

High-level safety guidelines will need to be finalized by the National Highway Traffic Safety Administration as there are still open liability questions particularly regarding a determination of

fault in the event of an accident. Spurred by these guidelines, industry can develop appropriate performance and safety standards in a market that is still emerging while avoiding the possibility of market fragmentation. It's important that all key stakeholders in the autonomous vehicle ecosystem participate in these safety discussions and standards development activities.

Vehicle safety and data protection are key concerns in both the U.S. and international communities, so there will likely be extensive oversight and regulatory guidance needed in the short term. The benefits to be gained, including improved safety, convenience, and operational cost reduction are likely to largely offset the burden of regulatory conformance.

**Implementation considerations:** There should be inclusiveness to involve a diverse range of stakeholders including autonomous vehicle manufacturers, roadside infrastructure manufacturers, communication technology providers, software developers, academia, and government agencies. This ensures that the resulting standards and guidelines are comprehensive, practical, and aligned with the needs and priorities of all relevant parties.

There is a need to prioritize safety. Deaths from traffic accidents continue to increase and standards/guidelines need to address how these technologies can help to decrease these. There is a need to build on existing standards first such as leveraging existing industry standards and best practices as a starting point. In particular there is a need for how connected vehicles that have a human driver present should interact with transportation infrastructure.

There is a need to design standards and protocols such that they are flexible and able to be adapted with time to accommodate new technologies, emerging threats, and evolving industry needs. There must be encouragement and incentive for widespread adoption of standards and protocols through education, outreach, and support programs. And there is a need to develop mechanisms to monitor and enforce compliance with the established standards and protocols, including certifications, audits, and penalties for non-compliance.

**Potential barriers:** The autonomous vehicle market needs to have sufficient time to develop. There are technical challenges that exist in areas such as radar interference, driving in extreme weather conditions. Developing standards and guidelines too early may hinder its growth. AVs will require certain infrastructure aspects like clear lane striping and a means to charge if they are electric.

Developing and implementing industry standards and protocols can be resource-intensive, requiring significant investments in time, money, and expertise. There is a current lack of regulatory guidance and high-level guidance is needed from applicable government agencies to set the safety requirements for autonomous vehicles. The board notes there is still an open issue of liability concerns that needs resolution. There are also public concerns that warrant the need for consumer education on autonomous vehicle technology.

**Supporting Recommendation 2.3:** The federal government should promote and adopt industry led standards for minimum baseline interoperability and cybersecurity requirements for

smart transportation technologies and corresponding transportation infrastructure (i.e., sensors in roads, cameras at intersections).

Industry standards and protocols ensure that devices from different manufacturers can communicate and work together seamlessly. The federal government should promote and adopt industry led standards that provide minimum interoperability and cybersecurity requirements for smart transportation technologies and corresponding transportation infrastructure. In particular, smart transportation systems focus on safety, so standardization (especially for security and interoperability needs) is vital to ensuring that devices can communicate basic safety information to other vehicles and to/from infrastructure.

There must be a way to address cybersecurity risks such that industry standards that describe minimum cybersecurity requirements of relevant technologies (i.e., having a unique set of keys for traffic controller cabinets) will help to provide implementing agencies some level of assurance that these risks are mitigated. Standards and protocols can set a path forward for subsequent government regulations or policies and are particularly relevant if industry led standards are attempting to address known gaps and market fragmentation issues. This is particularly important when dealing with multiple states and local jurisdictions.

Standards can stimulate innovation and competition by providing a level playing field for businesses and developers as well, regardless of their size or market share. With a level baseline companies can now build upon it and tailor their own solutions. Standardization can lead to cost savings for businesses by reducing the need for customized solutions and simplifying the procurement process. There are likely some areas where adopting or promoting standards can occur more readily such as sensors in roads that can detect defects and traffic cameras at intersections.

**Implementation considerations:** Same as Supporting Recommendation 2.2.

**Potential barriers:** Cybersecurity threats are constantly evolving, so standards and guidelines could be outdated rather quickly. There is concern over organization intellectual property (IP) whereas some organizations may have their own IP different from what's described in a baseline standard and not want to participate in activities that would deviate or reveal their IP. There are also cost and resource constraints to developing and implementing industry standards.

**Supporting Recommendation 2.4:** The federal government can facilitate and support the adoption of smart city and sustainable infrastructure standards.

Smart city infrastructure relies upon IoT technology to consistently operate. The Board recommends that the Working Group address funding and implementation considerations for smart cities. For example, municipalities may not have the budget to modernize IoT solutions that better integrate with those in other cities. Therefore, the government may need to develop creative solutions to help local, regional, and state entities to future proof their infrastructure.



**Implementation considerations:** Same as Supporting Recommendation 2.2

**Potential barriers:** There could be a resistance to standardization given the current landscape and multitude that exists. There could be fragmentation of existing standards and a resistance to creating more standards given the current landscape and multitude that exists. There could be cost and resource constraints and a considerably different landscape given rapid technological advancements.

**Supporting Recommendation 2.5:** The federal government should promote the development and adoption of existing industry standards activities with respect to energy efficient, clean, and renewable energy technologies that are used in sustainable infrastructure.

The federal government should consider interoperability to address the many technologies, some of which are proprietary technologies and the consideration for scalability over time. There needs to be innovation and competition, mitigation for any cybersecurity risks that exist, a way to save on costs through simplified procurement, a foundation for future policies through mechanisms of regulatory compliance, and the need to facilitate market entry.

**Implementation considerations:** Implementation considerations include: encouraging inclusiveness, prioritizing identified gaps, building on existing standards, encouraging flexibility and adaptability, promoting adoption, global collaboration, procurement and grants, and working with the states.

**Potential barriers:** Potential barriers include: that it may be time consuming and resource-intensive efforts to achieve consensus, there may be technological advancements, international harmonization may create more complexity and time, fragmentation may exist, and/or states may not all agree on adoption of standards.

**Supporting Recommendation 2.6:** Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT.

The proliferation of IoT devices without interoperable data will make it difficult to achieve interoperability the longer it diverges. In public safety, the interoperability of IoT device data will enhance incident responses and coordination among responder teams, providing safety benefits that would encourage the adoption of IoT. Solutions might include facilitation of adoption by funding grants for jurisdictions/agencies for procurement of interoperable IoT solutions. Support could also include development of education/training materials to help jurisdictions/agencies apply best practices for interoperability.

**Implementation considerations:** Compiling guidelines and best practices for entities from what currently exists as a starting point (e.g., NISTIR-8255:Interoperability Real-Time Public Safety Data, CISA SAFECOM Interoperability Continuum, etc.), prioritizing solutions which adhere to interoperability guidelines in government contracts for public safety IoT (e.g., bulk purchase pricing a la General Services Administration (GSA) catalog). From a high level, the consideration of tax incentives that would encourage companies to implement public safety IoT

with interoperable data standards and the education and promotion of interoperable data guidelines for public safety IoT across different jurisdictions (e.g., local and regional).

**Potential barriers:** There may be barriers to prioritizing data interoperability when procuring public safety IoT devices include limited budgets but also lack of understanding of what to require, there may be resistance from jurisdictions and public safety agencies that have already invested in an IoT solution, and there may be resistance from industry manufacturers because of concerns about their proprietary solutions.

**Supporting Recommendation 2.7:** (Under Review) Agencies can promote and, if necessary, develop a protocol for data exchange standards for IoMT (Internet of Medical Things) for interoperability, and promote the adoption of these standards. Solutions might include protection for medical data in mobile apps and IoT devices that is similar to the current Health Insurance Portability and Accountability (HIPAA) Act provisions.

Data exchange standards for IoMT would result in data interoperability, which would result in efficiencies and provide safety benefits that would encourage the adoption of IoT. This standardization would support coordination among relevant stakeholders, including product manufacturers and healthcare organizations, to ensure widespread adoption.

**Implementation considerations:** As data exchange standards for IoMT are developed and refined, agencies could prioritize the (in federal procurements and government contracts) solutions which adhere to or implement those solutions. Simply promoting the benefits (e.g., improved interoperability, potential cost reductions, avoiding vendor lock-in) to the community and education for healthcare organizations could increase adoption..

The federal government could also incentivize (e.g., through tax incentives) companies to implement the IoMT data exchange standard.

**Potential barriers:** There may be some resistance from healthcare organizations that have already invested in an IoT solution, or from industry manufacturers because of concerns about their proprietary solutions and captive user base.

## Key Recommendation 3.0: IoT Cybersecurity (including Critical Infrastructure)

The Federal Government should provide specific and consistent guidance for providers and adopters to ensure secure operations. While not the exclusive source of cybersecurity guidance, federal entities should continue to support NIST as a developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.

Until now, NIST's role has been to develop recommended baselines and outcomes for the entire IoT ecosystem. Industry subject-matter experts have participated in developing requirements for their specific sectors that align with NIST criteria. NIST's overall cybersecurity expertise is well-known, as is that of the sector-specific experts. By tasking NIST with developing required outcomes, and industry with specific requirements to meet those outcomes, each side works in an area of strength. These roles are working and should continue.

**Supporting Recommendation 3.1:** The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

By upgrading these buildings, they can set an example for private industry to follow. They could then promote conversion in other market segments such as industrial factories or power plants. Credibility and assurance can be provided to the private sector when the Federal Government leads by example.

Many government buildings are reliant on building control systems which provide the functional, operational, and safety needs of a building. These can serve as gateways for malicious actors who can take control of critical applications (including life and safety-related services) within a building (i.e., heating, air conditioning, physical access).

While such upgrades may be costly, it is possible that some of those costs could be offset by reduced cybersecurity insurance premiums and other fiscal benefits.

It is also notable that a great deal of data in an unprotected building control system may contain significant amounts of personal and confidential information.

**Implementation considerations:** The Environmental Protection Agency (EPA) has a program for Energy Star Building Certifications and there could be a similar program that addresses cybersecurity within a building. There are some efforts already underway within the commercial real estate sector that could be leveraged (<https://buildingcybersecurity.org/>). There are also parallels that could be explored such as the National Cyber Labeling Program for Consumer IoT versus Energy Star on appliances.

Implementation could occur through updated requirements, such as in the GSA Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR).

Owners of buildings used by federal organizations should, at a minimum, use basic cyber hygiene best practices (i.e., changing default passwords, segmentation of networks by using items such as firewalls, installing patches) as directed within requirements.

**Potential barriers:** Funding to upgrade the existing legacy base could be considerable. Also, if additional validation/certifications are needed for a particular building there is an additional upfront cost.

Building owners and managers may have limited knowledge of how to protect against cybersecurity attacks, especially in today's fast-moving technical environments, so lack of knowledge (or insufficient training) may be a barrier to such updates. These considerations would also be quite different depending upon the facility in question. For example, a medical building may have different needs and associated risks from a commercial office building.

Due to the evolving threat landscape, there may be frustration with changing requirements. As the threat landscape is constantly evolving, concerns may exist if a building has been updated with cybersecurity systems and malicious actors can still gain access to it. This condition is often the case, though, and should not impede whatever improvements can be made.

**Supporting Recommendation 3.2:** The government should 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.

Since supply chain security concerns can be a hindrance to IoT adoption, security provisions will enhance competitiveness and innovation, and will reduce resistance to information sharing. A more secure supply chain will help to protect sensitive data and provide operational assurance, as well as supporting compliance with various security regulations.

#### **Implementation considerations:**

The government can support better supply chain security through:

- Expanded research and development;
- Promotion of security-by-design principles;
- Allocation of resources to facilitate training and awareness;
- Encouragement of collaboration among industry stakeholders and government agencies; and,
- Improved maintenance of cybersecurity policies, regulations and best practices that adapt to an evolving threat landscape.

**Potential barriers:** Agencies have limited resources for implementing and maintaining the improvements described. Further, the complexity of supply chain logistics, resistance to information sharing among supply chain participants, and an evolving risk landscape add further to these concerns.

**Supporting Recommendation 3.3:** The government should prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices.

As the NSC-hosted workshop (Oct. 2022) demonstrated, it is possible to establish a national label program quickly and at scale, provided existing ecosystem mechanisms are used.

Efficiently using these processes requires taking advantage of industry expertise. Continued industry engagement as the program is scoped, planned, and executed will be critical to the program's success. Existing label programs vary; the more flexible the government can be in qualifying the process rather than dictating it, the better.

Process qualification should be outcome-based rather than centrally determined. These outcomes determine the need for trust mechanisms such as meeting the NISTIR 8425 Criteria and having industry-accredited processes.

The Administration should encourage Congressional support to deploy this program, including establishing incentives for manufacturers to participate. Increasing market incentives will be enhanced by introduction of the label program, but only if manufacturers participate. There is strong interest now, but the Administration and Congress can accelerate adoption with earned safe harbors, preemption of mismatched state laws for program participants, negotiation of mutual recognition or "equivalence" opportunity across borders and coordinate agency efforts with regard to consumer education.

Incentives may require legislation. However, there are a range of other options. Authorities of the responsible agencies may need adjustment.

**Implementation considerations:** Existing label programs vary; the more flexible the government can be in qualifying the process rather than dictating it, the better. Process qualification should be outcome-based rather than centrally determined. These outcomes determine the need for trust mechanisms such as meeting the NISTIR 8425 criteria and having industry-accredited processes.

**Potential barriers:** There may be a perceived advantage in defining a uniform U.S. government scheme rather than defining the necessary outcomes from various industry schemes.

**Supporting Recommendation 3.4:** The federal government should continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.

NIST's role has historically been to develop recommended baselines and outcomes for the entire IoT ecosystem. Industry subject-matter experts have participated in developing requirements for their specific sectors that align with NIST criteria. NIST's overall cybersecurity expertise is well-known, as is that of the sector-specific experts. By tasking NIST with developing required outcomes, and industry with specific requirements to meet those outcomes, each side works in an area of strength. These roles are working and should continue.

**Implementation considerations:** None identified

**Potential barriers:** None identified

**Supporting Recommendation 3.5:** The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.

Participation in the U.S. cybersecurity label program began strong, but with the expectation that certain issues would be addressed over time. Manufacturers cite concerns over perceived new liabilities incurred by adding the label to the product, as well as concerns over the existing possibility of enforcement action by relevant agencies in the event of a device hack. Relief from this concern could be via an earned safe harbor provision. Other potential incentives include relief from a patchwork of state requirements via a federal preempt and a successful negotiation of mutual recognition of U.S. marks with other nations and the EU. Coordinating agency messaging to ensure "one voice" on these label and certification programs to the private sector is also important.

Increasing market incentives will be enhanced by introduction of the label program, but only if manufacturers participate. There is strong interest now but the Administration and Congress can accelerate adoption with earned safe harbors, preemption of mismatched state laws for program participants, negotiation of mutual recognition or "equivalence" opportunity across borders, and coordinate agency efforts with regard to consumer education.

**Implementation considerations:** Existing label programs vary; the more flexible the government can be in qualifying the process rather than dictating it, the better.

Process qualification should be outcome-based rather than centrally determined. These outcomes determine the need for trust mechanisms such as meeting the NISTIR 8425 Criteria and having industry-accredited processes.

**Potential barriers:** There may be a perceived advantage in defining a uniform U.S. government scheme rather than defining the necessary outcomes from various industry schemes.

**Supporting Recommendation 3.6:** (Under Review) The Federal Government should update Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience requiring a sector-specific Internet of Things (IoT) data strategy.

Existing Presidential Policy Directives are outdated and should be updated to reflect the current risk associated with critical infrastructure reliability, resilience, security, and sustainability.

Most of the critical infrastructure assets/systems are owned and operated by private sector entities, thus, requiring crucial conversations with said infrastructure owners/operators. The Board feels development of the language and context should include input from the National Security Council, the Office of Management and Budget, and Intelligence Communities. Once developed, the language could/should be shared with additional communities of interest/practice (e.g., North American Electric Reliability Corporation (NERC), Federal Energy Regulatory Commission (FERC), and national information sharing and analysis centers (ISACs)).

Continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage critical infrastructure risk. Accurate and up-to-date accounting of assets residing on federal networks is also essential. Implementation would include enhancing visibility into agency assets and associated vulnerabilities, focusing on two core activities essential to improving operational visibility for a successful cybersecurity program: asset discovery and vulnerability enumeration.

**Implementation considerations:** None additional

**Potential barriers:** Consensus on language and processes to update will be difficult to coordinate among key stakeholders, based on disparate missions and competing priorities.

The fact that most critical infrastructure assets/systems are owned and operated by private sector entities will require crucial conversations with said infrastructure owners/operators.

**Supporting Recommendation 3.7:** The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.

The expansive development and adoption of IoT assets and systems should map to IoT performance metrics intended to strengthen critical infrastructure security and resilience. Agency Chief Technology Officers and other officers and associated program offices could serve as the nexus for convening peer stakeholders. Performance metrics will need to be defined in conjunction with owners/operators of critical infrastructure assets/systems (both Information Technology (IT) and Operations Technology (OT)). The Board also recommends that the SCO in each agency will participate in a Community of Practice, like the Federal Chief Information Officer (CIO) Council format, which, in turn, will serve to convene officers across all agencies.

**Supporting Recommendation 3.8:** (Proposed Update) The federal government should promote and support the development of an overarching guideline developed in a multi-stakeholder process that more clearly distinguishes the major sectors of the IoT for use when dealing with concerns such as cybersecurity.

This overarching guideline would serve as a reference tool to distinguish the operating environments for the major sectors of the IoT and how cybersecurity concerns or issues would be addressed in a particular sector. For the guideline to be relevant it needs to be developed in a multi-stakeholder process that is open and includes industry participation across the various sectors (i.e., consumer, industrial, healthcare, finance, transportation). This guideline would not necessarily define the major IoT sectors, it is better used as guidance when cybersecurity legislation or regulations are being considered.

An example of a high-level writeup that would be included in this guideline that targets the industrial IoT sector is provided below: The Industrial IoT or OT sector leverages existing cybersecurity standards such as the IEC 62443 series of international standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems. Industrial automation and control systems are used in nearly every industrial sector such as manufacturing, transportation, energy, and water treatment industries. There are also several conformity assessment and certification programs that exist for these standards. When legislative or regulatory language is developed targeting this sector, ideally it should reference these standards.

**Justification:**

The justification an overarching guideline that distinguishes the major sectors of the IoT with respect to cybersecurity concerns is provided below.

- **Use/Scope:** Consumer IoT devices are typically used for personal and home use, whereas Industrial IoT (IIoT) devices are used in industrial settings for manufacturing, transportation, energy, and other critical infrastructure.
- **Utility:** Consumer IoT devices are generally used for convenience and entertainment purposes, whereas IIoT devices are used for enhancing productivity, improving efficiency, and reducing costs in industrial processes
- **Applications:** Consumer IoT devices are used for a range of applications such as home automation, health monitoring, and entertainment, whereas IIoT devices are used for industrial applications such as monitoring and control of machinery, inventory management, and supply chain optimization.
- **Impact:** Cybersecurity breaches in consumer IoT devices may result in loss of personal data and privacy violations, whereas security breaches in IIoT devices can cause significant damage to critical infrastructure, including production downtime, supply chain disruptions, and safety risks.
- **Life Support:** Some IIoT devices such as medical devices and aerospace systems may involve human safety, and their cybersecurity vulnerabilities can lead to fatal outcomes.



- Automation: IIoT devices are often automated and may interact with other machines and systems, whereas consumer IoT devices are interact primarily with their human users and other consumer IoT devices.
- Reliability: IIoT devices must operate reliably and continuously in harsh environments, whereas consumer IoT devices typically operate in more controlled environments.
- Privacy: Consumer IoT devices may collect and transmit personal data, and protecting user privacy is a critical cybersecurity concern. IIoT devices may also collect sensitive data, but the privacy concerns may differ based on the application.
- Interoperability: IIoT devices are often part of larger systems and must be interoperable with other devices and systems, whereas consumer IoT devices are often standalone and may not require interoperability (although there is a trend towards increased interoperability in certain scenarios)
- Scalability: IIoT systems often involve a large number of devices and must be scalable to accommodate growth, whereas Consumer IoT systems may be smaller in scale
- Regulation: Legislation or regulations that are developed targeting a particular sector do not necessarily apply across all sectors. IIoT devices may be subject to industry-specific regulations or are already heavily regulated (i.e., healthcare). Consumer IoT devices may be subject to general data privacy regulations.
- Attack Surface: IIoT devices have a larger attack surface due to their connectivity and may be vulnerable to various types of cyber threats such as hacking, malware, and ransomware. Consumer IoT devices may also be vulnerable to similar threats, but the attack surface may be smaller.
- Criticality: The cybersecurity of IIoT devices is critical for the operation of critical infrastructure, whereas consumer IoT devices may not be as critical
- Distinction: IIoT devices are starting to incorporate Consumer IoT devices (i.e., sensors, cameras) and the distinction between IIoT and Consumer IoT is blurring.

#### **Implementation Considerations:**

- Multi-Stakeholder process: It's critical that this guideline development has participation and representation across the relevant IoT Sectors. NIST could convene workshops similar to the process they use with respect to the Cybersecurity Framework (CSF)
- Use the CSF: The CSF guidelines could be extended to distinguish these major IoT Sectors.
- Use Cases and Examples: For each Sector that the guideline addresses it needs to rely on existing information from the corresponding sectors (i.e., National Label Program for

Consumer Devices-Consumer Sector, FDA requirements for new internet-connected medical devices-Healthcare Sector). The guideline could also include examples from each sector of how they utilize best practices/industry standards to mitigate cybersecurity threats. Harmonization: The guideline could help to promote international harmonization.

**Potential barriers:**

- Resource constraints: Staff resources would be needed to put this together are likely significant.
- Coordination across government agencies: Having government agencies reference or point to this guideline could be challenging. Education and outreach would definitely be needed.
- Existing regulations/legislation/frameworks: Some states like California and other nations like Europe already have existing material and there would be a question of how this guideline would align with them.
- Evolving threat landscape: As the threat landscape is constantly evolving there are concerns with this becoming outdated and in need of updating.

## Key Recommendation 4.0: IoT Connectivity Improvement and Expansion

The federal government should expand and improve programs that ensure reliable and sufficient connectivity among and between IoT devices in all areas of the country. The government should further promote accelerated innovation to ensure improved communications by ensuring the availability of suitable and sufficient spectrum resources, the development of wide-area networking technologies, and enhancing interoperability.

By definition, IoT technology must be able to interconnect through some physical, ad hoc/mesh, or wireless capability. While communications technologies (e.g., satellite, cellular, broadband/Wi-Fi, and other traditional licensed communications technologies) have expanded in both geographic scope and capacity to accommodate higher data loads in recent years, the capabilities are not unlimited. This condition is exacerbated by the fact that, in many cases, the very places where some IoT sensors are needed, such as for remote security and environmental monitoring, are locations with limited connectivity. Scalability represents another IoT challenge: the communications infrastructure must simultaneously support hundreds of billions of digital conversations.

The rapid evolution of communications technology in recent history demonstrates the significant promise and opportunity for the nation to improve IoT connectivity. Current capabilities that were science fiction in the past are now routine in our daily lives. The U.S. must continue such advances to ensure that IoT can securely and reliably communicate and interoperate wherever devices are applied.

Supporting Recommendation 4.x: (Proposed) To promote continued U.S. leadership on spectrum policy, the government should continue to free up spectrum for licensed and unlicensed use via spectrum sharing and repurposing underutilized federal spectrum.

The government, through collaboration between the National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC) has successfully identified a significant amount of under-utilized federal spectrum that could be made available for private sector use, including for IoT applications. This policy should be continued and should continue to support both licensed and unlicensed applications.

As has been noted, IoT applications are expanding and continued growth is expected.<sup>1</sup> The technology industry uses both licensed and unlicensed spectrum to enable this growth. Spectrum availability should not become a choke point in this growth.

- Licensed spectrum usage through 5G (discussion of 5G)
- Whereas unlicensed spectrum typically (discussion of unlicensed) ...

---

<sup>1</sup> *Op cit* the prior background discussion on billions of IoT devices in coming years.

- A comprehensive report on U.S. unlicensed spectrum usage is available from <https://shop.cta.tech/collections/research/products/unlicensed-spectrum-and-the-us-economy-quantifying-the-market-size-and-diversity-of-unlicensed-devices>

**Supporting recommendation 4.1:** The federal government should consider increasing funding and accelerating implementation of broadband deployment across rural America.

A recent US Department of Agriculture (USDA) report reported that 60% of US farmland doesn't have good Internet connectivity. While innovative solutions have expanded in recent years, point to point solutions and satellite-based connectivity quickly become expensive and do not resolve all issues. For example, it can be difficult to maintain connectivity to all areas of a farm.

The federal government currently offers limited funding and grants (ex. Department of Agriculture – Community Connect Grant Program) to help fund broadband deployment in rural communities, however, these opportunities have not advanced quickly enough to provide broadband coverage for certain areas of rural America.

**Implementation considerations:** The U.S. should mandate broadband infrastructure deployment across rural areas until U.S. coverage is complete. Current federal funding operates across several programs making it difficult to identify and find the opportunities available to specific areas.

In some cases, network communications equipment could be installed if power sources were adequately available. For this reason, funding might include options for supplying energy sources such as solar power, wind power, or micro-hydro power where access to reliable electricity is limited.

Other connectivity solutions that federal agencies could explore include taking advantage of modern communications technology and protocols, such as 5G mobile broadband, fixed wireless systems, and low-earth orbit (LEO) satellites.

**Potential barriers:** Connectivity is improving every day, yet expansion may be limited if there are few eligible service providers in certain areas. It may be helpful to better understand why some areas remain underserved, so agencies may want to review previous expansion efforts to identify lessons learned, both positive and negative.

**Supporting recommendation 4.2:** The federal government should actively promote and support the adoption of satellite narrowband IoT systems for agricultural IoT, with the aim of improving connectivity, data collection, and decision-making in rural and remote agricultural areas.

Note: While the focus for this topic by the Board relates to agricultural needs, the opportunity applies to any IoT connectivity where devices are deployed in remote areas.

Satellite IoT systems provide a reliable and efficient means of connectivity and data transfer in remote agricultural areas where traditional terrestrial connectivity options may be limited or

unavailable. Encouraging the adoption of satellite IoT systems will enable farmers to optimize their operations through real-time data management, resulting in benefits for various stakeholders, including farmers, policy makers, agricultural companies, and consumers.

Encouraging the adoption of satellite IoT systems will enable adopters, such as farmers, to optimize their operations through real-time data management, resulting in benefits for various stakeholders, including farmers, policy makers, agricultural companies, and consumers.

Reliable and consistent support for such remote connectivity requires harmonization of standards for satellite narrowband IoT. The Board recommends that satellite narrowband solutions be explored and developed for specific applications such as agricultural applications and environmental monitoring needs.

**Implementation Considerations:** Harmonize standards for satellite narrowband IoT: This is an early stage tech, but having appropriate standards will help drive the ecosystem. For example, should sensors be allowed to communicate with IoT satellites from different providers?

Establish a public-private-academia partnership: This partnership should involve satellite service providers, IoT technology companies, Agriculture data-platform providers, Ag Extension Centers, research institutions, and relevant government agencies. The goal of this partnership would be to support the development, implementation, and adoption of satellite IoT systems in agriculture.

Define specific agricultural applications: Consider specific use cases for satellite IoT in agriculture, such as precision farming, crop monitoring, water management, livestock tracking, and supply chain traceability. Tailor solutions to address these specific needs to maximize the impact of satellite IoT technology in the agricultural sector.

Develop financial incentives and subsidies: Provide incentives or subsidies to facilitate the adoption and integration of satellite IoT systems by farmers and agricultural businesses. These incentives could include tax breaks, grants, or low-interest loans to help offset the upfront costs associated with implementing satellite IoT systems.

Promote education and training: Create educational programs and resources to help farmers and agricultural professionals understand the benefits of satellite IoT technology and how to effectively implement and use these systems. This can be achieved through collaborations with Ag Extension Centers, universities, and industry experts.

The role of states should be clearly defined, and funding for satellite IoT infrastructure and adoption may be allocated to states to manage and distribute. Incentives or subsidies for satellite IoT adoption and integration could be considered as part of the upcoming Farm Bill or other relevant legislation. There might be international coordination, along with spectrum considerations with the International Telecommunications Union (ITU).

**Potential barriers:** High upfront costs and limited expertise in satellite IoT technology may hinder widespread adoption. Additionally, effective collaboration between multiple agencies, stakeholders, and the private sector will be necessary to ensure successful implementation. Ensuring data privacy and security, as well as addressing any potential regulatory or licensing issues, will also be crucial factors to consider.

## Key Recommendation 5.0: Address Privacy Considerations for IoT

The Federal Government should address privacy specific considerations for IoT. The successful adoption of IoT technology depends heavily on gaining the trust and confidence of the organizations, agencies, consumers, and others that will implement and expand its use.

IoT provides powerful benefits, as described above, but reaping those benefits requires placing sensors and devices in physical locations that can be highly sensitive and intrusive. While IoT promises exciting innovation and advancement opportunities, trust in that technology (and in the protection of associated data) by industrial adopters and other stakeholders is a key prerequisite. Trust considerations directly influence IoT adoption, including IoT devices' safety, reliability, and ability to protect sensitive information stored and processed.

**Supporting recommendation 5.1:** Develop and implement a privacy transparency system for IoT devices, using the "U.S. Cyber Trust Mark" for business, government, and consumer data for Connected Devices and other transparency programs as a guide.

**Implementation Considerations:** Empowering businesses, governments, and consumers to make informed decisions about IoT devices based on their privacy features and practices. Encouraging IoT device manufacturers to prioritize privacy, fostering competition and innovation in privacy-enhancing technologies. Enhancing overall Cybersecurity and data protection by promoting greater business, government, and consumer data awareness of privacy practices. Considering input from privacy experts, industry stakeholders, and business, government, and consumer data advocacy groups to develop privacy transparency, including content and design. Developing guidelines and standards for privacy transparency, including required information, format, and or product information. And encouraging IoT device manufacturers to adopt privacy transparency and provide resources to help them align with the new recommendations.

**Potential Barriers:** Ensuring broad adoption and compliance with the privacy transparency system across different industries and sectors. Incentivizing IoT device manufacturers who may perceive privacy transparency as burdensome, costly, or restrictive. Balancing the need for comprehensive privacy information with simplicity and ease of understanding for businesses, the government, and consumers.

**Supporting recommendation 5.2:** Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.

PETs support broader U.S. goals of leveraging technology for societal benefits and protect privacy while extracting valuable insights from the vast IoT data. The use of PETs fosters trust and promotes acceptance of IoT solutions. There is an alignment to responsible data use without compromising user privacy. The implementation of PETs can be used to prevent data breaches and associated legal issues.

Also there is alignment in existing proposals through the White House in the White House's Advancing a Vision for Privacy-Enhancing Technologies proposal (June 2022) and the National

Cybersecurity Strategy Implementation Plan from July 2023 on Initiative Number: 1.2.1 Initiative Title: Scale public-private partnerships to drive development and adoption of secure-by-design and secure-by-default technology.

**Implementation Considerations:** There are measures to ensure that there are robust security measures for PETs to prevent unauthorized data access. Conducting comprehensive technical and ethical evaluations of PETs before their adoption. There is a need to enhance public understanding and trust in PETs, encourage interoperability between different PET systems, and potentially establish a framework for monitoring the effectiveness and impacts of PETs in IoT technology.

**Potential Barriers:** Limited technical expertise to understand, implement, and manage PETs, possible resistance from private sectors due to perceived risks or costs, and the complexity of developing universally accepted privacy standards for IoT.

**Supporting recommendation 5.3:** Use Plain Language in IoT Privacy Policies as part of the Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020.

The federal government should advocate for the simplification of IoT privacy policies, privacy notices, and data use policies to enhance accessibility and comprehension for users. Improved understanding of data privacy policies for users will lead to more informed decisions when adopting and using IoT devices. The creation of requirements for IoT providers will foster implementation of simplified IoT privacy policies for government contracts.

Because the expectations, requirements, and cautions will be better understood, the use of plain language may lead to increased compliance and will enhance public trust in IoT devices and related technologies.

Two areas of the Use National Cybersecurity Strategy Implementation Plan July 2023 align:

- Initiative Number: 3.2.1 Initiative Title: Implement Federal Acquisition Regulation (FAR) requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020
- Initiative Number: 1.1.1 Initiative Title: Establish an initiative on cyber regulatory harmonization

**Implementation considerations:** Develop guidelines and best practices for organizations to follow when simplifying privacy policies, establish high-level guidance for evaluating and assessing the readability of privacy policies, coordinate with relevant stakeholders, including the private sector and business, government, and consumer data advocacy groups, to ensure widespread adoption.

**Potential barriers:** Resistance from organizations that may perceive simplification as a limitation on their legal protections. Possible challenges in defining the appropriate level of simplification while maintaining accuracy and comprehensiveness. Monitoring and updating the



simplification guidelines to account for technological advancements and emerging privacy concerns.

[Ed Note: Privacy R04 – Include IoT in U.S. Federal Privacy Regulation Proposal – is not included and is being reviewed for potential addition.]

## Key Recommendation 6.0: Sustainable Infrastructure

The Federal Government should lead in the adoption and integration of sustainable infrastructure and emerging technologies into the US economy and infrastructure.

**Supporting Recommendation 6.1:** The federal government should specify and utilize energy efficient and sustainable technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.

The U.S. lags behind other nations in reducing environmental impact, such as by reducing carbon footprint and greenhouse gas emissions. By requiring increased use of energy efficient technologies, the U.S. can make progress toward environmental goals.

Implementation might include adoption of building and energy codes that include language like automated demand response technologies, EV Read, EV Capable, etc.

**Implementation considerations:** Look at incorporating energy savings through performance contracts and examination of building energy use benchmarking. Adoption of building and energy codes that include language like automated demand response technologies, EV Read, EV Capable, etc. GSA FAR specifies energy efficiency requirements for procurement in federal owned and operated buildings.

**Potential barriers:** Funds such as high costs to scale conversion to energy efficiency. Supply chain issues (e.g., in distribution transformers, mining limitations for batteries, etc.) that manufacturing is trying to overcome. Legacy equipment and existing equipment (e.g., boilers, furnaces, etc.) that have a long lifetime.

**Supporting Recommendation 6.2:** The federal government should consider new models for sustaining and support in considering project feasibility.

Grants offset acquisition and build, but many organizations lack financial means and resources to sustain operations and maintenance. Because of this constraint, projects either shut down after funds run out or some entities are discouraged from applying. IoT requires additional levels of support and resources that buyers may not have accounted for – software licenses, data maintenance, data analysis, for example.

IoT enables new business and operating models. Economic service models to assist could include extended funding for O&M for select applicants (i.e., rural, tribal, small towns, etc.),

encourage regional cost sharing for multiple cities in a region to apply as one, and encourage innovative models (i.e., corporate, sponsorships).

**Implementation considerations:** There are types of models - 1) Extended Funding – extending funding for O&M for select applicants (rural, tribal, small towns, etc.). 2) Regional cost sharing – encourage multiple cities in a region to apply as one. 3) Innovative – encourage innovative models (corporate, sponsorships).

**Potential barriers:** Non-traditional and innovative models may be difficult to evaluate and track. IoT funding may be embedded into a broader funding package and not easy to separate the two.

**Supporting Recommendation 6.3:** The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.

EmT is rapidly evolving, with transformational value, and unexplored opportunities. Emerging technology is broad (AI, IoT, quantum, etc.) and some agencies may have some existing EmT interagency roles. Agencies consider participating in a Community of Practice, like the Federal CIO Council format, which, in turn, will serve to convene EmT officials across all agencies. This recommendation is in parallel to the supporting recommendation (below 6.4) on establishing a National Emerging Technologies (EmT) Office. The aim should be to establish new and/or leverage existing FACAs to augment knowledge and expertise gaps and a process for defining what EmT is and a list of EmT should do.

**Implementation considerations:** Establish specialized capabilities (e.g., IoT, smart cities, AI, quantum, etc.), in each office. Use language specified in the Oversee Emerging Technology Act (S.1577, 5/11/2023) on advising on responsible use of emerging technologies; providing expertise on responsible policies and practices, collaborate with officials and coordinating bodies across the Federal government, and offer input for responsible procurement policies; and the identification of the official and provide a description of the official's authorities and responsibilities to Congress.

**Potential barriers:** Agencies lack expertise on EmTs and the resources/capacity to implement an agency strategy, develop policy or other associated support, practices, programs and actions. There is limited EmT coordination between agencies that lead to uneven treatment, policies and siloed execution.

**Supporting Recommendation 6.4:** The Federal Government should establish a national Emerging Technologies Program Office within the Executive office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage emerging technology initiatives across the United States.

The US should lead in the adoption and integration of emerging technologies into the US economy and infrastructure. Currently a lack of coordination from the Executive Office leads to

siloeed planning, policies, execution, suboptimal utilization of resources, duplicate programs, monitoring, thus limiting realization of economic, social, security and other values and benefits.

This office should be aligned with the Office of Science and Technology Policy to: 1) work with federal departments and agencies and with Congress to create bold visions, unified strategies, clear plans, wise policies, and effective, equitable programs for IoT and Smart Cities modernization; 2) engage with external partners, including industry, academia, philanthropic organizations, and civil society; state, local, Tribal and territorial governments; and other nations; and 3) ensure equity, inclusion, and integrity in all aspects of IoT implementations.

The specific roles, responsibilities and interactions with the EmT function in the federal agencies and with states should be identified. There is a need to establish new and/or leverage existing FACAs to augment knowledge and expertise gaps. The necessary coordination and integration with the NIST (FWIoT and Global City Teams Challenge (GCTC)) protocols should be in place ( i.e., IoT implementations involve the integration of multiple technologies, systems, and stakeholders).

**Implementation considerations:** Establish specialized capabilities (e.g., IoT, smart cities, AI, quantum, etc.), in each office. Consider alignment with the U.S. Chief Technology Officer role. Consider language specified in the Global Technology Leadership Act (S. \_\_\_, 6/8/2023) for some of the functions, including:

- Identify technologies that matter most to US economic and national security
- Assess US capacity with each, including manufacturing, workforce, supply chain, capital access and R&D
- Evaluate technology leadership relative to other countries
- Determine appropriate policy response

**Potential Barriers:** Siloeed execution and Lack of coordination from the Executive Office, minimal support from designated agency leadership, lack of branding, lack of coordination, stakeholder engagement, resource allocation, and performance monitoring.

**Supporting Recommendation 6.5:** The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP). IoT can bring great economic and societal benefits to our cities, but specific smart city and sustainable infrastructure expertise in industry is limited, unevenly distributed, and fragmented. Some cities and agencies also lack the tools and resources, and even smaller cities and agencies may be even more constrained. Municipalities and agencies may not have the budget, the empowerment, or the ability to engage the necessary resources.

A different way to engage these resources is needed. The public procurement processes to engage private sector resources are burdensome. A SCSEP similar to existing partnerships

(e.g., MEP, USDA) would be a worthwhile investment, and would provide an improved model over the current public procurement process to engage private sector resources.

SCSEP should be put in place and operational to support sustainable infrastructure projects funded through the Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act (IRA). The role of states should be defined. In particular, some BIL and IRA funding may be given to states to manage and allocate. Consideration should be given as to whether some of these activities can be performed through the existing extension offices and infrastructure, or through partnerships with regional consortiums or states.

**Implementation Considerations:** Smart cities, sustainable infrastructure and IoT are broad in scope and discipline. A SCSEP should be a multidisciplinary center with spanning expertise (technical, operations, cybersecurity, etc.). The expertise lies across a variety of areas and could be implemented through partnerships with public (state, local) agencies, industry, and universities. There are a small number of regional “smart city” type consortiums across the country. Consider establishing partnerships or collaboration with these consortiums to support or enable these capabilities. For example, the USDA agriculture extension offices and the US Department of Commerce manufacturing extension partnerships model as starting points. They have built infrastructure and processes. In some rural areas, perhaps this is how these capabilities of the SCSEP should be delivered.

**Potential barriers:** Limited expertise in the market and industry; resources and expertise may be difficult to secure. Establishing a new extension office infrastructure will take time and resources. There is not a clear or obvious federal agency owner for this.

**Supporting Recommendation 6.6:** The federal government should consider the specification and utilization of IoT and “smart” technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.

The federal government should consider the specification and utilization of IoT and “smart” technologies into infrastructure and other projects that are funded in full, or partially, with federal funding. Every year, the federal government, through its many agencies, supports and funds billions of dollars of infrastructure planning, construction and operation projects. These projects include projects owned by non-federal stakeholders (municipalities, utilities, agencies, states, etc.) and federal stakeholders (federal facilities, infrastructure, etc.).

The federal government should take this opportunity to specify and incorporate IoT and smart technologies into infrastructure projects spanning the project lifecycle from design, construction, to commissioning and operation. For example, IoT technologies can be specified and used during the construction phase of infrastructure projects. Air quality sensors can be specified to monitor vehicle emissions and dust and particulate matter generated during construction in order to comply with local air quality regulations. When air quality levels reach certain levels, mitigation measures can be implemented to minimize impacts to worker and community health. IoT sensors and intelligent traffic solutions can be specified into roadway projects to support future intelligent highway and autonomous vehicle projects. Remodeling or construction of new

federal facilities, including airports, military bases and buildings can specify the use of various IoT solutions, such as smart building sensors and energy management systems, smart parking, and other technologies.

The federal government, through its procurement and funding activities, can influence and facilitate action. For example, the GSA and the U.S. Army Corps of Engineers specified the use of Building Information Modeling (BIM) in its projects. As a result, contractors had to comply with the requirement and used BIM tools, which enabled both the government and the contractor to reduce construction and project risks. A similar approach was used to accelerate the utilization of small and disadvantaged businesses (SB and SB8a) in federally funded transportation projects.

**Implementation Considerations:** While it is easy to say “you shall incorporate IoT technologies”, it is more difficult to specify what IoT technologies should be acceptable to be used. Some concrete and specific IoT applications should be defined for inclusion in the project and funding requirements, based on project types. Without this list, the contractors will be left on their own to interpret what is meant by IoT, and in some cases, will do the minimum possible just to comply or comply with things that meet the definition but not make any sense. Additionally, a broader vision and understanding of how IoT is to be incorporated, used and operated is needed by project owners, governments and operators in order to develop the requirements and specifications.

**Potential Barriers:** Project owners may have limited to no IoT awareness of knowledge. Limited expertise and resources in government and marketplace to support IoT in the projects. Specification of IoT may add complexity and cost to the project, the requirements, and to the timeline. No pre-defined acceptable or allowable IoT is to be considered and specified for the different types of projects.

**Supporting Recommendation 6.7:** The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility.

The federal government should consider models to help select adopting organizations sustain and support beyond the initial acquisition and building of new projects incorporating IoT technologies. While grants for projects help offset the initial cost of capital procurement, integration and development, the cost of operating the asset or system is left to the organization, municipality or agency. Some select organizations have the resources, funding models, or mechanisms to find the resources to sustain the operation and maintenance of this asset or system. However, many other organizations, especially the smaller ones, or those in rural and tribal areas, that benefit from these technologies the most, do not have these mechanisms (budget, taxes, etc.), and may forgo these types of projects, or only operate the IoT applications short term until the funds run out. Similarly, current agency grant application evaluation criteria may screen out those that don't meet the financial requirements for sustaining operations.

**Implementation considerations:** Extended Funding: For existing grant programs, consider extending funding for operations from one to two years for applicants that meet specific criteria of those that can benefit from IoT but could not otherwise sustain it (rural areas, tribal areas, small cities and towns, etc.) Regional models: Incorporate models that encourage regional partnerships. For example, one small community may not have the means to sustain a small IoT application. But if multiple adjacent communities apply for a grant together, they may be able to leverage some economies of scale to purchase and set up the application but may be able to employ synergies and cost sharing to maintain the application together. Innovative partnerships: Incorporate criteria that encourage and reward innovative approaches to sustaining operations. For example, one city was able to sustain operations by implementing a “support a AQ node” and getting corporate sponsors in the business community to support the maintenance and operation of the network.

**Potential barriers:** IoT funding may be embedded into a broader funding or project package, and it may not be easy to separate the two. Non-traditional and innovative funding models may be challenging to track and evaluate. All federal agencies that provide grants and funding for projects where IoT may be incorporated.

**Supporting Recommendation 6.8:** The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models.

The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models that capture and document the ecosystem. Smart cities are complex ecosystems of communities, neighborhoods, districts, buildings, other cities, utilities, and businesses that co-exist, collaborate occasionally and interoperate with each other. Reference models capture the various components of the ecosystem and provide a blueprint for design and planning, collaboration, coordination and communication in smart city efforts, sharing and economies of scale.

These reference models include technical and operations frameworks and architectures, operational concepts, and draft requirements and reference standards. The reference models serve as a template that planners can use to plan, design and build their smart city projects, and if followed, provides a path for interoperability, scalability, integration and security. Furthermore, these models incorporate best practices and facilitate collaboration between various stakeholders, accelerate adoption and scaling, and are replicable. A broader reference model/architecture helps to identify use cases, potential areas of collaboration between entities, as well as identify areas of “sharing” and economies of scale.

**Implementation considerations:** The NIST GCTC has already established a structure and model to create, engage and support industry/academia/government partnerships. This effort should consider inclusion of public entities such as counties, states, and other regional agencies and utilities. There is not a one size fits all “reference model and architecture”. There is one for small cities, large cities, as well as “smart regions”, utilities, buildings, etc. Key participants in developing the reference model include government (states), federal, industry (and industry and standards bodies), and academia. There are various efforts around models and standards.

Consider projects that are funded using federal money to incorporate the use of these reference models. NIST has developed the Smart City Framework v1.0 (<https://pages.nist.gov/smartcitiesarchitecture/>) and that is a starting point for building on something that may be more usable to city planners.

**Potential barriers:** Complexity of coordinating various stakeholders together to define a reference model or Architecture. There may be work in these models undertaken by consortiums or industry. Integrating and aligning existing parts of models may be challenging.

**Supporting recommendation 6.9:** The federal government should promote development and adoption procedures that accelerate and streamline planning, permitting, and interconnection aspects related to energy efficient technologies.

The US could benefit from improvements in decarbonization and reduction of greenhouse gas emissions. Many of the energy efficient technologies today incorporate the use of IoT (smart inverters, energy storage systems, etc.). There are improvements to be made in the deployment, permitting, and interconnection processes. Improvements to deployment of critical electric transmission to move electric power from location constrained renewables. Improvements to the installation and operation of rooftop solar panels for the permitting and interconnection process. The board indicates that 70 to 80% of projects never make it past permitting and interconnection queue to commercial operation.

**Implementation Considerations:** Permitting legislation being discussed in Congress. Department of Energy (DOE) RFI designation of National Interest Electric Transmission Corridors (NIETCs). FERC-Back-stop siting authority. Use of existing rights of ways (i.e., railroads and highways). DOE Solar APP+.

**Potential Barriers:** Time consuming and resource-intensive developers lose interest and cancel projects. Overcoming Resistance. Cost- accounting for them accurately and acceptably. Supply chain. Grid infrastructure requires developers to pay for upgrades to support energy sources.

**Supporting recommendation 6.10:** Accelerate the promotion and adoption of procedures and methods to make the electric grid more reliable and resilient.

A more reliable and resilient grid can better accommodate the integration of renewable energy sources enabled by IoT. This is made possible through the incorporation of technologies enabled by IoT (i.e., smart inverters, energy storage systems) resulting in quicker restoration from natural and man-made threats, more efficient transmission of electricity, and potential cost reductions both for utilities and consumers.

**Implementation Considerations:** DOE Funding. Near-term technologies provide short-term solutions at a lower cost (e.g., Dynamic Line Ratings, Volt/Var, Power-Flow Controllers, Energy Storage, Distributed Energy Resources, and Demand Response). Microgrids that operate and function as a grid resource.

**Potential Barriers:** Resources including significant labor and cost implications. Moving away from the traditional process that utilities use to determine rates. Supply chain is an ongoing issue with distribution transformers.



## Key Recommendation 7.0: Workforce

The federal government should invest in and promote education and workforce. Workforce and education are broad topics. Specialized training programs could start as early as high school and include cybersecurity topics. Inclusion of yearly certifications is encouraged.

When discussing IoT worker capabilities, there are many roles that are relevant, from designers to implementers to operations staff. For each role to be filled, the government can help foster collaboration about the necessary skills in each role and the knowledge needed to fulfill relevant tasks.

The federal government can help to develop targeted criteria and encourage expanded access to education and training opportunities. Agencies could help provide (or at least coordinate) means to assist learners through financial aid, scholarships, and online learning options. The U.S. can also encourage industry/academia partnerships as it has in other areas. This would help provide a focus on opportunities for existing workforce to adapt and better support digital transformation.

**Supporting Recommendation 7.1:** The federal government should consider “student loan forgiveness” programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies.

The federal government should consider “student loan forgiveness” programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies. These programs, analogous to the National Health Science Corps, provide expertise to municipalities, agencies and utilities, especially smaller ones, that can help them to adopt, and accelerate the implementation and execution of these “smart solutions”.

Many cities lack the type of digital talent that is critically needed to implement and operate advanced technology. Moreover, many small cities and rural areas face an exodus (or “brain drain”) of workers. Cities, in general, often find it difficult to attract sufficient digital talent at a scale that will have an impact. Federal agencies can help cities to leverage a similar model to that used by the National Health Science Corps. They can seek opportunities to partner with non-profit organizations (e.g., FUSE Corps) to find, attract, and hire talent.

**Implementation considerations:** Leverage the model used by the National Health Science Corps. These resources can work with non-profit organizations that support government agencies (e.g., FUSE Corps). Identification of specified work roles/skills needs (cybersecurity, data analytics, software development).

**Potential barriers:** For critical skills like cybersecurity and data science, it may still be hard to attract someone to this program since there is fierce competition from the private sector. There is a lack of sufficient numbers of certain skills, especially working with cybersecurity, AI, ML, etc. There may not be enough of these skill sets.

**Supporting Recommendation 7.2:** The federal government promote Continuing Education, Professional Development, and Vocational Training for IoT Integration in Supply Chain Management.

The recommendation to focus on education and workforce development, specifically geared toward the Internet of Things (IoT), is a response to the growing need for professionals adept in the design, implementation, and management of IoT systems within supply chain operations. This involves not just building knowledge in areas such as data science, analytics, data integration, and software development, but also developing a robust framework of continuing education, professional development, and vocational training. Such initiatives aim to equip businesses with a workforce capable of unlocking the full potential of IoT technologies.

The focus of these efforts should be a commitment to lifelong learning and continuous skills upgrade. This can be facilitated through various professional development opportunities such as workshops, online courses, and certification programs. These initiatives should be designed to help professionals stay current with the latest IoT trends and innovations, thereby promoting the adoption of new technologies in the supply chain sector. Vocational training programs, for instance, could provide hands-on experience in areas such as IoT device management, data analytics, and software development, thereby fostering technical proficiency.

Partnerships with industry stakeholders and technology providers are crucial. These partnerships can lead to internships, apprenticeships, and real-world projects, offering practical experience in IoT implementation. By focusing on these aspects of education and development, the government can create a pool of professionals who are not just knowledgeable but are also adaptable and up-to-date. This will ensure the workforce is well-equipped to navigate the complexities of IoT adoption, ultimately driving growth and competitiveness in the supply chain industry.

The justification for the recommendation to invest in education and workforce development in the context of IoT adoption in supply chain management lies in the need to prepare the workforce for the technological advancements and skills required in the rapidly evolving industry. The main reasons for this recommendation are:

- **Addressing Skills Gap:** The surge in IoT utilization in supply chain management will necessitate a workforce proficient in specialized areas such as data analytics, software development, and data integration. Investments in continuing education, professional development, and vocational training can bridge this gap, ensuring businesses have the skilled talent for effective IoT implementation.
- **Enhancing Competitiveness:** The competitiveness of the manufacturing sector hinges on a well-equipped workforce. Government investment in lifelong learning and skills development can bolster businesses' competitiveness, enabling them to maintain a robust global standing.
- **Fostering Innovation:** A workforce with deep-rooted IoT knowledge can spark innovation in supply chain management. Government-led educational and training programs can cultivate this innovative spirit, supporting the creation of avant-garde solutions.

- **Supporting Digital Transformation:** As the manufacturing sector undergoes digital transformation, there is a need to adapt operations to accommodate IoT and similar technologies. Education and workforce development investments can empower workers with the skills needed to support this transition, facilitating seamless integration of IoT in supply chains.
- **Encouraging Job Creation:** The integration of IoT in supply chain management can open new job avenues in areas like data analysis, software development, and cybersecurity. Government investment in education and workforce development can prepare workers for these opportunities, stimulating economic growth and job creation.
- **Promoting Social Inclusion:** Education and workforce development programs can enhance social inclusion, providing underrepresented groups with the necessary skills and training for the IoT-centric job market. This includes opportunities for professional development, vocational training, and continuous learning.
- **Ensuring Long-term Sustainability:** As the manufacturing sector evolves, businesses need to adapt to emerging technologies and industry trends. Government investment in education and workforce development can support the sector's long-term sustainability, assisting businesses in their ongoing IoT adoption and integration efforts.

**Implementation Considerations:** Agencies should consider the following implementation considerations for investing in education and workforce development for supply chain IoT adoption inclu:

- **Identifying Skill Requirements:** Carry out an exhaustive analysis to identify the specific skills and expertise required to support IoT integration in supply chain management. This includes technical proficiencies in data analytics, software development, and data integration, and managerial competencies.
- **Developing Targeted Curricula:** Partner with training providers, industry stakeholders, and educational institutions to create curricula and training programs that cater to these identified skills. These programs should focus on professional development and vocational training, promoting lifelong learning and adaptability in the IoT domain.
- **Expanding Access to Education and Training:** Implement policies and programs that ensure extensive access to continuing education and training focused on IoT. This should involve financial assistance, scholarships, and online learning options, making these resources accessible to a broad audience, including underserved communities.
- **Encouraging Industry-Academia Partnerships:** Foster relationships between industry and educational institutions that facilitate real-world learning experiences, internships, and collaborative research projects. These initiatives can enhance practical skills development and provide valuable industry exposure.
- **Focusing on Reskilling and Upskilling:** Launch initiatives to reskill and upskill the existing workforce, ensuring they can adapt to the evolving demands of IoT-driven supply chain management. This reinforces the importance of continuous professional development and staying current with the latest trends and innovations.
- **Promoting Vocational Training:** Encourage interest in vocational training in the fields of science, technology, engineering, and mathematics (STEM), focusing on the

development of IoT competencies within the existing workforce. This will lay the groundwork for future workforce development in the IoT field.

- **Establishing Performance Metrics:** Develop performance indicators and evaluation methods to assess the effectiveness of continuing education and professional development initiatives. This will enable data-driven improvements, ensuring these programs remain relevant and effective in meeting the demands of the IoT-centric job market.

**Potential barriers:** Impediments to implementing this recommendation include:

- **Insufficient Funding:** Limited resources may restrict the government's capacity to invest in continuing education, professional development, and vocational training programs at the necessary scale. This could impact the availability and accessibility of these programs for the workforce.
- **Resistance to Change:** Some industry stakeholders may be hesitant to invest in new training and professional development initiatives due to concerns about costs, time commitments, or disruption to existing workflows. This resistance could slow the pace of upskilling and reskilling efforts in the IoT field.
- **Difficulty in Identifying Skill Requirements:** The rapid evolution of technologies and market dynamics can pose challenges in accurately identifying the specific skills needed for successful IoT adoption in supply chain management. This could impact the design and relevance of continuing education and professional development programs.
- **Skills Mismatch:** A disparity between the skills imparted through vocational training and professional development programs and the skills demanded by the industry can limit the effectiveness of these initiatives. This mismatch could result in a workforce that is not fully equipped to navigate the complexities of IoT integration in supply chain operations.

**Supporting recommendation 7.3:** (proposed) The federal government should invest and promote education and workforce development in smart transportation technologies.

The federal government can also promote the concept of outcomes-based contracting in surface transportation for those entities and jurisdictions who have an existing workforce that are not familiar with these types of smart transportation technologies.

While workforce development and education are a broader topic across the IoT, there are specialized training/apprenticeship programs needed in the area of smart transportation. They could start as early as high school (and could also be summer intern programs) and need to include cybersecurity topics. The inclusion of yearly certifications on these is also encouraged.

The concept of outcomes-based contracting in surface transportation is also a viable solution for those entities and jurisdictions with an existing workforce that are not familiar with these smart transportation technologies but have transportation issues and problems that they need solved. When the focus of the contract is on results and outcomes, procurement officers and agency leaders can better design contracts that drive innovative, cost-effective services, reasonable risk-sharing, and measurable results.

**Implementation considerations:** For investing in education and workforce development include:

- Identifying skill requirements: Conduct a thorough analysis of the specific skills and expertise needed.
- Developing targeted curricula: Collaborate with educational institutions, industry stakeholders, and training providers to develop targeted curricula and training programs unique to the transportation sector.
- Expanding access to education and training: Implement policies and programs that ensure broad access to this and training, including financial aid, scholarships, and online learning options to reach underserved communities.
- Encouraging industry-academia partnerships: Promote partnerships between industry and educational institutions to facilitate real-world learning experiences, internships, and collaborative research projects.
- Focusing on reskilling and upskilling: Implement programs to reskill and upskill the existing workforce, enabling them to adapt to the changing requirements of the transportation sector.
- Establishing performance metrics: Develop performance metrics and evaluation methods to assess the effectiveness of education and workforce development initiatives and make data-driven improvements as needed.
- Outcomes-based Contracting: Outcomes-based Contracting is a form of contracting comprised of four discrete characteristics: Identification, Alignment, Measurement, and Adjustment.

**Potential barriers:** Possible barriers to implementing this recommendation include:

- Insufficient funding and resources: Limited resources may constrain the government's ability to invest in education and workforce development programs at the desired scale. Also, some state and local agencies may not have enough staff on hand.
- Resistance to change: Some industry stakeholders may resist investing in new training and education programs due to concerns about costs, time constraints, or disruption to existing processes. This is particularly relevant to those traffic engineers who have spent their entire career on replacing concrete and asphalt on roads and bridges.
- Difficulty in identifying skill requirements: Rapidly evolving technologies and market dynamics may make it challenging to accurately identify the specific skills needed. As these technologies become smarter and more digitized it will require more than one core skill set to operate and maintain installed transportation equipment.

- Skills mismatch: A mismatch between the skills taught in educational institutions and the skills required by industry can limit the effectiveness of education and workforce development initiatives.

**Supporting recommendation 7.4:** Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.

Education and training is needed to enhance the US workforce. There are increases in the understanding and safe use of IoT technologies. There is demand for a highly skilled workforce capable of addressing IoT privacy challenges. And boosting business, government, and consumer data trust will forge the adoption of IoT devices and services.

**Implementation considerations:**

- Defining the scope and content of educational initiatives
- Identifying key target audiences (schools, universities, businesses, general public)
- Collaborating with educational institutions and industry leaders
- Ensuring the relevancy and practicality of the educational content
- Regularly updating the initiatives to keep pace with technological changes
- Workforce development to encompass personas, including manufacturers, implementers, service providers, and workers

**Potential Barriers:** Difficulty in keeping up with the fast-paced advancements in IoT, challenges in reaching and engaging the targeted audiences, securing sufficient funding and resources.

**Supporting recommendation 7.5:** The federal government should develop and facilitate programs and grants to reskill existing workers, train future workers across manufacturing, construction, and clean technology / renewable industries.

IoT is a critical technology in renewable energy systems. This recommendation would leverage existing initiatives and programs that address workforce development. Federal considerations include the need to consider integration with existing workforce development programs and infrastructure.

**Implementation considerations:** Leverage existing initiatives and programs that address workforce development.

**Potential barriers:** Labor shortage in renewable and adjacent industries (manufacturing, construction) and lower wages in renewables than in other industries.

**[Editorial note: Preceding this section, there should be some introductory text that the remainder of the Key Recommendations are specifically those called out in the NDAA legislation, differentiating them from the above 7 Key Recommendations.]**

## Key Recommendation 8.0: Smart Traffic and Transit

[Key recommendation text is still being developed.]

**Supporting Recommendation 8.1:** The federal government should consider developing programs and grants to allow underserved and less developed communities as well as rural areas to adopt smart transportation technologies.

Doing so would help improve national accessibility to benefits from the adoption of IoT technologies that are not currently available to all citizens and municipalities. Government grants and programs targeted towards these areas could spur private investment in these areas, as well, further amplifying the economic and societal benefits that would result from such funding.

Funding opportunities for these underserved and rural communities will create jobs and promote economic growth. As digital technologies are adopted in these areas, they will require skilled workers to develop, implement, and maintain these systems. Financial incentives can help stimulate this job growth and support the development of a skilled workforce in the IoT sector. to adopt smart transportation technologies.

### Implementation Considerations

The government will need to identify appropriate tactics and methods, such as ADA-compliant EV Charging stations, adding EV-Ready language into building codes, small- disadvantaged business set asides, or Department of Transportation (DOT) Grand challenges as programs/grants are developed. Clear eligibility criteria should be established to ensure that these grants/incentives are targeted only at these types of communities and areas. The federal government should establish a system for monitoring and evaluating the effectiveness of these grants/incentives.

### Potential Barriers

Individuals that reside in these areas may not be fully aware of all the potential benefits that smart transportation technologies provide. Connectivity might be an issue in rural areas. Initial efforts may need to focus on those rural areas that already have some base level of connectivity. Other barriers include budget constraints, lack of political support, or concerns about market distortion. The federal government should address these concerns by demonstrating the potential economic and environmental benefits of IoT adoption in supply chains, leveraging public-private partnerships to share costs, and ensuring that the financial incentives are designed to minimize market distortions.

**Supporting Recommendation 8.2:** The Federal Government should provide overarching regulatory guidance for the drone industry. The Federal Government should also provide funding for the drone industry for additional research in order that existing technical obstacles can be overcome.

There are conflicting regulations that govern drones for recreational pilots versus those that govern drones for commercial pilots. The regulations that govern drones for commercial pilots are put forth by the Federal Aviation Administration (FAA) as they regulate that section of the airspace. Sometimes these regulations are mistakenly applied to recreational pilots. In some jurisdictions there is uncertainty over who regulates the airspace for recreational pilots (FAA versus Local Police).

In addition, there are commercial drone pilots that fly large aircraft in sections of the airspace that fall under Advanced Air Mobility (AAM) jurisdiction. Another issue facing the drone industry is Remote ID — a requirement for a drone to have an internal signal broadcasting the drone's location, latitude, longitude and heading. Not all drones currently have this requirement.

**Implementation Considerations:** It will be necessary to involve all stakeholders: drone equipment manufacturers, communications providers, among others need to be involved. This should be accompanied by expanding access to education and training: particularly on safety aspects related to drones.

**Potential Barriers:** Limited resources may constrain the government's ability to fund drone research. The drone industry is facing supply chain challenges. Drones approved by the Department of Defense (DoD) need to be on the Blue UAS Cleared Drone List. Drones on this list are validated as cyber-secure and safe to fly and are available for government purchase and operation.

Notes:

- Data/Privacy Framework is covered in Recommendation 1.
- Industry-led Standards for AVs are covered in Recommendation 2.
- Standards for interoperability and security are covered in Recommendation 2.
- Education and Workforce are covered in Recommendation 7.



## Key Recommendation 9.0: Augmented Logistics and Supply Chains

[Full recommendation still being developed.]

Note: IoT for Supply Chain is grouped into two segments: 1) the actual logistics of producing, transporting, and storing products (and providing services), and 2) the reliability and security of that chain of goods and services. Those segments are illustrated as “logistics” and “transparency” throughout Recommendation 9.

### Augmented Supply Chain Logistics

**Supporting Recommendation 9.1:** Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.

This federal IoT strategy would outline clear goals and objectives for IoT adoption in supply chain management and would encompass regulatory frameworks, infrastructure development, education, and incentives for implementation.

The justification for developing a national IoT strategy lies in the numerous benefits that IoT can bring to various industries, including supply chain management, as well as the overall economy and society. A comprehensive and coordinated national IoT strategy can help ensure that these benefits are fully realized and that potential challenges and risks are adequately addressed. Key benefits of an IoT supply chain logistics strategy include:

- **Economic growth and competitiveness:** A national IoT strategy for adoption in supply chain management can foster innovation, drive economic growth, and enhance the competitiveness of industries by promoting the widespread adoption and integration of IoT technologies. This can lead to increased productivity, reduced operational costs, and new business opportunities across various sectors.
- **Enhanced efficiency and resilience of supply chains:** IoT technologies can significantly improve supply chain efficiency, transparency, and resilience by enabling real-time monitoring, data-driven decision-making, and automation of processes. A national IoT strategy can provide guidance and support for businesses to adopt and integrate IoT solutions within their supply chains, thereby enhancing overall supply chain performance.
- **Job creation and workforce development:** The widespread adoption of IoT technologies will lead to the creation of new jobs and the need for skilled workers in areas such as data analytics, IoT device development, and cybersecurity. A national IoT strategy for adoption in supply chain management can help guide investments in education and workforce development to ensure that citizens are equipped with the necessary skills for the future IoT-driven job market.
- **Addressing cybersecurity and privacy concerns:** As IoT devices generate and process large amounts of data, there are inherent risks related to cybersecurity and data

privacy. A national IoT strategy for supply chain management can help establish guidelines, standards, and best practices for IoT security and data protection, ensuring that the risks are adequately addressed and managed.

- **Encouraging collaboration and standardization:** A national IoT strategy can promote collaboration among businesses, academia, and government agencies, fostering innovation and knowledge sharing. Furthermore, it can help drive the development and adoption of IoT standards for supply chain management, which are essential for interoperability, security, and scalability of IoT solutions.
- **Ensuring equitable access and benefits:** A national IoT strategy can ensure that the benefits of IoT technologies are distributed equitably across enterprises engaged in supply chain management, addressing potential digital divides and promoting inclusive growth.

**Implementation Considerations:** A comprehensive strategy should begin with engage with key stakeholders, including businesses, academia, and government agencies, to identify priorities, needs, and challenges related to IoT adoption in supply chain management. This collaboration will ensure the strategy is comprehensive, practical, and aligned with industry requirements.

Additional considerations include:

- **Focusing on key areas:** Prioritize areas within the supply chain where IoT can provide the most significant benefits and address the most pressing challenges, such as inventory management, transportation and logistics, and quality control.
- **Supporting innovation and R&D:** Foster innovation and R&D in IoT technologies by providing funding, incentives, and resources to businesses and research institutions. This will accelerate the development and commercialization of advanced IoT solutions tailored to supply chain management.
- **Developing standards and guidelines:** Establish standards and guidelines for IoT implementation in supply chain management, focusing on interoperability, security, and data privacy. This will facilitate seamless integration and adoption of IoT technologies across supply chains while addressing potential risks.
- **Promoting workforce development:** Invest in education and workforce development programs to ensure that workers have the necessary skills and expertise to thrive in an IoT-driven supply chain environment.
- **Encouraging public-private partnerships:** Foster collaboration between public and private sectors to promote IoT adoption in supply chain management, share knowledge, and address common challenges.

- **Monitoring progress and adapt:** Establish mechanisms to monitor and evaluate the progress of IoT adoption in supply chain management, and adapt the national strategy as needed based on emerging trends, technologies, and challenges.

**Potential barriers:** The following considerations represent barriers that would need to be addressed by those creating a supply chain logistics strategy:

- **Funding constraints:** Allocating sufficient funds to support IoT infrastructure, research and development, and workforce development initiatives can be a challenge, especially when competing with other national priorities.
- **Interagency coordination:** Developing a national IoT strategy requires close coordination among various federal agencies, which may have different goals, agendas, and regulatory frameworks. Ensuring a cohesive and consistent approach across agencies can be challenging.
- **Resistance to change:** Some stakeholders within the supply chain ecosystem may resist adopting IoT technologies due to concerns about job displacement, technological complexity, or fear of change. Overcoming this resistance requires effective communication, education, and change management strategies.
- **Cybersecurity and data privacy concerns:** Ensuring the security and privacy of the vast amounts of data generated by IoT devices is a significant challenge. Addressing these concerns requires investment in robust security measures and the development of comprehensive data protection policies and regulations.
- **Standardization and interoperability:** The IoT ecosystem consists of a wide variety of devices, platforms, and communication protocols. Developing and enforcing standards for interoperability can be a complex and time-consuming process, which may slow down the implementation of a national IoT strategy.
- **Skilled workforce shortage:** The rapid growth of IoT technologies and applications may outpace the availability of a skilled workforce in fields such as data analytics, IoT device development, and cybersecurity. Addressing this talent gap requires investments in education and workforce development programs.
- **Legal and regulatory barriers:** Existing laws and regulations may not adequately address the unique challenges posed by IoT technologies in supply chain management. Updating and harmonizing these legal and regulatory frameworks can be a complex and time-consuming process.
- **Balancing innovation and regulation:** Striking the right balance between promoting innovation and ensuring consumer protection, security, and privacy can be challenging. The federal government must carefully consider the potential trade-offs and unintended consequences of new regulations on IoT adoption and innovation.

**Supporting Recommendation 9.2:** Establish and provide financial incentives to encourage businesses to adopt IoT technologies in their supply chain operations by reducing the initial investment costs and perceived risks associated with the implementation of IoT solutions.

Financial incentives, such as tax breaks, grants, subsidies, or low-interest loans, can help lower the financial barriers for companies to experiment with and deploy IoT systems, leading to more widespread adoption and innovation in the sector. By offering financial support, the government can promote the development and integration of IoT solutions into supply chain management, enabling businesses to capitalize on the various benefits IoT offers, such as improved efficiency, transparency, and resilience. Furthermore, financial incentives can stimulate private sector investment, drive the growth of IoT technology providers, and foster an ecosystem that encourages collaboration and innovation within the industry.

It is crucial, however, for the government to carefully design and target these financial incentives, ensuring that they align with strategic objectives and deliver measurable impact. By doing so, the federal government can effectively drive IoT adoption in supply chain management, unlocking its full potential to transform the industry and strengthen national competitiveness.

Providing financial incentives would accelerate the adoption of IoT technology in supply chain management, particularly within the manufacturing sector. Financial incentives can lower the initial barriers to entry, making IoT adoption more feasible and attractive for businesses.

The main reasons for this recommendation are:

- **Encouraging investment:** Financial incentives, such as tax credits, grants, or low-interest loans, can help businesses offset the costs associated with implementing IoT solutions in their supply chains. This financial support can encourage companies to invest in IoT technology, even if they are initially hesitant due to the perceived risks or costs involved.
- **Stimulating innovation:** Financial incentives can spur innovation in the IoT space for supply chain management by providing companies with the resources they need to experiment with new technologies and solutions. This can lead to the development of new IoT applications and the refinement of existing ones, ultimately contributing to the overall competitiveness of the manufacturing sector.
- **Enhancing competitiveness:** By lowering the barriers to IoT adoption, financial incentives can help businesses in the manufacturing sector become more competitive on a global scale. Companies that leverage IoT technology can improve their supply chain efficiency, responsiveness, and resilience, allowing them to better compete with international rivals.
- **Creating jobs and economic growth:** The implementation of IoT technology in supply chains can lead to job creation and contribute to economic growth. As companies adopt

IoT solutions, they will require skilled workers to develop, implement, and maintain these systems. Financial incentives can help stimulate this job growth and support the development of a skilled workforce in the IoT sector.

- **Promoting sustainability:** IoT technology can contribute to more sustainable supply chain practices, such as reducing waste, conserving resources, and minimizing emissions. Financial incentives can encourage businesses to adopt IoT solutions that support these goals, ultimately promoting environmental sustainability and corporate social responsibility.

**Implementation Considerations:** Financial incentives for supply chain IoT adoption include the following:

- **Identifying appropriate incentives:** The federal government should assess the most effective financial incentives to promote IoT adoption in the supply chain, such as grants, tax credits, low-interest loans, or subsidies. This may involve consulting with industry experts, conducting cost benefit analyses, and evaluating the success of similar programs in other countries or sectors.
- **Defining eligibility criteria:** Clear eligibility criteria should be established to ensure that the financial incentives are targeted at companies that can benefit the most from IoT adoption across supply chains, such as small and medium-sized enterprises or businesses in critical industries. Criteria may include company size, revenue, industry sector, or proposed IoT projects.
- **Coordinating among federal agencies:** Federal agencies that may be impacted by this recommendation include the Department of Commerce, the Small Business Administration, and the Department of Energy. These agencies should coordinate their efforts to ensure efficient and effective implementation of the financial incentives program. Collaboration with state and local governments may also be necessary to align initiatives and maximize the impact.
- **Monitoring and evaluation:** The federal government should establish a system for monitoring and evaluating the effectiveness of the financial incentives program. This may include tracking key performance indicators, such as the number of IoT projects funded, the amount of private investment leveraged, and the impact on supply chain efficiency and sustainability. Periodic reviews should be conducted to assess the program's success and identify areas for improvement.
- **Addressing potential barriers:** Possible barriers to implementing this recommendation may include budget constraints, lack of political support, or concerns about market distortion. The federal government should address these concerns by demonstrating the potential economic and environmental benefits of IoT adoption in supply chains, leveraging public-private partnerships to share costs, and ensuring that the financial incentives are designed to minimize market distortions.

- **Raising awareness and providing technical assistance:** The federal government should consider implementing outreach campaigns to inform companies about the available financial incentives and the benefits of IoT adoption in supply chain management. Additionally, providing technical assistance to businesses in identifying, developing, and implementing IoT projects can help ensure the successful deployment of these technologies and maximize the impact of the financial incentives program.

**Potential barriers:** The following impediments may need to be addressed as part of this incentivization recommendation:

- **Budget constraints:** Limited budgetary resources can restrict the federal government's ability to allocate sufficient funds for financial incentives. This may result in a smaller or less comprehensive program, reducing its overall impact on IoT adoption. DRAFT – Supply Chain Logistics Recommendations
- **Political opposition:** Financial incentives may face opposition from certain political groups or stakeholders who argue against government intervention in the market or perceive the incentives as favoring specific industries or companies.
- **Bureaucratic hurdles:** The implementation of financial incentives may require collaboration and coordination among multiple federal agencies, which can introduce bureaucratic challenges and delays in rolling out the program.
- **Inefficient allocation of resources:** There is a risk that financial incentives may be allocated to businesses that do not use the funds effectively or do not fully commit to IoT adoption, leading to an inefficient use of government resources.
- **Market distortion:** Financial incentives may inadvertently create market distortions if they disproportionately benefit certain companies or industries, leading to an uneven playing field and potential resistance from competitors.
- **Difficulty in measuring impact:** Assessing the direct impact of financial incentives on IoT adoption in supply chains can be challenging, as multiple factors contribute to a company's decision to invest in new technologies. This may make it difficult for the federal government to demonstrate the effectiveness of the incentives program and justify its continued funding.
- **Lack of awareness:** Companies may not be aware of the available financial incentives or may not understand the potential benefits of IoT adoption in their supply chains, limiting the program's effectiveness in driving change.

**Supporting Recommendation 9.3:** Federal entities can also help 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.

Establishing and fostering public-private partnerships (PPPs) focused on IoT adoption aims to facilitate collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia. By creating a platform that encourages the exchange of ideas, resources, and expertise, PPPs can help to accelerate the development, deployment, and adoption of IoT technologies in supply chain management.

Public-private partnerships can play a pivotal role in overcoming common challenges associated with IoT adoption, such as the lack of infrastructure, technical knowledge, and financial resources. By pooling resources and aligning efforts, PPPs can enable the development of innovative IoT solutions, pilot projects, and proof-of-concept initiatives that demonstrate the value and benefits of IoT in supply chain operations.

Additionally, PPPs can support workforce development and training programs, ensuring that businesses have access to skilled professionals capable of implementing and managing IoT systems. They can also facilitate the creation of regulatory frameworks and standards, promoting a conducive environment for IoT adoption across the supply chain industry. To implement this recommendation, the government should actively engage with relevant stakeholders, identify shared goals and objectives, and establish mechanisms for ongoing collaboration and support. By fostering public-private partnerships focused on IoT adoption, the government can create a thriving ecosystem that drives innovation and competitiveness in the supply chain sector, ultimately realizing the full potential of IoT technologies.

**Implementation Considerations:** Considerations for fostering public-private partnerships for supply chain IoT adoption include:

- **Identifying key stakeholders:** The federal government should identify relevant private sector stakeholders, including businesses, industry associations, research institutions, and technology providers, who can contribute to the development and implementation of IoT solutions in supply chain management.
- **Establishing a collaborative framework:** A formal framework should be established to facilitate collaboration between the public and private sectors. This may include creating joint working groups, industry forums, or innovation hubs, where stakeholders can share ideas, knowledge, and resources.
- **Defining clear goals and objectives:** Public-private partnerships should have well-defined goals and objectives that align with the overall strategy for promoting IoT adoption in supply chain management. This will help ensure that all stakeholders are working towards a common vision and can measure their progress.
- **Developing joint projects and initiatives:** The federal government and private sector stakeholders should collaborate on joint projects and initiatives that address specific challenges or opportunities in supply chain management. These could include pilot projects, research and development programs, or the development of new IoT standards and protocols.

- **Ensuring effective communication and coordination:** Open and transparent communication between the public and private sectors is critical for successful collaboration. Regular meetings, progress reports, and information sharing mechanisms should be established to facilitate coordination and maintain momentum.
- **Monitoring and evaluation:** The federal government should establish a system for monitoring and evaluating the effectiveness of public-private partnerships in promoting IoT adoption in supply chain management. This may involve tracking key performance indicators, such as the number of joint projects implemented, the amount of private investment leveraged, and the impact on supply chain efficiency and resilience.

**Potential barriers:** Possible barriers to implementing this recommendation include:

- **Mistrust between public and private sectors:** A lack of trust between the government and private sector stakeholders can hinder collaboration and limit the effectiveness of public-private partnerships.
- **Differing priorities and objectives:** Public and private sector stakeholders may have different priorities, objectives, and timelines, which can create challenges in aligning their efforts.
- **Intellectual property and data privacy concerns:** Private sector stakeholders may be hesitant to share proprietary information or data with the government, hindering collaboration and knowledge sharing.
- **Limited resources:** Both the government and private sector organizations may face resource constraints that limit their ability to participate in public-private partnerships.

**Supporting Recommendation 9.4:** Promote international collaboration in IoT adoption across global supply chains to share knowledge, best practices, and resources between countries & regions, driving innovation & accelerating widespread adoption of IoT technologies in supply chain operations worldwide.

The recommendation to promote international collaboration in IoT adoption across global supply chains aims to facilitate the sharing of knowledge, best practices, and resources between countries and regions, driving innovation and accelerating the widespread adoption of IoT technologies in supply chain operations worldwide. By engaging in international collaboration, governments can foster a global ecosystem that supports the development and deployment of IoT solutions, overcoming challenges related to interoperability, standardization, and regulatory compliance.

Promoting international collaboration involves creating platforms and forums where policymakers, industry stakeholders, technology providers, and researchers from different countries can come together to exchange ideas, discuss common challenges, and explore opportunities for joint projects and initiatives. This can lead to the development of harmonized



regulations, standards, and guidelines that enable seamless integration of IoT systems across borders, fostering efficient and resilient global supply chain networks.

In addition, international collaboration can facilitate the pooling of resources and expertise to support research and development efforts, pilot projects, and capacity building initiatives aimed at promoting IoT adoption in supply chain management. This can help bridge the digital divide between developed and developing countries, ensuring that businesses worldwide have access to the tools and technologies needed to harness the potential of IoT in their supply chain operations.

To implement this recommendation, the government should actively engage with international partners, participate in relevant forums and organizations, and seek opportunities to collaborate on IoT-related projects and initiatives. By promoting international collaboration in IoT adoption across global supply chains, the government can contribute to the development of a connected and resilient global supply chain ecosystem that benefits businesses and consumers alike.

Promoting international collaboration in the context of IoT adoption in supply chain management is based upon the inherently global nature of supply chains and the need for a coordinated approach to address common challenges. The main reasons for promoting international collaboration are:

- Global nature of supply chains: Modern supply chains often involve multiple countries, making it essential for governments and organizations to collaborate across borders to ensure seamless, efficient, and secure operations.
- Harmonization of standards and regulations: International collaboration can help develop and promote the adoption of common standards, protocols, and regulations, which can reduce inconsistencies and friction between countries, making it easier for organizations to operate globally.
- Addressing global cyber threats: Cyber threats are not limited by geographical boundaries; therefore, international collaboration can enable the sharing of threat intelligence, best practices, and resources, improving collective defense against cyber attacks.
- Leveraging global expertise: Collaborating with international partners allows countries to benefit from the expertise, technologies, and best practices developed by others, leading to more effective and efficient IoT adoption in supply chain management.
- Fostering innovation: International collaboration can stimulate innovation by enabling the exchange of ideas, knowledge, and technologies among countries, research institutions, and businesses.
- Building trust: Working together on common challenges can help build trust between countries, which is crucial for the smooth functioning of global supply chains.

- Addressing social and environmental challenges: International collaboration can help address global social and environmental issues related to supply chain management, such as labor rights, environmental sustainability, and resource management.

**Implementation Considerations:** Implementation considerations for promoting international collaboration for supply chain include:

- Establish bilateral and multilateral agreements: Form strategic partnerships with key countries to facilitate collaboration on IoT-related supply chain initiatives, standards, and best practices.
- Participate in international forums and organizations: Engage in existing forums and organizations dedicated to supply chain management, IoT, and cybersecurity to contribute to and benefit from global discussions and initiatives.
- Share information and best practices: Promote the exchange of information, threat intelligence, and best practices related to IoT adoption and supply chain security among international partners.
- Collaborate on research and development: Engage in joint research and development projects with international partners to foster innovation and develop new technologies for supply chain management.
- Promote capacity building: Support capacity building initiatives and programs to help countries strengthen their IoT infrastructure, develop relevant skills, and improve supply chain management practices.
- Identify key international partners: Assess which countries are critical for collaboration based on their role in global supply chains, technological capabilities, and mutual strategic interests.
- Leverage existing diplomatic channels: Utilize existing diplomatic relationships to initiate dialogue and cooperation on IoT adoption in supply chain management.
- Coordinate with relevant federal agencies: Ensure that all relevant federal agencies are involved in the development and implementation of international collaboration initiatives.

**Potential barriers:** Possible barriers to implementing this recommendation include:

- Differing priorities and interests: Different countries may have varying priorities and interests, which could make it challenging to align objectives and collaborate effectively.
- Trust and data privacy concerns: Sharing sensitive information and best practices may be hindered by trust and data privacy concerns among collaborating countries.

- Regulatory and legal barriers: Differences in regulations, standards, and legal frameworks may impede collaboration efforts and create challenges in harmonizing policies.

**Supporting Recommendation 9.5:** The government should provide an intentional process to 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.

By regularly monitoring and evaluating the progress of IoT implementation, the government can identify areas of improvement, assess the impact of its policies and initiatives, and make informed decisions to optimize its strategies and investments in the future. Monitoring and evaluating progress involves establishing a set of measurable indicators and targets that reflect the key objectives and desired outcomes of IoT adoption in supply chain management. These indicators may include the level of IoT technology adoption, efficiency gains, cost reductions, improvements in transparency and traceability, and advancements in cybersecurity, among others.

To implement this recommendation, the government should develop a comprehensive framework for data collection, analysis, and reporting, which includes input from industry stakeholders, technology providers, and relevant government agencies. Regular assessments should be conducted to track the progress of IoT adoption against the established targets, identify any gaps or challenges, and evaluate the effectiveness of the implemented policies and initiatives. Based on the findings of these assessments, the government should adapt its strategies and actions to address the identified issues, optimize resource allocation, and maximize the impact of its efforts. By monitoring and evaluating progress, the government can ensure that its approach to driving IoT adoption in supply chain management remains agile, responsive, and results-oriented, ultimately contributing to the long-term success and competitiveness of the industry.

The need to monitor and evaluate progress in IoT adoption for supply chain management stems from the need to ensure the effectiveness of implemented strategies, measure their impact, and identify areas for improvement. Regular monitoring and evaluation are crucial for several reasons:

- **Assess effectiveness:** Monitoring and evaluation help determine whether the implemented strategies and policies are achieving their intended goals and objectives.
- **Measure impact:** Assessing the impact of IoT adoption in supply chain management is essential to understand the benefits, such as efficiency improvements, cost savings, and enhanced resilience.
- **Identify areas for improvement:** By evaluating progress, the government can identify weaknesses or gaps in the implementation of IoT adoption strategies, enabling targeted improvements and adjustments to ensure better outcomes.

- **Allocate resources efficiently:** Monitoring and evaluation provide insights into the effectiveness of various initiatives, helping the government make informed decisions on resource allocation and prioritize investments in areas with the most significant potential impact.
- **Enhance accountability:** Regular assessment of progress helps ensure transparency and accountability for the government and other stakeholders involved in IoT adoption and supply chain management.
- **Facilitate knowledge sharing:** Monitoring and evaluating progress can generate valuable knowledge and insights that can be shared with other stakeholders, helping to improve practices and drive further innovation in the field.
- **Inform future strategies:** The insights gained from monitoring and evaluating progress can inform the development of future policies and strategies, ensuring they are more effective and better aligned with the evolving needs of supply chain management.

**Implementation Considerations:** Implementation considerations for monitoring and evaluating progress for supply chain include:

- **Establish clear goals and objectives:** Define specific, measurable, and time-bound goals and objectives for IoT adoption in supply chain management to enable effective monitoring and evaluation.
- **Develop relevant performance indicators:** Identify key performance indicators (KPIs) that reflect the desired outcomes of IoT adoption and can be used to measure progress and impact.
- **Implement data collection and reporting mechanisms:** Set up systems and processes for collecting, storing, and analyzing data related to IoT adoption and supply chain performance.
- **Conduct periodic assessments:** Schedule regular evaluations of progress and impact, using the collected data and KPIs to assess the effectiveness of IoT initiatives in supply chain management.
- **Foster a culture of continuous improvement:** Encourage feedback and learning from monitoring and evaluation results, using the insights to improve and refine policies and initiatives.
- **Collaborate with stakeholders:** Engage with industry, academia, and other relevant stakeholders to gather their insights and perspectives, ensuring a comprehensive understanding of progress and challenges

- **Assign responsibility:** Designate a lead federal agency or interagency group responsible for overseeing the monitoring and evaluation process for IoT adoption in supply chain management.
- **Develop a monitoring and evaluation plan:** Create a detailed plan outlining the goals, objectives, KPIs, data collection methods, and evaluation schedule.
- **Allocate resources:** Ensure adequate financial, human, and technical resources are allocated to support monitoring and evaluation activities.

**Potential barriers:** Possible barriers to implementing this recommendation include:

- **Lack of clear goals and objectives:** Ambiguous or poorly defined goals can make it difficult to assess progress and impact.
- **Inadequate data collection and reporting mechanisms:** Ineffective systems for collecting, storing, and analyzing data can hinder accurate and reliable monitoring and evaluation.
- **Resource constraints:** Limited resources can impede the government's ability to conduct thorough and consistent monitoring and evaluation.
- **Resistance to change:** Stakeholders may resist sharing information or adopting new practices based on evaluation results, limiting the impact of monitoring and evaluation efforts.

**Supporting Recommendation 9.6:** The federal government should select the most appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic IoT manufacturing supply chain.

These policies, incentives, and requirements are particularly relevant in the transportation sector as that becomes increasingly connected, electric, shared, integrated, seamless, and ultimately autonomous. Rapid advances in transportation technologies are already occurring that are further augmented by several communication and information technologies, including the Internet of Things (IoT). In addition, the sector is becoming increasingly electrified.

The recommendations in this section can apply to all aspects of domestic IoT manufacturing. American manufacturers share the goal of fostering and strengthening domestic manufacturing and supply chain capabilities. With the recent influx of federal funding and executive orders in this sector, there is an increasing trend to support the “Buy American” concept.

The justification for an appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic manufacturing supply chain market is provided below:

- Absent significant time to build new manufacturing capacity, develop new supply chains, and train workers, tighter domestic preference requirements could create supply constraints and prevent the manufacturers from meeting even modest deployment goals.
- In some cases, U.S. manufacturing capacity cannot meet increased demand that would be sparked by anticipated federal investment/incentives let alone current domestic demand.
- In some cases, there are no domestic alternatives for components and subcomponents, limiting the ability of equipment providers to control their domestic content. US Manufacturers cannot force their component and subcomponent suppliers to relocate facilities to the U.S.
- Compliance with federal domestic preference requirements is time consuming and costly particularly when it comes to the country of origin of components and subcomponents. This burden will increase as subcomponents become smaller and more integrated.

**Implementation Considerations:** Methods for fostering and strengthening domestic manufacturing and supply chain capabilities include:

- Phasing in domestic content requirements. An extended phase in period is necessary in order to avoid supply shortages and provide domestic manufacturers and their suppliers with sufficient time to develop domestic manufacturing capabilities, build up supply chains, and train their workforce.
- Accelerate domestic manufacturing with an investment tax credit for associated capital costs.
- Provide clear rules governing domestic content requirements, including guidelines on how they apply across all funding and procurement programs. Further, this guidance should also be provided to implementing state agencies.
- Avoid any rules that require determining the country of origin of subcomponents integrated into larger domestically manufactured components.
- The component test should include all costs associated with the manufacturing of a product, such as labor, transportation, allocable overhead, and material. And clearly designate that the domestic labor used in the final assembly of a product is included in the component test.
- Allow 100% of manufacture value added (MVA) or substantial transformation to be classified as domestic content in component tests.

- Countries should be designated outside of the US from which materials and components can be procured and the component test for products substantially transformed in one of these acceptable countries can be waived. These could be countries that the US already has established trade agreements with such as: USMCA (United States-Mexico-Canada Agreement) countries, European Union member states, The United Kingdom, and Indo-Pacific

**Potential barriers:** Impediments to implementing this recommendation include:

- Current Supply Chain constraints meeting domestic content requirements - while there are a number of North American manufacturing plants for EV components particularly batteries being developed and constructed, there is a ramp up time to get to full production.
- Funding constraints: There is a huge initial capital cost investment to build up new domestic manufacturing plants.
- Resource constraints: There will need to be an influx of skilled engineers and technicians to support this domestic buildup.

## Smart Supply Chain Traceability

**Supporting Recommendation 9.7:** The government should promote the development and use of standards for supply chain logistics, traceability, and assurance.

This is foundational to changing supply chain behavior. The objective is to enable and accelerate IoT adoption using IoT technology and standards to improve supply chain logistics, traceability, and assurance of IoT products & services.

### Description

The federal government should promote standards and protocols for supply chain logistics, traceability, and assurance. Collaboration with Standards Development Organizations (SDOs) and international allies can ensure manufacturers produce assured and traceable products. Incentives should encourage suppliers to establish unique corporate, product, asset, and part IDs linked to a digital thread for improved supply chain efficiency, transparency, resilience, and security. Additionally, supporting industry-led initiatives and education campaigns for IoT standards and protocols will drive adoption, minimize risk, and maximize economic value. These standards will ensure interoperability, reliability, and security across IoT-enabled supply chains, benefiting businesses and users.

### Detailed Description

The federal government should foster the development, adoption, and use of standards and protocols for supply chain logistics, traceability, and assurance. It should collaborate with Standards Development Organizations (SDOs) and international allies to promote assured & traceable products by manufacturers for efficient, reliable, and secure supply of goods. It should incentivize suppliers to establish unique corporate IDs, product IDs, asset IDs, and part IDs linked to a digital thread of information and data, that are used to track and trace goods while improving supply chain efficiency, transparency, resilience, and security.

Additionally, the federal government should also support industry-led initiatives and education campaigns to foster the development and adoption of IoT standards and protocols for supply chain management, traceability, and enablement of economic value. These standards should best enable interoperability, reliability, and security across IoT-enhanced supply chains, facilitating data exchange, decision-making and services. By creating and promoting such standards, the government can drive widespread adoption of IoT technology, minimize supply chain risk, and maximize economic value to businesses and users.

### Justification

1. Interoperability: Standards are vital for integrating IoT technologies into complex supply chains, where multiple stakeholders and systems are involved. It ensures seamless communication and collaboration between IoT devices, systems, and platforms from different manufacturers.



2. Scalability: Standardization facilitates the scalability of IoT implementations by providing consistent protocols and guidelines. This allows businesses to easily add new devices and expand their IoT networks, reducing the risk of incompatibilities and simplifying the integration of new components.
3. Innovation and competition: Standards and protocols drive innovation and competition by leveling the playing field for businesses and developers, of any size or market share. This fosters the creation of new products and services adhering to established standards, benefiting consumers and the entire industry.
4. Cybersecurity and data privacy: Industry standards for cybersecurity and data privacy can help mitigate risks related to IoT, such as cyber threats and data privacy issues. They establish robust protocols and guidelines, fostering consumer trust and driving the adoption of IoT technologies in the supply chain.
5. Simplified integration and maintenance: Industry standards and protocols streamline the process of integrating IoT technologies into existing systems and processes, reducing the time and resources required for implementation, making systems easier to maintain and troubleshoot in the field.
6. Cost savings: Standardization saves costs for businesses by reducing the need for customized solutions and simplifying procurement. It also drives economies of scale, allowing for more efficient production of standardized components and devices, resulting in lower costs for manufacturers and end-users.
7. Regulatory compliance: Standards and protocols provide a foundation for government regulations and policies on IoT and supply chain management. They promote adherence to best practices for security, privacy, and environmental impact, enhancing the security, stability, and sustainability of IoT ecosystems.
8. National Security: Identifier standards used to improve visibility and transparency of products in the supply chain can reduce the risk of counterfeit or tampered goods used in critical sectors, as well as ensure the authenticity and integrity of IoT systems, parts, or any goods or services being tracked.
9. Public Health and Safety: Standards for fast identification and recall of products posing functional safety, cybersecurity, privacy, concerns are key. Consumers demand greater visibility, transparency, and accountability of detailed information on the origin and custody of goods, from development through delivery and use.
10. Sustainability and Economic Growth: Use of standard identifiers provides better traceability in the supply chain, from raw materials all the way to recycling or disposal by facilitating tracking of goods, reducing waste. They also enable the creation of a digital thread of data which can drive economic value.

## Implementation Considerations

1. Encourage Inclusiveness: Involve a diverse range of businesses, technology providers, academia, and government agencies, in the development of standards that align the interests of many stakeholders.
2. Prioritize critical areas: Focus on the critical aspects of supply chain management where standardization can yield significant benefits, such as data exchange, device interoperability, security, and privacy.
3. Build on existing standards: Leverage industry standards and best practices as a starting point and adapt or expand upon them as necessary to address the specific requirements of supply chain management. Identify where gaps exist, and standards are not available and whether new standards are needed.
4. Encourage flexibility and adaptability: Design standards and protocols that are flexible and can be easily updated to accommodate new technologies, emerging threats, and evolving industry needs.
5. Promote adoption: Encourage and incentivize businesses to adopt the established standards and protocols through government adoption, contract flow-down, education, outreach, and support programs.
6. Ensure compliance: Develop mechanisms to monitor and enforce compliance with the established standards and protocols, including certifications, audits, and penalties for non-compliance.
7. Foster Global Collaboration: develop programs that incentivize suppliers to adopt global identifier methods based on standards for supply chains with an emphasis on electronics and IoT.
8. Promote Use of Identifiers: Encourage suppliers to establish unique corporate IDs, product IDs, asset IDs, and part IDs to drive consistency, interoperability, and trustworthiness in any supply chain.
9. Speed Adoption of Identifiers: Facilitate the adoption of identifiers through incentives, education, and outreach programs. Promote linking Identifiers to IoT cybersecurity labeling programs for consumers and industrial IoT.
10. Improve Supply Chain Systems: Create incentives to upgrade existing supply chain management systems to include global identifier standards that ensure seamless tracking and tracing.

## Potential implementation barriers

1. Resistance to standardization: Some businesses and stakeholders may resist standardization efforts due to concerns about the potential loss of competitive advantage, customization capabilities, or intellectual property rights.
2. Fragmentation Challenges: The IoT landscape and supply chains are highly fragmented, with numerous vendors, platforms, and technologies and types of stakeholders, suppliers, manufacturers, and distributors. Achieving consensus and collaboration among all stakeholders can be challenging.
3. Cost and resource constraints: Developing and implementing industry standards and protocols can be resource-intensive, requiring significant investments in time, money, and expertise.
4. Rapid technological advancements: The IoT field is rapidly evolving, making it difficult to keep standards and protocols up-to-date and relevant. The rapid growth of AI will make it even more complex.
5. Technical Implementation Challenges: Suppliers may view implementation of Identifier infrastructure as burdensome and expensive and may be reluctant to invest time and money into adopting new standards, especially if they lack the resources and expertise.
6. International Harmonization Challenges: 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 (selectively share) the Identifiers and related information across borders.

## Federal considerations

1. Engage and support Standards Development Organizations (SDOs) and their committees working with industry and academia to create standards for supply chain logistics, traceability, and assurance.
2. Provide a regulatory framework for developing catalogs and taxonomy of supply chain standards that supports standardization efforts while promoting innovation and competition.
3. Collaborate with international allies to ensure that the standards and protocols are globally relevant and can be harmonized with international guidelines while being consistent with U.S. trade policy goals.
4. Offer financial and technical support to businesses, particularly small and medium-sized enterprises, to help them adopt and comply with the established standards and protocols.

5. Monitor and evaluate the effectiveness of the standards and protocols over time and adjust as needed to address emerging challenges and opportunities.
6. Prioritize the protection of sensitive information and ensure the security and reliability of databases used to manage the identifiers and related information.
7. Encourage the use of Global Identifier Standards (such as GLS of GS1) in procurement contracts and regulatory frameworks and track goods and info related to assets and data, to optimize risk, cost, benefits, and value.

**Supporting recommendation 9.8:** Agencies should support creation of cryptographically strong architectures and infrastructure that enable supply provenance, traceability, and lifecycle management by linking HBOM, SBOM to the design & manufacturing processes and data into a foundation of trust enabling IoT services.

### **Description**

The federal government should incentivize suppliers to develop trusted architectures for supply chain logistics, provenance, traceability, assurance of supply and IoT lifecycle management. By cryptographically linking SBOM to trusted HBOM<sup>2</sup> in any IoT device or system, industries can help mitigate the risks associated with supply chain security, compromised components, and ensure the security and reliability of critical systems. This will provide benefits for national security, public safety, and economic stability, making it a valuable investment for the government and society.

### **Justification**

1. The use of trusted architectures for supply chain provenance and traceability can help mitigate the risks associated with vulnerabilities or compromised components.
2. 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.
3. 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.
4. Cryptographic linking of SBOM to trusted HBOM enhances supply chain security, visibility, chain of custody and product lifecycle management. (and overall user confidence).

---

<sup>2</sup> Trusted HBOM includes Root of Trust with a source of Entropy such as PUF or TRNG for security and unique ID.

## Implementation Considerations

1. Educate stakeholders in the value chain on the benefits of using trusted architectures for supply chain provenance and traceability.
2. Promote industry adoption of trusted architectures through education and outreach. Incentivize hardware suppliers to develop trusted architectures that enable supply chain provenance and traceability.
3. Develop guidelines for how the trusted architectures should be implemented by linking HBOM and SBOM with DBOM<sup>3</sup> to facilitate provenance and traceability and encourage the adoption of standards and best practices.
4. Foster collaboration between government agencies and industry stakeholders (Private-Public Partnerships) to develop and promote trusted architectures that support secure protocols for provisioning and market access.

## Potential Implementation Barriers

1. Lack of awareness or understanding of the benefits of trusted architectures.
2. Resistance from industry stakeholders who are not interested in investing in new technologies. (or are considering competing technologies).
3. Implementation costs associated with developing and deploying new systems.
4. Technical challenges associated with integrating new systems with existing infrastructure.
5. Complexities involved in developing and deploying trusted architectures at scale.

**Supporting Recommendation 9.9:** The government should establish incentives for industries to adopt capabilities for tracing design, manufacturing, and supply chain workflows that cryptographically link parts, personas, and data to deliver traceable products and IoT systems that function as originally intended.

## Description

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. Classic supply chains focus on resilience and Availability. IoT Systems also require Confidentiality and Integrity and Assurance (CIA, as

---

<sup>3</sup> Digital Bill of Materials consisting of HBOM, SBOM and other info related to quality, reliability and workflow process.

defined in ISO/IEC 27002). The term “trusted” refers to whether IoT Systems and their parts operate as intended and whether any data they produce is not compromised or tampered with.

### **Justification**

1. Ensure the confidentiality and integrity of IoT electronics supply chains to prevent cyber-attacks in critical infrastructure and protect against human and economic losses.
2. 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.
3. Enable companies and businesses to foster innovation, create a competitive advantage with smart-secure-connected electronics IoT Systems and become smart-connected-secure suppliers.
4. Enable the creation of trusted ecosystems that accelerate end-to-end innovation, monetization, and growth of IoT-enabled digital economies.

### **Implementation Considerations**

1. Offer tax credits, grants, or other financial incentives to companies that market electronics products with traceable parts Country of Diffusion and Country of Origin<sup>4</sup>, provenance, and journey in the supply chain.
2. Require contractors and suppliers to adhere to specific security and traceability standards when bidding on government contracts, particularly for critical infrastructure.
3. Establish a certification process for connected electronics and IoT products that meet security and traceability standards to improve trust in the supply chain, possibly linked to cybersecurity labels.
4. Engage industry associations and other stakeholders to develop best practices and guidelines for secure connected electronics and IoT systems development and supply chain management.

### **Barriers**

1. Lack of awareness or expertise: Some companies may not be aware of traceability benefits, or the risks associated with lack of it. SMBs may lack the expertise to implement traceability methods effectively.

---

<sup>4</sup> Country of Diffusion where a part is fabricated and Country of Origin where the product made of parts is assembled.

2. Limited supply chain visibility: In some cases, it may be difficult to trace components back to their original source due to limited information or visibility into the supply chain.
3. 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.
4. 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 Considerations**

1. Provide financial incentives to companies to encourage the adoption of trusted traceability methods aligned with executive orders and broader government priorities.
2. Work with industry stakeholders to offer tax credits, grants, or other financial incentives to companies that offer traceable connected electronics products.
3. Incentivize contractors and suppliers to adhere to specific security and traceability standards when bidding on government contracts for critical infrastructure.
4. Promote partnerships of industry associations and stakeholders to identify potential gaps in the connected electronics supply chain and develop targeted solutions to address them.

**Supporting Recommendation 9.10:** As foundations of trust evolve and IoT devices are deployed, get connected to networks, and used in the field, the government should promote traceable and interoperable IoT ecosystems across value chains amongst devices, personas, and infrastructure.

### **Description**

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**

1. Trusted network ecosystems facilitate information sharing, innovation, data protection, international cooperation, and international trade.
2. They improve the security and resilience of critical infrastructure with information sharing, analytics, and feedback for digital twins.

3. They enable trusted data exchanges and protect against malicious attacks and data breaches.
4. They help manage threats and mitigate risks and consequences, economic, reputational and loss of life.

### **Implementation Considerations**

1. Drive awareness on how security and trust is established in IoT networks among devices, personas and applications operating in connected IoT environments.
2. Work with industry stakeholders to develop and promote standards, guidelines, and interoperability programs to ensure that devices and networks can communicate securely and reliably.
3. 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 IoT security.

### **Potential Implementation Barriers**

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

### **Federal Considerations**

1. Work with industry stakeholders to develop guidelines for trusted IoT network ecosystems and provide financial incentives to companies to encourage their adoption.
2. Promote the adoption of workflows, IoT technologies, and solutions that improve the security and resilience of critical infrastructure, especially for federal agencies.
3. Develop a comprehensive strategy for promoting the security of IoT devices and networks and invest in infrastructure to accelerate adoption of secure IoT solutions.
4. Collaborate with international partners to promote and harmonize global standards and best practices for securing IoT devices and networks.



**Supporting Recommendation 9.11:** Promote the use of digital threads among enterprises in disaggregated supply chains, to enable the creation of connected IoT value chains. Leverage digital threads of data across value chains to enable marketplaces of trusted data producers and data consumers.

### **Description**

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 Bills of Materials (DBOM, HBOM, SBOM) to identifiers and data to create trusted digital threads that can enable marketplaces of data producers and data consumers platforms. Business platforms for data exchange can have a significant impact on improving supply chain visibility, innovation, efficiency, security, and economic growth. Digital threads may extend from supply chains to the field use of IoT devices and connected ecosystems of data marketplaces.

### **Justification**

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

### **Implementation Considerations**

1. Develop educational and training programs to help businesses implement digital threads. Establish guidelines for creating a digital thread, including standards for selective data sharing and security.
2. Incentivize companies to digitalize their workflows through tax credits, grants, or subsidies for investing in digital technologies. Encourage collaboration among industry and government agencies on best practices.
3. Leverage the Cybersecurity labeling program to create a digital trail of Bills of Materials (DBOM, HBOM, SBOM, Security keys, certificates etc.) for IoT systems that will vary by vertical market.

4. Provide funding for research and development of methods and standards to facilitate development of best practices and guidelines for implementing digital threads.

### **Potential Implementation Barriers**

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

### **Federal Considerations**

1. 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.
2. 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.
3. Promote the adoption of digital threads in procurement contracts (e.g., DBOM linked to HBOM/SBOM) and foster PPPs that enable and promote supply chain traceability linked to security.

**Supporting Recommendation 9.12:** As digital threads and data platforms emerge, the government should incentivize the enablement and use of data marketplaces to increase visibility and economic growth with data enabled services while protecting proprietary IP and PII of stakeholders.

### **Description**

The government should incentivize the enablement and use of trusted data marketplaces where data producers and consumers query and share information about data, enabling better visibility, traceability, and monetization while protecting proprietary IP and PII. Trusted data marketplaces can be enabled through incentives such as tax credits or subsidies for companies that develop platforms for data exchange, or IoT services that establish market preference or regulated market access & use of goods. Platforms facilitate adoption of data marketplaces can help data producers and consumers reduce lifecycle costs, improve efficiency by streamlining processes and eliminate redundancies, especially in complex supply chains where information flows are often fragmented or disconnected.

## **Justification**

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

## **Implementation Considerations**

1. Identify suitable marketplaces to incentivize and support (e.g., EV charging and monetization). Develop guidelines and incentives for access and use of data in the marketplace.
2. Promote the benefits of data marketplaces to potential participants and provide tax credits and subsidies to encourage participation.
3. Ensure data security and confidentiality measures are in place. Monitor and evaluate the effectiveness of the data marketplaces. Use analytics to improve visibility, traceability, efficiency, and cost.

## **Potential Implementation Barriers**

1. Lack of awareness about the benefits of marketplace platforms. Concerns and resistance over data security and confidentiality
2. Difficulty in regulating and monitoring access and use of data in the marketplace. Unwillingness to share proprietary data without a license.
3. Lack of open and participatory business platforms for data marketplaces that can evolve over time as more business discover the value of digitalization.

## **Federal Considerations**

1. Implement data privacy and confidentiality regulations based on experience (GDPR, CDPP, etc.). Develop policies to prevent monopolies in the data marketplace.

2. 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.
3. Balance incentives for participation with data security, and confidentiality concerns so that enterprises are incentivized to join data marketplaces and grow their business.
4. Coordinate with other federal agencies and international allies to ensure a cohesive approach. Align with broader government efforts to promote open innovation platforms.

**Supporting Recommendation 9.13:** The government should encourage Private-Public partnerships to finance a unified infrastructure for the digitalization of enterprise business processes including design, production, procurement, distribution, etc. to accelerate adoption of digital threads.

### **Description**

The digitalization of all business functions (design, production, marketing, procurement, distribution, etc.) enables more efficient IoT product 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 impact in improving 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 in any value chains which will drive economic growth.

### **Justification**

1. Digitalization of business functions leads to greater management, efficiency, and visibility in supply chains.
2. Cryptographic methods improve security, reliability, and integrity of digital data, especially in hand-offs.
3. Digitalization enables secure ecosystems, opportunities for businesses/workers and economic growth.
4. Financing a digitalization infrastructure can increase adoption among stakeholders in IoT value chains.
5. Digitalization of value chains enhances security, reliability, and integrity of data for the digital economy.

### **Implementation Considerations**

1. Develop and communicate clear guidelines and criteria for eligibility for the subsidies.

2. Incentivize PPPs to work on Proof of Concept (PoC) pilot projects before investing to deploy at scale.
3. Create a streamlined application and approval process for businesses to apply for the subsidies.
4. Ensure that the funds are accessible to businesses of all sizes and types in the IoT value chain.
5. Monitor the effectiveness of the funds to ensure that they are achieving the intended outcomes.
6. Provide incentives for businesses to invest in digitalization and adopt digital technologies and tools.
7. Encourage collaboration and knowledge sharing among businesses to promote best practices.

### **Potential Implementation Barriers**

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

### **Federal Considerations**

1. Ensure that any funds for digitalization align with broader federal priorities and goals, such as promoting economic growth and national security.
2. 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.
3. Monitor and evaluate the impact of the subsidies in IoT value chains and digital economies.
4. Encourage equitable access to digital technologies and tools across different regions and industries and ensure that digitalization efforts prioritize security and privacy matters.

**Supporting Recommendation 9.14:** To speed up the creation of connected value chains the government should promote PPPs that facilitate the adoption of end-to-end digital threads using consistent digitalization methods capturing receivables, processes, and certified deliverables.

### **Description**

The federal government can accelerate the creation of traceable supply chains by encouraging orchestration of connected Private-Public Partnerships (PPPs) among stakeholders across complex value chains who maintain Trust through collaboration and accountability by digitalizing portions of supply chains piecemeal using consistent methods of “receivables-process-deliverables”. This can help supply chain stakeholders to have PPPs collaborating in parallel to accelerate adoption of digital threads and become more efficient which will help businesses to grow new data-enabled revenue streams on top of IoT products and services that will fuel economic growth.

### **Justification**

1. Orchestrated PPPs can accelerate the adoption of end-to-end digital thread and traceability in complex supply chains, by digitalizing portions of supply chains piecemeal in parallel using consistent methods.
2. Collaboration and accountability among enterprises in IoT value chains can create resilient and secure supply chains that can help businesses drive economic growth.
3. Traceability can help businesses reduce risk, increase resilience, and protect against supply chain risks of vulnerabilities, intrusions, and adversaries, which can lead to business and economic growth.
4. Ensure that IoT supply chain infrastructure is secure, transparent, and trustworthy. Drive shared monetization among stakeholders leveraging fintech to enable scalable economics.

### **Implementation Considerations**

1. Encourage orchestration of connected Private-Public Partnerships (PPPs) across complex value chains, by providing incentives for businesses to adopt transparent workflow practices and engage in PoCs.
2. Promote consistent digitalization methods for "receivables-process-deliverables" across supply chains by digitalizing portions of supply chains piecemeal to facilitate collaboration among stakeholders.
3. Fund the development of digital infrastructure, training programs, and other resources necessary for successful partnership implementation. All requirements are equal responsibility of all PPP stakeholders.

4. Create taxonomy of entities in market-specific supply chains that can be orchestrated to maintain trust through collaboration, guidelines, and standards among connected stakeholders.

### **Potential Implementation Barriers**

1. Resistance to change from supply chain stakeholders who are accustomed to traditional methods and may be hesitant to share or exchange data with competitors in the value chain.
2. Limited awareness about the benefits, or lack of technical expertise, or capacity to join PPPs, or costs associated with implementing digitalization methods across enterprises in the supply chain.
3. Lack of awareness about the importance of trustworthy and secure supply chains and resource constraints for smaller businesses that may not have the capacity to participate in partnerships.
4. Difficulty in creating a taxonomy of enterprises in supply chains orchestrating and coordinating multiple stakeholders across fragmented supply chains.

### **Federal Considerations**

1. Prioritize PPPs that promote transparency, efficiency, and security and ensure that any incentives align with established guidelines and standards and not unfairly disadvantage SMBs or create monopolies.
2. Foster collaboration among federal agencies, industries, and value chains to accelerate adoption with a unified approach to IoT supply chain security and transparency.
3. Consider the potential impact on domestic and international trade policies and the importance of ensuring that any subsidies are distributed equitably across various stakeholders.

**Supporting Recommendation 9.15:** As digital threads drive growth of data among marketplaces, policies will be needed regarding data privacy, confidentiality, ownership, control, management, access, licensing, and trust for data use in applications, to minimize security risks and maximize economic value.

### **Description**

Monetization of data will require infrastructure for Security, Privacy, Data Sharing, Ownership plus Control Frameworks for Identity and Access management (IAM), Data Protection, Sharing and Exchange, Data Analytics and 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 they can fuel synergistic ecosystems and the future digital economies.

### **Justification**

1. Data policies can have a major impact on privacy, security, interoperability, transparency, accountability, innovation, and monetization.
2. A lack of clear and consistent data policies can create uncertainty and hinder the growth of digital economies. The right data strategy can drive business growth and fuel synergistic ecosystems.
3. Data requires infrastructure for data security, confidentiality, sharing, ownership, control, licensing, identity & access management (IAM), and analytics to minimize risks and maximize economic value.
4. Anonymization of collected data is essential for privacy, critical infrastructure, safety initiatives, threat minimization and operation of smart cities, roads, and transportation.

### **Implementation Considerations**

1. 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.
2. Establish policies related to trusted data that need to be created and enforced to ensure compliance with regulatory requirements.
3. Promote essential requirements and guidelines for data privacy, confidentiality and anonymization.
4. 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**

1. 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 related to privacy and security.
2. The lack of clear and consistent data policies can create uncertainty and hinder the adoption by businesses and workers as well as the growth of digital economies.
3. The cost of establishing infrastructure for data security, privacy, sharing, and exchange, as well as data analytics with AI, may be significant.



4. Developing data policies that balance privacy and security concerns with innovation and economic growth can be challenging.

### **Federal Considerations**

1. Consider the 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.
2. Create policies that should promote interoperability to enable data sharing across different systems and corporations. Consider the impact of such policies on SMBs.
3. Promote collaboration and information sharing among federal agencies and industry partners to improve data policies and infrastructure.

**Supporting Recommendation 9.16:** As data produced in supply chains and during field use becomes the “new gold”, the government should raise awareness about the value of data marketplaces and incentivize the creation business ecosystems and data-driven networks of products, businesses, and value chains.

### **Description**

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 that can leverage synergies to enhance existing products and services, will accelerate creation of new revenue streams and enable digital twins.

### **Justification**

1. 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.
2. Data analytics can provide insights that drive innovation, improve decision-making, and enable data monetization strategies. This can lead to significant benefits and economic growth.
3. Trusted data marketplaces can promote data sharing and collaboration. Data-driven business ecosystems can lead to new revenue streams and enhanced products and services.

4. 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.
5. Data regulations can provide a framework for businesses to manage and use data responsibly and using tools for monitoring and managing data marketplaces can ensure transparency and accountability.

### **Implementation Considerations**

1. Develop educational programs for businesses and individuals. Raise awareness about data-driven business ecosystems through public campaigns, conferences, and workshops.
2. Provide funding and incentives for data-driven ecosystem and solutions PPPs with industry leaders, innovative startups, and academic institutions.
3. Foster the development of platform-based business ecosystems by providing incentives and resources to businesses.
4. Encourage collaboration and innovation among businesses by promoting network effects. Provide tools and resources for monitoring and managing data marketplaces.

### **Potential Implementation Barriers**

1. Lack of awareness and understanding about data-driven business ecosystems and platforms.
2. Limited resources and expertise for implementing data monetization strategies from data analytics.
3. Lack of national strategy to enable the creation of platform-based ecosystems and balance the benefits of data-driven businesses and marketplaces with data privacy and security concerns.

### **Federal Considerations**

1. Ensure fair competition and prevent monopolies. Balance the need for data confidentiality and security with the benefits and value of data-driven business ecosystems for data management and sharing.
2. Encourage the private sector to invest in data-driven economic growth. Promote collaboration between government, industry, and academia. Promote collaboration businesses while ensuring fair competition.

3. Ensure transparency and visibility in data marketplaces by encouraging the use of data analytics to improve government operations and services.
4. Address the digital divide to ensure that all businesses have access to the resources and tools needed to participate in data-driven business ecosystems.

**Supporting Recommendation 9.17:** Considering the rapid growth of AI, the federal government should assess the supply chain risks of intrusions and attacks as well as opportunities to speed up adoption, as AI will have profound impact risk management, security, resilience, and economic growth.

### **Description**

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**

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

### **Implementation Considerations**

1. Promote how to leverage AI and IoT technologies to create end-to-end supply chain visibility and traceability.
2. 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.

3. Companies can use AI-powered predictive analytics to anticipate supply chain disruptions and take proactive measures to mitigate them.
4. The government can work with industry stakeholders and global allies to develop AI-specific security standards, best practices and regulations for the use of AI to create SBOMs used in critical infrastructure.
5. AI systems used in critical infrastructure should be subject to rigorous testing and evaluation to identify potential vulnerabilities and ensure they are secure.
6. The government should provide funding and resources for research into AI security and develop tools to detect and respond to AI-powered attacks.

### **Potential Implementation Barriers**

1. The rapid evolution of AI technology makes it difficult to keep pace with emerging threats and vulnerabilities.
2. Lack of data quality regarding the accuracy and completeness of supply chain data can be a challenge, making it difficult for AI algorithms to provide reliable insights.
3. Sharing supply chain data with third-party AI vendors can raise concerns about data privacy and security. Regulating AI for SBOM at an international level is a critical consideration.
4. Implementing AI-powered supply chain traceability requires significant technical expertise and resources and there are challenges associated with securing AI systems.
5. 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 considerations**

1. 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.
2. 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.
3. The government should promote international collaboration on AI-powered supply chain traceability to help establish global standards and best practices.
4. The government should work with industry stakeholders to develop standards and best practices for securing AI systems used in critical infrastructure.

5. The government should promote collaboration and information sharing among federal agencies and industry partners to improve AI security.

## Key Recommendation 10.0: Precision Agriculture

Develop a comprehensive national strategy for agricultural IoT to establish a clear vision and roadmap for the integration of IoT in agriculture, addressing current challenges, fostering innovation, and promoting long-term sustainability and competitiveness of the agricultural sector.

As IoT technologies continue to advance, their adoption in agriculture can significantly enhance productivity, resource efficiency, and environmental sustainability. However, without a cohesive national strategy, the potential benefits of agricultural IoT may be hindered by fragmented initiatives, limited interoperability, and a lack of clear direction. This strategy should be developed in collaboration with stakeholders, such as farmers, technology providers, industry experts, and research institutions, to ensure broad consensus and commitment to its implementation.

The Federal government should identify and prioritize the most pressing challenges faced by the agricultural sector that can be addressed through the use of IoT technologies, such as water management, pest control, and labor shortages. The government should develop specific goals, timelines, and milestones for the integration of IoT in agriculture, ensuring alignment with broader national objectives related to food security, environmental sustainability, and economic growth. This could be accomplished by establishing an interagency task force to oversee the development and implementation of the national strategy, involving relevant agencies such as the USDA, FCC, and DOE.

**Supplemental Recommendation 10.1:** The federal government should consider subsidizing the use of IoT in farms.

The federal government should consider programs to help growers and producers adopt IoT technologies. This should include subsidies around connectivity, sensors, and digital applications. The programs could be similar to other subsidies that the USDA has for farmers around agricultural inputs or climate smart agriculture. The use of IoT in agriculture will benefit all stakeholders, including the farmer, the policy makers, the agricultural companies, and the consumer.

The upfront cost of IoT typically limits the adoption of data-driven agriculture, and the farmers who may have the most need may be the ones least likely to take advantage of digital technology. Federal subsidies can help scale the technology, which will drive down costs for all, and could help marginalized farmers and smallholder farmers who might need more help to leverage technology.

**Implementation Considerations:** Developing an approach to IoT subsidization could involve a public / private / academic partnership and leveraging the knowledge and capabilities of Agricultural Extension centers. Particular attention should be paid to defining approaches that will enable marginalized and smallholder farmers to leverage available subsidies to deploy and benefit from IoT technology.

**Potential Barriers:** There is limited expertise in the market and industry, meaning resources and expertise may be difficult to secure.

**Supplemental Recommendation 10.2:** : The federal government should consider fully funding the deployment of a “farm of the future” setup in every land grant university nationwide. This nationwide test-farm IoT network should span different forms of agriculture, including, but not limited to broadacre, horticulture, livestock, and aquaculture.

The proposed initiative advocates for the federal government to allocate sufficient funding to implement a "farm of the future" setup in all land grant universities across the United States, providing a showcase for farmers in the region on how to collect and analyze data from their farms.

The data collected by the IoT network could be used to develop and refine machine learning algorithms, which could help farmers predict future crop yields and identify potential issues before they occur. (Note: That data might also be housed and shared through data repositories described in other recommendations.)

The nationwide "farm of the future" IoT network would enable universities to share data and insights with each other more easily, fostering a collaborative approach to agriculture.

The implementation of a nationwide IoT network in land grant universities could help to advance research and development in agriculture, leading to the creation of new technologies and practices that could benefit farmers and consumers alike.

It is difficult to specify what IoT technologies should be acceptable to be used. Some concrete and specific IoT applications should be defined for inclusion in the project and funding requirements, based on project types.

**Implementation Considerations:** “Farm of the Future” efforts should look to assist in determining what IoT technologies should be acceptable to be used. Some concrete and specific IT applications should be defined for inclusion in the project and funding requirements, based on project types. This may require coordination with other federal agencies in alignment with their objectives. Different land grant universities might pose different challenges with respect to implementation, including connectivity, tech readiness, etc. It is important to include every university, including the HBCUs.

**Potential Barriers:** Project owners may have limited IoT awareness and knowledge, and there may be limited expertise and resources available in the marketplace to support IoT in the projects. Given the large number of land grant universities and the cost of agricultural equipment (e.g., connected combines, aquaculture systems), significant funding will be needed.

**Supporting recommendation 10.3:** The federal government should actively promote and support the adoption of Generative AI applications for agricultural IoT, with the aim of improving



decision-making, optimizing resource utilization, and enhancing productivity in the agricultural sector through innovative and data-driven solutions.

Generative AI applications have the potential to revolutionize the way farmers analyze and use the data collected from IoT devices in agriculture. By leveraging advanced algorithms and machine learning techniques, Generative AI can enable farmers to identify patterns, optimize resource allocation, and make better informed decisions. This will result in benefits for various stakeholders, including farmers, policy makers, agricultural companies, and consumers.

Federal stakeholders could establish a public-private-academia partnership that would define specific agriculture applications (e.g., yield prediction, pest and disease management, irrigation scheduling, supply chain optimization) that might benefit from AI. Agencies could support the partnership through financial incentives and subsidies, and through formal promotion of education and training opportunities (perhaps in concert with other workforce efforts described.)

**Implementation Considerations:** Define specific agricultural applications: Consider specific use cases for Generative AI in agriculture, such as

- **Yield prediction:** Generative AI can analyze historical and real-time data from IoT devices to predict crop yields more accurately, helping farmers to make better informed decisions regarding planting, harvesting, and marketing.
- **Pest and disease management:** Generative AI can use data collected from IoT sensors to identify patterns in pest and disease occurrences, enabling farmers to adopt targeted and timely interventions for prevention and control
- **Irrigation scheduling:** Generative AI can optimize irrigation schedules by analyzing data from IoT devices such as soil moisture sensors, weather stations, and satellite imagery, ensuring efficient water use and reducing water waste.
- **Supply chain optimization:** Generative AI can analyze data from IoT devices throughout the supply chain to optimize logistics, reduce food waste, and increase overall efficiency.

Provide incentives or subsidies to facilitate the adoption and integration of Generative AI applications by farmers and agricultural businesses. These incentives could include tax breaks, grants, or low-interest loans to help offset the upfront costs associated with implementing Generative AI solutions.

Create educational programs and resources to help farmers and agricultural professionals understand the benefits of Generative AI technology and how to effectively implement and use these applications. This can be achieved through collaborations with Ag Extension Centers, universities, and industry experts. Offer workshops, webinars, and online courses to ensure widespread access to knowledge and training opportunities.

**Potential Barriers:** Limited expertise and understanding of Generative AI technology may hinder widespread adoption. Additionally, effective collaboration between multiple agencies, stakeholders, and the private sector will be necessary to ensure successful implementation. Ensuring data privacy and security, as well as addressing any potential ethical concerns related to the use of AI in agriculture, will also be crucial factors to consider. Furthermore, the integration of Generative AI applications with existing agricultural IoT systems may require significant technical and operational adjustments.

## Key Recommendation 11.0: Environmental Monitoring

[Key recommendation text is still being developed.]

**Supplemental Recommendation 11.1:** The federal government should establish or encourage IoT environmental data repositories in support of open, available data. Promoting the open availability of data would promote research, improve transparency, and encourage proactive improvement by industry participants.

As described in other recommendations throughout this report, improved interoperability and competitiveness will help benefit all IoT adopters, and an open model for shared and consistent data will help take strides toward those objectives.

**Implementation Considerations:** The Department of Energy's Energy Information Administration (EIA) sharing of data (e.g., power plants) could be used as a possible implementation template. Data sharing protocols should avoid differences in post processing. Data sharing may need to be incentivized.

**Potential Barriers:** There may be significant variations in data quality and challenges with harmonization. There may be privacy concerns associated with some data, and companies may be resistance to sharing data for proprietary reasons.

**Supplemental Recommendation 11.2:** The federal government should facilitate and support the research, development and deployment of low cost air quality sensors. (Could we expand to additional types of monitoring?)

The Board observed that there is a need to shift from expensive (i.e., highly sensitive regulatory grade) sensors that limit deployment by organizations and municipalities. While such sensors are vital for particular monitoring purposes, large scale deployment of these types of monitoring equipment would be expensive and difficult.

Encouraging development and implementation of local, scalable air quality monitoring would support a variety of use cases, including:

- Increasing public awareness of air quality conditions;
- Informing environment and public policy, including through real-time testing and demonstration of policy impacts;
- Environmental justice work;
- Supplementing regulatory grade sensing with IoT commercial sensors;
- Public health research;
- Construction site emissions monitoring; and,

- Rapid or emergency air quality monitoring for particular circumstances.

Currently, regulatory monitoring is often limited to a few pollutants; the government can encourage expanded coverage of other emerging chemicals of concern (including greenhouse gasses) in monitoring and sensing systems.

**Implementation Considerations:** Agencies should encourage automated and consistent measurement and can facilitate research in low-cost sensing technologies for criterial pollutants. This effort should focus on

- **Measurements:** facilitate research in low-cost sensing technologies for criterial pollutants, such optical particle scanning for particulate matter and M0x elements for gasses, as well as detection of emerging chemicals of concern.
- **Correlation:** facilitate and support research and a program in correlating regulatory grade data with low cost AQ data
- **Expansion:** facilitate the expansion of wireless connectivity to support remote monitoring and sensing in areas not serviced by traditional connectivity (TV white space, satellite, etc.)

The government should facilitate the expansion of wireless connectivity to support remote monitoring and sensing in areas not serviced by traditional connectivity. This recommendation supports (and is supported by) those described in Recommendation 4.

**Potential Barriers:** Regulatory monitoring spans multiple agencies, from the federal and state to county levels. Different monitoring regimes often operate with different calibration protocols. In addition there may be both funding and resource constraints, as well as legal barriers to be addressed

## Key Recommendation 12.0: Public Safety

[Key and supporting recommendation text are still being developed.]

**Supporting Recommendation 12.1:** The federal government should create a stockpile of public safety IoT devices that is available for immediate access.

The federal government should create a stockpile of public safety IoT devices that are finite in type and need but contains a medley of manufacturers to choose from rather than a single or a couple of manufacturers from which stockpiles are sourced. Stewards could refresh the stockpile per labeling requirements and best use-by date.

The safety and wellbeing of each and every citizen, including their ability to live in safe environments and conditions, is paramount and vital. Having a stockpile of certified and approved devices to be used by law enforcement, EMS, fire, and rescue will enable public safety officials to arrive at scenes of crime and disasters armed with devices that interoperate, can be shared/exchanged while on duty, and enable ease-of-use.

**Implementation Considerations:** Similar to the Department of Health and Human Services (DHHS) stockpiles of vaccines, personal protective equipment (PPE), etc., we recommend the US government add public safety devices to their procurement list. Initial and ongoing funding is needed along with cooperation from manufacturers who wish to participate in the stockpile program develop APIs and interoperability to other competing and complementary devices.

**Potential Barriers:** Lack of funding and resources needed to manage an additional set of assets found in stockpile.

Note: Implementation and adoption of interoperable data standards for public safety IoT is addressed in Recommendation 2.6.

## Key Recommendation 13.0: Health Care

[Key and recommendation text is still being developed.]

**Supporting Recommendation 13.1:** (Under Review) Raise Priority for IoMT to Healthcare Facilities' Executive Leadership Teams

IoMT should be equivalent in priority for all healthcare stakeholders as is IT infrastructure, cybersecurity posture, or applications. IoMTs monitor, detect, inform, and deliver therapies to patients, therefore, they deserve just as much attention and call out as cloud services, for example. Currently IoMTs are ignored by healthcare IT organizations, as the responsibility to make decisions and/or purchase the devices is owned by the biomedical engineering department. IoMTs may not undergo strict infrastructure, privacy, and security guidelines as to large capital equipment investments such as MRI scanners.

**Implementation Considerations:** None identified.

**Potential Barriers:** None Identified.

Note: Data exchange for Internet of Medical Things (IoMT) is #2.7.

## Key Recommendation 14.0: International Considerations

[Key and recommendation text is still being developed.]

**Supporting recommendation 14.1:** The IoTAB strongly supports the voluntary public/private partnership that created the US Cyber Trust Mark.

<https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/>

The U.S. Department of State must be committed to supporting the FCC, NIST, the Departments of Homeland Security and Energy, the IoT Federal Working Group, and industry to identify and engage allies and partners toward harmonizing standards and pursuing mutual recognition of the US Cyber Trust Mark and similar labeling efforts.

**Supporting recommendation 14.2:** The government should create internationally compatible data minimization guidance related to IoT devices, aligning with the NIST Privacy Framework and NIST Cybersecurity Framework principles.

Data minimization processes (related to both collection and retention of sensitive data) reduce potential harm from data breaches or unauthorized access. Data minimization is inherently supportive of Privacy By Design. Implementation of these processes, and reduced risk that would result, may boost consumer trust by ensuring data is only used for necessary purposes. Consistent processes (supported by international agreement) would also help establish uniform data privacy standards globally.

The government should collaborate with public sector, private sector, and international counterparts to develop universally acceptable guidance on data minimization that would be tailored to various IoT applications.

**Implementation considerations:** Those working to foster international agreement on data minimization should recognize that the resulting processes should not hinder innovation or competitiveness in the IoT industry. This will be a delicate balance that may require a long-term commitment to advocacy since international agreements often require considerable time and negotiation. Principles of this guidance would be considered in future international agreements.

**Potential barriers:** Differences in privacy laws and cultural attitudes towards privacy in different countries will represent a challenge to achieving international agreements. There may also be significant resistance from companies that rely on extensive data collection.

## 10. Conclusion

- A concluding statement from the report that summarizes the work and the findings and that encourages continued progress from the Board.
- A cordial invitation for follow-up questions, if needed and as permitted by the FACA process.
- Thank you to the IoT Advisory Board members for their contributions and support.



## 11. References

Specific documents cited in the report (end notes) (standards, guidelines, policies) (with hyperlinks).

The following **international** data transfer agreements may have an impact on IoT:

Global Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR)

Canada, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America are current economies participating in the APEC CBPR System

<https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border> [commerce.gov]

EU-U.S. Data Privacy Framework (EU-U.S. DPF) - Privacy Shield Replacement

<https://www.commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data> [commerce.gov]

US & UK Data Bridge (Added to the Privacy Shield Replacement)

<https://www.commerce.gov/news/press-releases/2023/06/us-uk-joint-statement-us-uk-data-bridge> [commerce.gov]

## 12. Acknowledgements

This section will acknowledge the work of groups or individuals (outside of the Board itself, which is listed elsewhere) who have contributed to the project. Such contributions include support for meetings, useful discussions, or extensive copy-editing of the publication.

**Include speakers with links to meeting materials**

## 13. Appendices

- Other selected industry references (standards, guidelines, corporate reports) considered during discussions and for recommendations.
- Other Federal regulations and statutes affecting IoT
- Summaries of other federal reports supporting IoT improvement / actions
- Glossary of Selected Terms
- Abbreviations / Acronyms
- Other ideas?

## 14. Compliance Matrix

The IoTAB fulfills the role of the “steering committee” as established under subsection (b)(5)(A) of the NDAA Section. It supports the IoTFWG which is the working group convened under subsection (b)(1).

The IoTAB herein advises working group in the following areas:

Advisory Topic	Relevant Report Sections
(i) the identification of any Federal regulations, statutes, grant practices, programs, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development of the Internet of Things;	
(ii) situations in which the use of the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States, including benefits from or to	
(I) smart traffic and transit technologies;	
(II) augmented logistics and supply chains;	
(III) sustainable infrastructure;	
(IV) precision agriculture;	
(V) environmental monitoring;	
(VI) public safety; and	
(VII) health care;	
(iii) whether adequate spectrum is available to support the growing Internet of Things and what legal or regulatory barriers may exist to providing any spectrum needed in the future;	
(iv) policies, programs, or multi-stakeholder activities that—	
(I) promote or are related to the privacy of individuals who use or are affected by the Internet of Things;	

Advisory Topic	Relevant Report Sections
(II) may enhance the security of the Internet of Things, including the security of critical infrastructure;	
(III) may protect users of the Internet of Things; and	
(IV) may encourage coordination among Federal agencies with jurisdiction over the Internet of Things;	
(v) the opportunities and challenges associated with the use of Internet of Things technology by small businesses; and	
(vi) any international proceeding, international negotiation, or other international matter affecting the Internet of Things to which the United States is or should be a party.	

[To be added before submission: The IoTAB is pleased to provide this report within the one year timeframe specified within the section. It represents independent advice (as specified in the NDAA) and represents the independent judgement of the steering committee, each member of which is acting as a stakeholder outside of the Federal Government with expertise relating to the Internet of Things.]