Infrastructure	Secondary category	Rec #	Enhance and modernize infrastructure supporting IoT	
		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.	
	supply chain	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.	
	transportation	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).	
	transportation	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).	
	sustainable infrastructure	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
	Trust, US Leadership, Sustainable infrastructure	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.	
	Public Safety	Supporting Recommendation 2.6	Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT.	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.
	healthcare, adoption	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.	Issues: Recommendation should focus on data interoperability as a goal, rather than data exchange standards as the means to that goal
		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.	
		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.	
	Government	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.	
	, Government	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.
		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.	Issues: Government doesn't usually play a role in harmonizing standards; possibly should be broader than satellite communications;
				Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 4.
Trust	**Secondary category**	**Rec #**	**Create trust in IoT**	
	Infrastructure?	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.	
	, Infrastructure, US Leadership	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.	
	, Infrastructure	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.	
	Adoption	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.	
	, Infrastructure, US Leadership	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.	
	Infrastructure	Supporting recommendation 1.6	The government can encourage and foster data policies that drive economic growth, such as through this framework.	
	Infrastructure	Key Recommendation 3.0	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.	
		Key Recommendation 5.0	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.	
		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.	
	US leadership (if rec adds on fund research in PETs)	Supporting recommendation 5.2	Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.	
		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.	
Adoption	**Secondary category**	**Rec #**	**Facilitate industry adoption (including govt, small business adoption) and value realization of IoT.**	

		Supporting Recommendation 3.1	The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.	
		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.	
		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.	
		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.	
		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.	Issues: May need to be reconciled or combined with 10.4.
		Supporting Recommendation 6.2	The federal government should consider new models for sustaining and support in considering project feasibility.	
		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.	Issues: May need to be reconciled or combined with 6.1.
		Supporting Recommendation 6.7	The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility.	Maybe missing: SUS-R06: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.
	sustainable infrastructure, transportation	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.	
	transportation	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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
		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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
	supply chain	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.	
	Sustainable infrastructure	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.	
Workforce	**Secondary category**	**Rec #**	**Develop, grow, and maintain a workforce to support the IoT economy**	
		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.	
	Adoption, sustainable infrastructure	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.	
	Adoption, supply chain	Supporting Recommendation 7.2	(Updated) The federal government promote Continuing Education, Professional Development, and Vocational Training for IoT Integration in Supply Chain Management.	
	Transportation	Supporting recommendation 7.3	(proposed) The federal government should invest and promote education and workforce development in smart transportation technologies.	
	Trust	Supporting recommendation 7.4	Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.	
		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.	
International	**Secondary category**	**Rec #**	**Address challenges of IoT in a global ecosystem and economy**	

	Adoption, supply chain	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.	
	Trust	Supporting Recommendation 14.1	(Proposed) The IoTAB strongly supports the voluntary public/private partnership that created the US Cyber Trust Mark.	
	Trust	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.	
Supply Chain	**Secondary category**	**Rec #**	**Ensure IoT supply chain integrity and resilience**	
		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.	
		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.	
	infrastructure	Supporting Recommendation 9.7	The government should promote the development and use of standards for supply chain logistics, traceability, and assurance.	
	infrastructure, trust	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.	
	trust	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.	
Government	**Secondary category**	**Rec #**	**Develop government capability to support and sustain a IoT economy**	
		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.	From May: Issues: More information is needed to resolve the relationship of sustainable infrastructure to critical infrastructure and smart cities.
		Supporting Recommendation 3.7	(Under Review?) The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.	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.
	, US Leadership	Supporting Recommendation 6.3	The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.	
	, US Leadership	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.	
	Adoption, sustainable infrastructure	Supporting Recommendation 6.5	The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).	
US tech leadership	**Secondary category**	**Rec #**	**Facilitate US IoT technology and innovation leadership**	
		Supporting Recommendation 3.5	The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.	
Policy goals	**Secondary category**	**Rec #**	**Align federal actions in IoT to advance policy goals**	
Sustainable infrastructure				
	Adoption?	Supporting Recommendation 6.8	The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models.	Issues: This recommendation has some overlap with Recommendation 2.4.
		Supporting recommendation 6.10	Accelerate the promotion and adoption of procedures and methods to make the electric grid more reliable and resilient.	
Traffic and transport				
		Key Recommendation 8.0	[Smart Traffic/Transit recommendation text is still being developed.]	
Precision ag				
	Government	Supporting Recommendation 10.0	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.	
			Issues: This recommendation needs refinement. While it is too generic, it could perhaps be combined with similar recommendations from other subgroups;	
			Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 6.	
	adoption	Supplemental Recommendation 10.1	The federal government should consider subsidizing the use of IoT in farms.	
			Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 1.	
	adoption	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.	

			Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 2.	
	government	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.	
			Issues: Concerns regarding privacy, maturity of the AI technology; premature for government to “promote” use of this technology	
			Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 5.	
Environmental monitoring				
		Key Recommendation 11.0	[Key recommendation text for environmental monitoring is still being developed.]	
	adoption, government	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.	
	adoption, government	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?)	
Public Safety				
		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.	
Healthcare				
		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	
			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.	
	trust	Supporting Recommendation: NEW	This was discussed in May but not included herein: 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.	

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Trust	Infrastructure?	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.
Trust	, Infrastructure, US Leadership	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.
Trust	, Infrastructure	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.
Trust	Adoption	Supporting Recommendation 1.3	Conformance to any specific set of requirements should be voluntary.
Trust		Supporting recommendation 1.4	(Under review) The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations.
Trust	, Infrastructure, US Leadership	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.
Trust	Infrastructure	Supporting recommendation 1.6	The government can encourage and foster data policies that drive economic growth, such as through this framework.
Infrastructure		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.
Infrastructure	supply chain	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.
Infrastructure	transportation	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).

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Infrastructure	transportation	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).
Infrastructure	sustainable infrastructure	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
Infrastructure	Trust, US Leadership, Sustainable infrastructure	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.
Infrastructure	Public Safety	Supporting Recommendation 2.6	Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT. 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.
Infrastructure?	healthcare, adoption	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. Issues: Recommendation should focus on data interoperability as a goal, rather than data exchange standards as the means to that goal
Trust	Infrastructure	Key Recommendation 3.0	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.
Adoption		Supporting Recommendation 3.1	The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.
Supply Chain		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.

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Adoption		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.
Adoption		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.
US Leadership		Supporting Recommendation 3.5	The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.
Government		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. From May: Issues: More information is needed to resolve the relationship of sustainable infrastructure to critical infrastructure and smart cities.
Government		Supporting Recommendation 3.7	(Under Review?) The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience. 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.
Infrastructure		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.
Infrastructure		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.
Infrastructure	Government	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.

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Infrastructure	, Government	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.
Infrastructure		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. Issues: Government doesn't usually play a role in harmonizing standards; possibly should be broader than satellite communications; Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 4.
Trust		Key Recommendation 5.0	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.
Trust		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.
Trust	US leadership (if rec adds on fund research in PETs)	Supporting recommendation 5.2	Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.
Trust		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.
Adoption		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.
Adoption		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. Issues: May need to be reconciled or combined with 10.4.
Adoption		Supporting Recommendation 6.2	The federal government should consider new models for sustaining and support in considering project feasibility.
Government	, US Leadership	Supporting Recommendation 6.3	The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.
Government	, US Leadership	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.

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Government	Adoption, sustainable infrastructure	Supporting Recommendation 6.5	The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).
Adoption		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. Issues: May need to be reconciled or combined with 6.1.
Adoption		Supporting Recommendation 6.7	The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility. Maybe missing: SUS-R06: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.
Sustainable infrastructure	Adoption?	Supporting Recommendation 6.8	The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models. Issues: This recommendation has some overlap with Recommendation 2.4.
Adoption	Sustainable infrastructure	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.
Sustainable infrastructure		Supporting recommendation 6.10	Accelerate the promotion and adoption of procedures and methods to make the electric grid more reliable and resilient.
Workforce		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.
Workforce	Adoption, sustainable infrastructure	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.
Workforce	Adoption, supply chain	Supporting Recommendation 7.2	(Updated) The federal government promote Continuing Education, Professional Development, and Vocational Training for IoT Integration in Supply Chain Management.
Workforce	Transportation	Supporting recommendation 7.3	(proposed) The federal government should invest and promote education and workforce development in smart transportation technologies.
Workforce	Trust	Supporting recommendation 7.4	Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.
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.
Traffic and transportation		Key Recommendation 8.0	[Smart Traffic/Transit recommendation text is still being developed.]

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Adoption	sustainable infrastructure, transportation	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.
Adoption	transportation	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.
Supply Chain		Key Recommendation 9.0	[Full recommendation for supply chain still being developed.]
Supply Chain		Supporting Recommendation 9.1	Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.
Adoption	supply chain	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.
Adoption	supply chain	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.
International	Adoption, supply chain	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.
Adoption	supply chain	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.
Adoption	supply chain	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.
Supply Chain	infrastructure	Supporting Recommendation 9.7	The government should promote the development and use of standards for supply chain logistics, traceability, and assurance.
supply chain	infrastructure, trust	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.
Adoption	supply chain	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.
Adoption		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.

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Adoption	supply chain	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.
Adoption	supply chain	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.
Adoption	supply chain	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.
Adoption	supply chain	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.
Adoption	supply chain	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.
Adoption	supply chain	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.
Supply Chain	trust	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.
Precision ag	Government	Supporting Recommendation 10.0	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. Issues: This recommendation needs refinement. While it is too generic, it could perhaps be combined with similar recommendations from other subgroups; Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 6.
Precision ag	adoption	Supplemental Recommendation 10.1	The federal government should consider subsidizing the use of IoT in farms. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 1.
Precision ag	adoption	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. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 2.

Theme (primary)	Theme (secondary)	Recommendation #	Recommendation Description
Precision ag	government	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. Issues: Concerns regarding privacy, maturity of the AI technology; premature for government to “promote” use of this technology Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 5.
Environmental Monitoring		Key Recommendation 11.0	[Key recommendation text for environmental monitoring is still being developed.]
Environmental Monitoring	adoption, government	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.
Environmental Monitoring	adoption, government	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?)
?		Key Recommendation 12.0	[Recommendation text for public safety is still being developed.]
Public safety		Supporting Recommendation 12.1	The federal government should create a stockpile of public safety IoT devices that is available for immediate access.
Healthcare		Key Recommendation 13.0	[Recommendation text for health care is still being developed.]
Healthcare		Supporting Recommendation 13.1	(Under Review) Raise Priority for IoMT to Healthcare Facilities’ Executive Leadership Teams 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.
Healthcare	trust	Supporting Recommendation: NEW	This was discussed in May but **not included herein**: 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.
International	Trust	Supporting Recommendation 14.1	(Proposed) The IoTAB strongly supports the voluntary public/private partnership that created the US Cyber Trust Mark.
International	Trust	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.

Recommendation #	Theme	Recommendation Description
Key Recommendation 1.0	Trust, Infrastructure	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.
Supporting recommendation 1.1	Trust, Infrastructure, US Leadership	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	Trust, Infrastructure	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	Adoption	Conformance to any specific set of requirements should be voluntary.
Supporting recommendation 1.4	Trust	(Under review) The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations.
Supporting Recommendation 1.5	Trust, Infrastructure, US Leadership	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	Trust, Infrastructure	The government can encourage and foster data policies that drive economic growth, such as through this framework.
Key Recommendation 2.0	Infrastructure	The Federal Government should establish methods to foster interoperability for IoT technology, including through the use of consistent models, protocols, and schemas.
Supporting Recommendation 2.1	Infrastructure	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.
Supporting Recommendation 2.2	Infrastructure	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).
Supporting Recommendation 2.3	Infrastructure	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).
Supporting Recommendation 2.4	Infrastructure	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

Recommendation #	Theme	Recommendation Description
Supporting Recommendation 2.5	Trust, Infrastructure, US Leadership	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.
Supporting Recommendation 2.6	Adoption	Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT. 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.
Supporting Recommendation 2.7	Adoption	(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. Issues: Recommendation should focus on data interoperability as a goal, rather than data exchange standards as the means to that goal
Key Recommendation 3.0	Trust, 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.
Supporting Recommendation 3.1	Government	The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.
Supporting Recommendation 3.2	Supply Chain	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.
Supporting Recommendation 3.3	Adoption	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.
Supporting Recommendation 3.4	Adoption	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.
Supporting Recommendation 3.5	US Leadership	The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.

Recommendation #	Theme	Recommendation Description
Supporting Recommendation 3.6	Government	(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. From May: Issues: More information is needed to resolve the relationship of sustainable infrastructure to critical infrastructure and smart cities.
Supporting Recommendation 3.7	Government	(Under Review?) The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience. 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	Infrastructure	(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.
Key Recommendation 4.0	Infrastructure	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.
Supporting Recommendation 4.x	Infrastructure, Government	(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.
Supporting recommendation 4.1	Infrastructure, Government	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.
Supporting recommendation 4.2	Infrastructure, Government	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. Issues: Government doesn't usually play a role in harmonizing standards; possibly should be broader than satellite communications; Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 4.
Key Recommendation 5.0	Trust	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.

Recommendation #	Theme	Recommendation Description
Supporting recommendation 5.1	Trust, Government	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.
Supporting recommendation 5.2	Trust	Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.
Supporting recommendation 5.3	Trust, Government	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.
Key Recommendation 6.0	US Leadership	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	Government, Adoption	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. Issues: May need to be reconciled or combined with 10.4.
Supporting Recommendation 6.2	Government, Adoption	The federal government should consider new models for sustaining and support in considering project feasibility.
Supporting Recommendation 6.3	Government, US Leadership	The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.
Supporting Recommendation 6.4	Government, US Leadership	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.
Supporting Recommendation 6.5	Government, US Leadership	The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).
Supporting Recommendation 6.6	Government, Adoption	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. Issues: May need to be reconciled or combined with 6.1.
Supporting Recommendation 6.7	Government, Adoption	The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility. Maybe missing: SUS-R06: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.
Supporting Recommendation 6.8	Government, Adoption, Sustainability	The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models. Issues: This recommendation has some overlap with Recommendation 2.4.
Supporting recommendation 6.9	Government, Adoption, Sustainability	The federal government should promote development and adoption procedures that accelerate and streamline planning, permitting, and interconnection aspects related to energy efficient technologies.

Recommendation #	Theme	Recommendation Description
Supporting recommendation 6.10	Sustainability	Accelerate the promotion and adoption of procedures and methods to make the electric grid more reliable and resilient.
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.
Supporting Recommendation 7.1	Adoption, Workforce	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.
Supporting Recommendation 7.2	Government, Adoption, Workforce	(Updated) The federal government promote Continuing Education, Professional Development, and Vocational Training for IoT Integration in Supply Chain Management.
Supporting recommendation 7.3	Government, Adoption, Workforce, Traffic and transport	(proposed) The federal government should invest and promote education and workforce development in smart transportation technologies.
Supporting recommendation 7.4	Workforce	Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.
Supporting recommendation 7.5	Government, Adoption, Workforce, Sustainability	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.
Key Recommendation 8.0	Adoption, Traffic and transport	[Smart Traffic/Transit recommendation text is still being developed.]
Supporting Recommendation 8.1	Government, Adoption, Traffic and transport	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.
Supporting Recommendation 8.2	Government, Adoption	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.
Key Recommendation 9.0	Supply Chain	[Full recommendation for supply chain still being developed.]
Supporting Recommendation 9.1	Government, adoption, supply chain	Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.
Supporting Recommendation 9.2	Government, adoption, supply chain	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.
Supporting Recommendation 9.3	Government, adoption, supply chain	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.
Supporting Recommendation 9.4	Government, adoption, supply chain	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.

Recommendation #	Theme	Recommendation Description
Supporting Recommendation 9.5	Government, adoption, supply chain	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.
Supporting Recommendation 9.6	Government, adoption, supply chain	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.
Supporting Recommendation 9.7	Government, adoption, supply chain	The government should promote the development and use of standards for supply chain logistics, traceability, and assurance.
Supporting Recommendation 9.8	Government, adoption, supply chain	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.
Supporting Recommendation 9.9	Government, adoption, supply chain	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.
Supporting Recommendation 9.10	Government, adoption, supply chain	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.
Supporting Recommendation 9.11	Government, adoption, supply chain	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.
Supporting Recommendation 9.12	Government, trust, adoption, supply chain	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.
Supporting Recommendation 9.13	Government, adoption, supply chain	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.
Supporting Recommendation 9.14	Government, adoption, supply chain	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.
Supporting Recommendation 9.15	Government, adoption, supply chain	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.

Recommendation #	Theme	Recommendation Description
Supporting Recommendation 9.16	Government, adoption, supply chain	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.
Supporting Recommendation 9.17	Government, adoption, supply chain	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.
Supporting Recommendation 10.0	Government, adoption, 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. Issues: This recommendation needs refinement. While it is too generic, it could perhaps be combined with similar recommendations from other subgroups; Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 6.
Supplemental Recommendation 10.1	Government, adoption, precision agriculture	The federal government should consider subsidizing the use of IoT in farms. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 1.
Supplemental Recommendation 10.2	Government, adoption, precision agriculture	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. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 2.
Supporting recommendation 10.3	Government, adoption, precision agriculture	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. Issues: Concerns regarding privacy, maturity of the AI technology; premature for government to “promote” use of this technology Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 5.
Key Recommendation 11.0	Environmental Monitoring	[Key recommendation text for environmental monitoring is still being developed.]
Supplemental Recommendation 11.1	Government, adoption, Environmental Monitoring	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.
Supplemental Recommendation 11.2	Government, adoption, Environmental Monitoring	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?)
Key Recommendation 12.0	?	[Recommendation text for public safety is still being developed.]

Recommendation #	Theme	Recommendation Description
Supporting Recommendation 12.1	?	The federal government should create a stockpile of public safety IoT devices that is available for immediate access.
Key Recommendation 13.0	Healthcare	[Recommendation text for health care is still being developed.]
Supporting Recommendation 13.1	Healthcare	(Under Review) Raise Priority for IoMT to Healthcare Facilities' Executive Leadership Teams 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.
Supporting Recommendation: NEW	Healthcare	This was discussed in May but **not included herein**: 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.
Supporting Recommendation 14.1	International	(Proposed) The IoTAB strongly supports the voluntary public/private partnership that created the US Cyber Trust Mark.
Supporting Recommendation 14.2	International, Trust	(Proposed) The government should create an international data minimization framework related to IoT devices, aligning with the NIST Privacy Framework principles.

Short Name	Organizing Themes	Description/examples/subgroups
Infrastructure	Enhance and modernize infrastructure supporting IoT	Connectivity, standards and interoperability, compute, etc.
Trust	Create trust in IoT	Cybersecurity, privacy, confidentiality, provenance, integrity, transparency, data usage and management
Supply Chain	Ensure IoT supply chain integrity and resilience	Augmented Logistics & Supply Chain
Workforce	Develop, grow, and maintain a workforce to support the IoT economy	Workforce Development (all subgroups)
International	Address challenges of IoT in a global ecosystem and economy	International subgroup (standards, trade, etc.)
Government	Develop government capability to support and sustain a IoT economy	(All subgroups)
Adoption	Facilitate industry adoption (including govt, small business adoption) and value realization of IoT.	Consumer awareness, government procurement, policies (tax credits, etc.)
US Leadership	Facilitate US IoT technology and innovation leadership	Research and development, technology transfer, etc.
	Align federal actions in IoT to advance policy goals	
	Climate change	
	Sustainabiliity	
	Healthcare	
	Environmental Monitoring	
	Traffic and transit technologies	
	Critical infrastructure	
	Precision agriculture	
	Technology transfer/lab to market	
	Augmented supply chains	

Recommendation #	Recommendation Description
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.
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.
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.
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.

Recommendation #	Recommendation Description
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).
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).
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
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.
Supporting Recommendation 2.6	Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT. 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.
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. Issues: Recommendation should focus on data interoperability as a goal, rather than data exchange standards as the means to that goal This was discussed in May but **not included herein**: 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.

Recommendation #	Recommendation Description
Key Recommendation 3.0	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.
Supporting Recommendation 3.1	The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.
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.
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.
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.
Supporting Recommendation 3.5	The Administration should encourage Congressional support to deploy IoT cybersecurity labeling initiatives, including establishing incentives for manufacturers to participate.
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. From May: Issues: More information is needed to resolve the relationship of sustainable infrastructure to critical infrastructure and smart cities.
Supporting Recommendation 3.7	(Under Review?) The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience. 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.

Recommendation #	Recommendation Description
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.
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.
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.
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. Issues: Government doesn't usually play a role in harmonizing standards; possibly should be broader than satellite communications; Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 4.
Privacy	
Key Recommendation 5.0	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.
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.
Supporting recommendation 5.2	Promote the implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.
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.
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.
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. Issues: May need to be reconciled or combined with 10.4.
Supporting Recommendation 6.2	The federal government should consider new models for sustaining and support in considering project feasibility.

Recommendation #	Recommendation Description
Supporting Recommendation 6.3	The Federal Government should establish an Emerging Technology (EmT) office within each of the federal agencies.
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.
Supporting Recommendation 6.5	The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).
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. Issues: May need to be reconciled or combined with 6.1.
Supporting Recommendation 6.7	The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility. Maybe missing: SUS-R06: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies.
Supporting Recommendation 6.8	The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models. Issues: This recommendation has some overlap with Recommendation 2.4.
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.
Supporting recommendation 6.10	Accelerate the promotion and adoption of procedures and methods to make the electric grid more reliable and resilient.
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.
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.
Supporting Recommendation 7.2	(Updated) The federal government promote Continuing Education, Professional Development, and Vocational Training for IoT Integration in Supply Chain Management.
Supporting recommendation 7.3	(proposed) The federal government should invest and promote education and workforce development in smart transportation technologies.
Supporting recommendation 7.4	Develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.

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

Recommendation #	Recommendation Description
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.
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.
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.
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.
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.
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.
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.
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.
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.
Supporting Recommendation 10.0	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.

Recommendation #	Recommendation Description
Supporting Recommendation 10.0	Issues: This recommendation needs refinement. While it is too generic, it could perhaps be combined with similar recommendations from other subgroups; Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 6.
Supplemental Recommendation 10.1	The federal government should consider subsidizing the use of IoT in farms. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 1.
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. Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 2.
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. Issues: Concerns regarding privacy, maturity of the AI technology; premature for government to “promote” use of this technology Note: This was presented in the July meeting as Sustainable Infrastructure Recommendation 5.
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.
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?)
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.
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 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.

Recommendation #	Recommendation Description
Supporting Recommendation 14.1	(Proposed) The IoTAB strongly supports the voluntary public/private partnership that created the US Cyber Trust Mark.
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.