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

July 18, 2023

IoT Advisory Board Members

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

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

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

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

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

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

Tom Katsioulas, Chair, Global Semiconductor Alliance

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

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

Ann Mehra

Robby Moss, President and Principal Consultant, TGL Enterprises LLC

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

Maria Rerecich, Senior Director of Product Testing, Consumer Reports

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

Arman Shehabi, Staff Scientist, Lawrence Berkeley National Laboratory

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

Contents

1. Executive Summary

[this will be drafted after other sections are complete]

2. Introduction

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

3. Background

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

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

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

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

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

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

3.1. Charter and Scope

FACA description, charter and scope

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

Note: Not sure this and the background info are needed

4. Summary of Recommendations of the Advisory Board

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

5. Methodology

5.1. Approach

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

5.2. Description of IoT in the Context of this Report

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

6. Commentary and Discussion Topics Related to IoT Adoption

6.1. IoT Technology

What is the current state

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

What is the future state

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

6.2. Artificial Intelligence (AI) Considerations

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

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

6.5. Regulations

6.6. Standards

6.7. IoT Personas

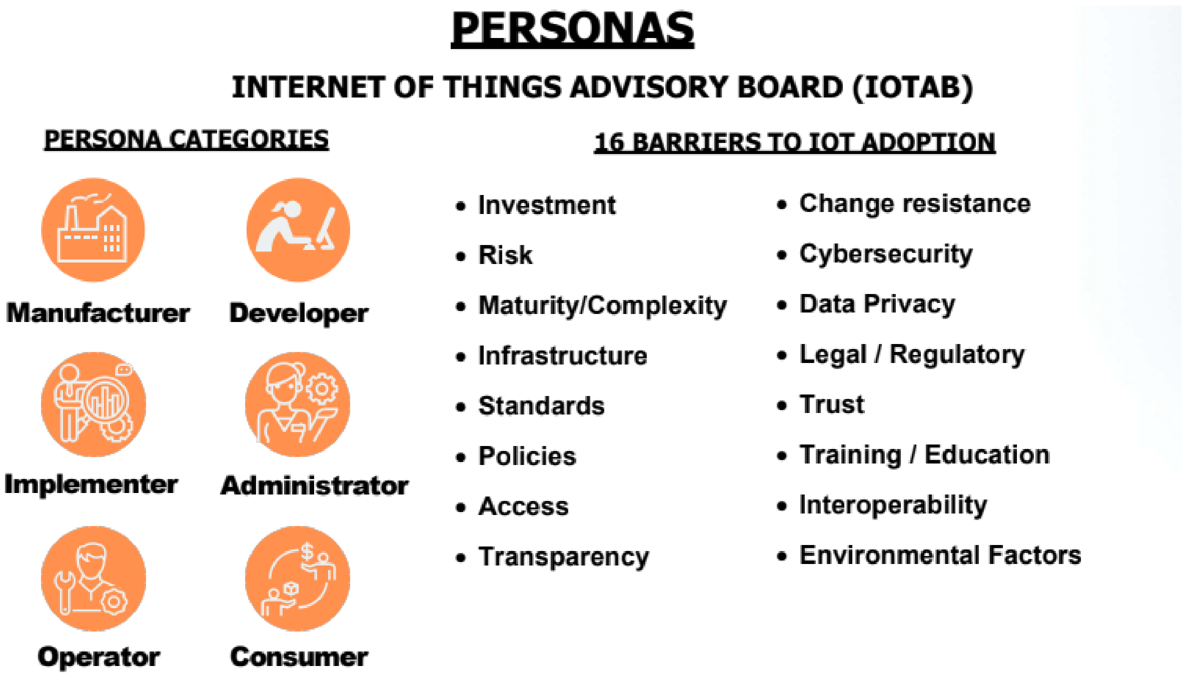
Brief background about the personas and their value in ensuring that the relevant and appropriate stakeholder groups are considered and, where applicable, included in the recommendations.

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

Persona Categories

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

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



PERSONAS

INTERNET OF THINGS ADVISORY BOARD (IOTAB)

PERSONA CATEGORIES

Manufacturer

Developer

Implementer

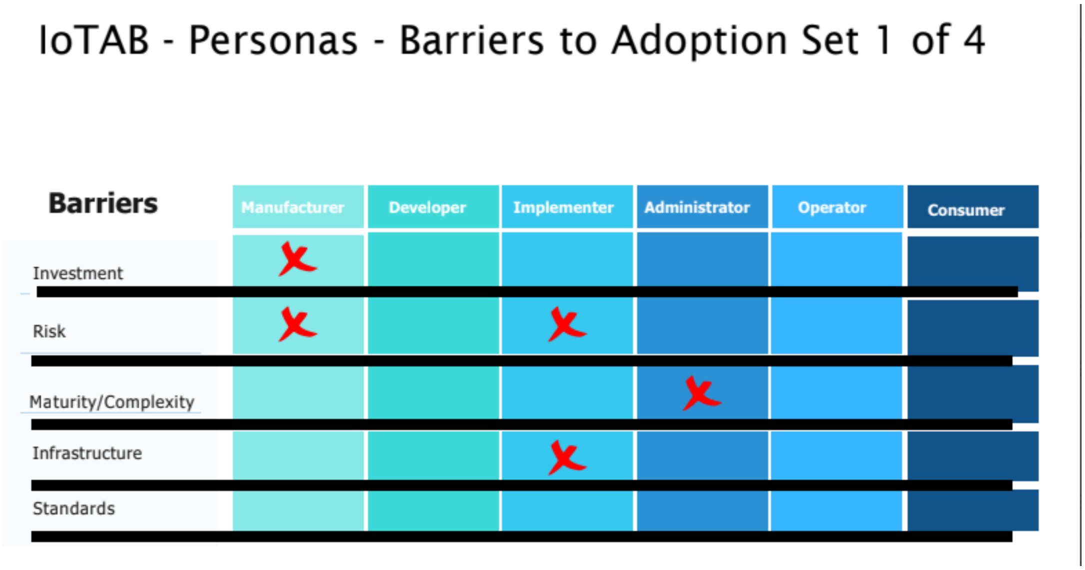
Administrator

Operator

Consumer

16 BARRIERS TO IOT ADOPTION

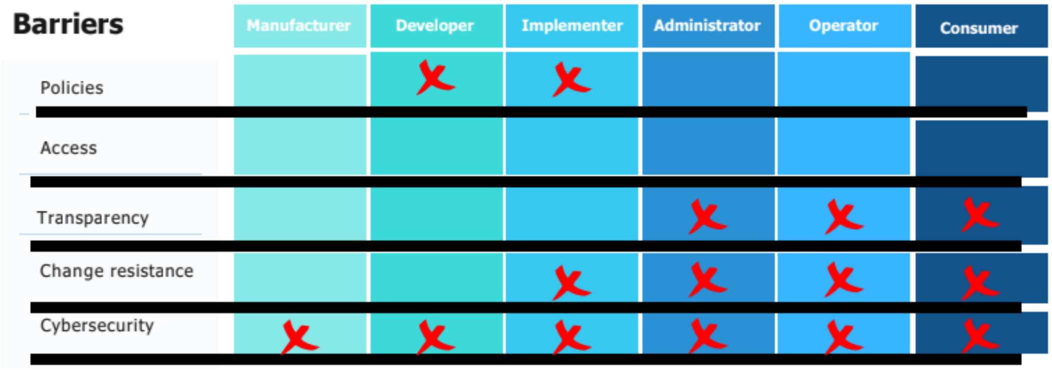
- Investment
- Risk
- Maturity/Complexity
- Infrastructure
- Standards
- Policies
- Access
- Transparency
- Change resistance
- Cybersecurity
- Data Privacy
- Legal / Regulatory
- Trust
- Training / Education
- Interoperability
- Environmental Factors



IoTAB - Personas - Barriers to Adoption Set 1 of 4

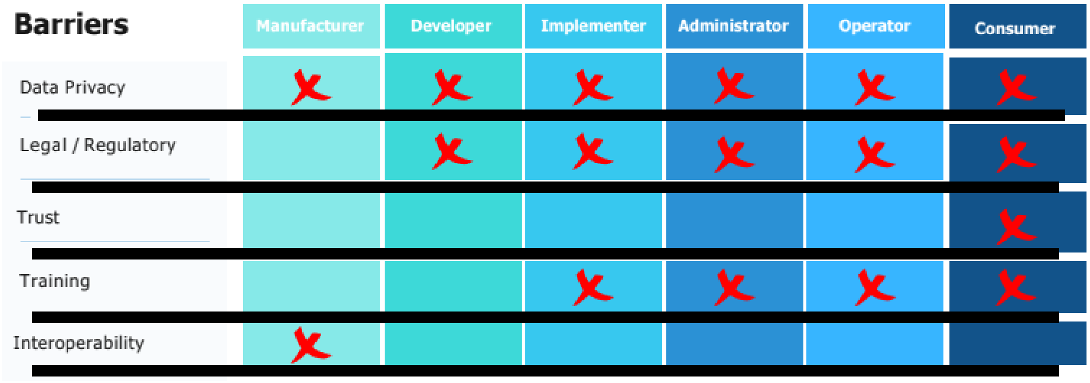
Barriers	Manufacturer	Developer	Implementer	Administrator	Operator	Consumer
Investment	✗					
Risk	✗		✗			
Maturity/Complexity				✗		
Infrastructure			✗			
Standards						

IoTAB - Personas - Barriers to Adoption Set 2 of 4



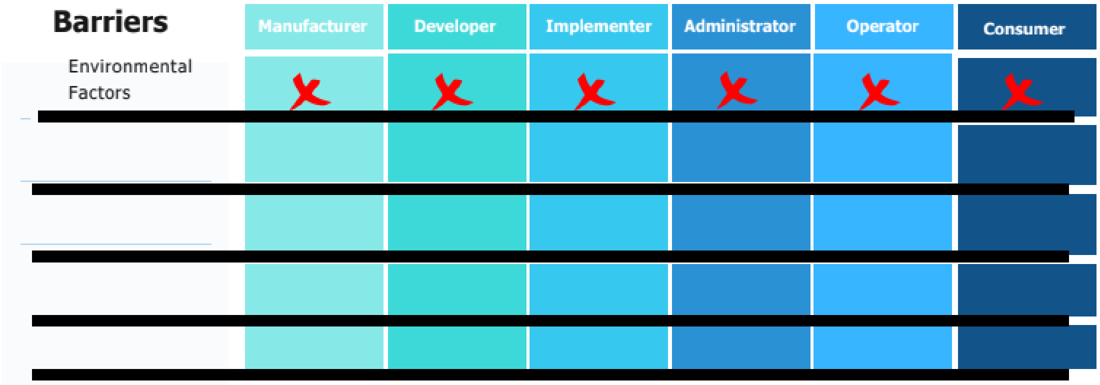
Barriers	Manufacturer	Developer	Implementer	Administrator	Operator	Consumer
Policies		✗	✗			
Access						
Transparency				✗	✗	✗
Change resistance			✗	✗	✗	✗
Cybersecurity	✗	✗	✗	✗	✗	✗

IoTAB - Personas - Barriers to Adoption Set 3 of 4



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

IoTAB - Personas - Barriers to Adoption Set 4 of 4



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

7. Detailed Findings of the Advisory Board

After the recommendations in Section 9 are complete, we will summarize the findings here. Originally it was intended to be parsed by topic, but it may be better to focus simply on broad challenges and opportunities. (Section 7.1 serves as an example to be iterated throughout the remaining subsections)

7.1. Smart traffic and transit technologies

7.1.1. Overview

- Definition of this topic area
- Why is this important and why are we addressing it?

7.1.2. Opportunities and benefits (for personas)

- Description of opportunity/market characteristic, etc
- Use cases/applications (3 representative use cases)
- Summary of key representative ongoing industry/government/academia efforts in this area

7.1.3. Barriers (faced by personas to IoT implementation)

- Description of barrier and examples
- Who is impacted?
- Impact/significance of this barrier (descriptive, or quantitative) and what benefits are being precluded?
- Summary of barriers

7.2. Augmented logistics and supply chains

7.3. Sustainable and critical infrastructure

7.4. Precision agriculture

7.5. Environmental monitoring

7.6. Public safety

7.7. Healthcare

8. Cross Market and Development Topic Areas

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

8.1. Cybersecurity

8.1.1. Overview

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

8.1.2. Opportunities and benefits of solving those challenges (for personas)

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

8.1.3. Barriers (faced by personas)

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

8.2. Privacy and data ownership

8.3. Skills, education, workforce development

8.4. Standards and interoperability

8.5. Regulations and commerce

8.6. Policies

8.7. International engagement

9. Recommendations

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

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

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

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

Key Recommendation 1.0: National Data Protection Framework

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

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

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

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

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

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

Example use cases include the following:

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

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

Supporting recommendation 1.2: (Under review) The government should examine opportunities to use the notional IoT Data Framework to support and document privacy considerations.

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

Supporting Recommendation 1.3: (Under review) 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 1.4: (Under review) The government could incentivize the creation of trusted data marketplaces where data producers and consumers share information about data.

Such an environment might enable data exchange, even providing some monetizing opportunities, and could be built in a manner that would protect intellectual property. The goal of the service would be to provide supply chain visibility, potentially reducing redundancies and simplifying logistics in complex supply chains.

Supporting recommendation 1.5: The government can encourage and foster data policies that drive economic growth, such as through this framework.

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

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

Key Recommendation 2.0: Standardize IoT Implementation

The U.S. should establish methods to foster interoperability and security for IoT technology, including through the use of consistent models, protocols, and schemas. Formal standards may be needed, such as those from a standards development organization or from a technical engineering organization (e.g., Institute of Electrical and Electronics Engineers (IEEE)). It is highly recommended not to mandate any formal or informal standard or protocol, but rather to encourage voluntary conformance in the interest of improved interoperability.

It is likely that wholly new standards and models will not need to be created “from scratch”; rather, industry collaboration is likely to advance existing communications and interoperability protocols that can rapidly be encouraged and adopted.

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

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

Supporting Recommendation 2.1: The government should promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across various IoT systems and devices. Doing so would foster innovation and competition among all parts of the supply chain and would simplify integration and maintenance for supply chain partners.

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).

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

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

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).

The federal government should promote and adopt industry led standards that provide minimum interoperability and cybersecurity requirements for smart transportation technologies and corresponding transportation infrastructure. This is particularly relevant if industry led standards are addressing known gaps and solving market fragmentation issues.

In particular, smart transportation systems focus on safety, so standardization (especially for security and interoperability needs) is vital to ensuring that devices can communicate basic safety information to other vehicles & to/from infrastructure.

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

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

Supporting Recommendation 2.5: Federal agencies can help support existing industry standards development activities with respect to energy efficient technologies used in sustainable infrastructure. Failure to standardize could result in confusion in the marketplace, possibly hindering participants from entering the product market.

Supporting Recommendation 2.6: Agencies should advocate for the implementation and adoption of interoperable data standards for public safety IoT. Solutions might include facilitation of adoption by funding grants for jurisdictions/agencies for procurement of interoperable IoT solutions. Support could also include development of education/training materials to help jurisdictions/agencies apply best practices for interoperability.

It is the Board's opinion that interoperability of IoT device data would enhance incident responses and coordination among responder teams, providing safety benefits that would encourage the adoption of IoT. Proliferation of IoT devices without interoperable data will make it difficult to achieve interoperability the longer it diverges. There may also be barriers to prioritizing data interoperability when procuring public safety IoT devices include limited budgets but also lack of understanding of what to require.

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

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

Specific solutions might include:

- Procurement: Prioritize solutions which adhere to the IoMT data exchange standard in government contracts;
- Tax Incentives: Provide tax benefits to companies that implement the IoMT data exchange standard; and,
- Promotion: Promote the IoMT data exchange standard and educate healthcare organizations about the benefits.

Supporting Recommendation 2.8: (Proposed) 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). This is particularly relevant if industry led standards are addressing known gaps and solving market fragmentation issues.

This approach would support interoperability as industry standards and protocols ensure that devices from different manufacturers can communicate and work together seamlessly. This is particularly important when dealing with multiple states and local jurisdictions. It would also address cybersecurity risks (primarily addressed in Key Recommendation 3) through industry standards that describe minimum cybersecurity requirements of these technologies.

Additional benefits include:

- Innovation and competition: Industry standards can stimulate innovation and competition by providing a level playing field for businesses and developers, regardless of their size or market share. With a level baseline on a particular product or device companies can now build upon it and tailor their own solutions.
- Cost savings: Standardization can lead to cost savings for businesses by reducing the need for customized solutions and simplifying the procurement process. This is especially relevant for agencies with limited budgets.

- Regulatory compliance: Industry standards and protocols can serve as a foundation for subsequent government regulations and policies.

There are numerous smart traffic-specific implementation considerations:

1. Inclusiveness: Industry standards activities in this sector typically involve a diverse range of stakeholders such as: autonomous vehicle manufacturers, roadside infrastructure manufacturers, communication technology providers, software developers, academia, and even government agencies. The industry standards and guidelines that already exist are comprehensive, practical, and aligned with the needs and priorities of all relevant parties.

2. Prioritize safety and Cybersecurity: Deaths from traffic accidents continue to increase and industry standards/guidelines can describe how connected vehicles and infrastructure equipped with Cellular Vehicle-to Everything (C-V2X) technologies can help to decrease them (NEMA US DOT Comments Enhancing Safety of VRUs at Intersections). Recognizing that these devices can serve as a gateways for malicious actors the industry is already taking steps in developing and implementing appropriate cybersecurity standards.

3. Built on existing standards: Industry standards that are being developed leverage other existing industry standards and best practices as a starting point and adapt or expand upon them as necessary.

4. Flexibility and adaptability: Industry standards and protocols that are flexible can be easily updated to accommodate new technologies, emerging threats, and evolving industry needs.

5. Promote adoption: Encourage and incentivize adoption of the established standards and protocols through government adoption, contract-flow-down, education, outreach, and support programs (particularly relevant for small-medium sized enterprises).

6. Foster global collaboration: collaboration with international allies can help to ensure that these standards are harmonized to the greatest extent possible, while being consistent with U.S. trade policy goals.

Key Recommendation 3.0: IoT Cybersecurity (including Critical Infrastructure)

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

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

Supporting Recommendation 3.1: The Federal Government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems. Security guidance will largely build on existing federal initiatives, including the recently announced U.S. national cybersecurity label for connected devices. The Board recommends that federal entities prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of that labeling program.

Efficiently using these processes requires taking advantage of industry expertise. Continued industry engagement as the program is scoped, planned, and executed will be critical to the program's success. Existing label programs have varied; the more flexible the government can be in qualifying the process rather than dictating it, the better the results will be. Process qualification should be outcome-based rather than centrally determined. These outcomes determine the need for trust mechanisms such as meeting the NISTIR 8425 Criteria and having industry-accredited processes. Notably, there may be a perceived advantage in defining a uniform U.S. government scheme rather than defining the necessary outcomes from various industry schemes.

Supporting Recommendation 3.2: 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. Doing so will help to protect sensitive data and provide operational assurance, as well as supporting compliance with various security regulations.

Since supply chain security concerns can be a hindrance to IoT adoption, security provisions will enhance competitiveness and innovation, and will reduce resistance to information sharing.

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

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

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

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

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

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

Supporting Recommendation 3.4: (Under Review) The Federal Government should update Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience requiring a sector-specific Internet of Things (IoT) data strategy.

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

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

Supporting Recommendation 3.5: The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.

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

Supporting Recommendation 3.6: The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

These buildings are reliant on building control systems which provide the functional, operational, and safety needs of a building. These can serve as gateways for malicious actors who can take control of critical lifesaving applications with a building (i.e., heating, air conditioning, physical access). More than just the building management is at stake: data that resides on an unprotected building control system that contains personal and confidential information could be used against an individual.

Credibility and assurance can be provided to the private sector when the Federal Government leads by example. There may be financial benefits, as well, since buildings that have their connected systems upgraded could save money on cyber insurance premiums.

The EPA has a program for Energy Star Building Certifications. There could be a similar program that addresses cybersecurity within a building. The GSA Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR) could have base level cybersecurity requirements for connected systems in building infrastructure.

Key Recommendation 4.0: IoT Connectivity Improvement and Expansion

[Key recommendation text is still being developed.]

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

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

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

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

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

Supporting recommendation 4.2: (Under Review) The federal government should actively promote and support the adoption of satellite narrowband IoT systems. While the focus for this topic by the Board relates to agricultural needs, the opportunity applies to any IoT connectivity where devices are deployed in remote areas.

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

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

Key Recommendation 5.0: Address Privacy Considerations for IoT

[Key recommendation text is still being developed.]

Supporting recommendation 5.1: (Under Review) The federal government should advocate for the simplification of privacy policies, privacy notices, and data use policies to enhance accessibility and comprehension for users. Improved understanding of data privacy policies for users will leading to more informed decisions when adopting and using IoT devices. Better and simplified may lead to increased compliance and will enhance public trust in IoT devices and related technologies.

Supporting recommendation 5.2: (Under Review) The federal government should (in coordination with the data protection framework referenced in Recommendation 1) create a set of "data use" basics that must be included in privacy policies for IoT devices. These can be designed with the consumers' needs and understanding in mind.

Supporting recommendation 5.3: (Under Review) The federal government should conduct a thorough analysis of existing and proposed privacy regulations to identify best practices and lessons learned for IoT data protection / privacy considerations. Observations gained may help inform the data protection framework referenced in x.x.

Supporting recommendation 5.4: (Under Review) The federal government should develop and implement a privacy label system for IoT devices, similar to nutrition labels on food products (similar to the White House initiative for cybersecurity labeling). Such a system would display essential privacy information in an easily understandable format for consumers, enhancing transparency and trust. While there are many parallels, the group recognizes that cybersecurity and data privacy are not the same, so this distinction should be evident in this labeling scheme. The system would empowers consumers to make informed decisions about IoT devices based on their privacy features and practices, and encourage IoT device manufacturers to prioritize privacy, fostering competition and innovation in privacy-enhancing technologies.

Note: there was little support for the recommendation to implement comprehensive privacy regulation so that has been omitted.

Key Recommendation 6.0: Sustainable Infrastructure

[Key recommendation text is still being developed.]

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

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

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

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

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

IoT enables new business and operating models; economic service models to assist could include:

- Extended Funding – extending funding for O&M for select applicants (rural, tribal, small towns, etc.)
- Regional cost sharing – encourage multiple cities in a region to apply as one
- Innovative – encourage innovative models (corporate, sponsorships)

Key Recommendation 7.0: Workforce

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

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

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

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

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

Supporting Recommendation 7.2: Agencies can support an improved Supply Chain Workforce by investing in and promoting education and workforce development for designing, implementing, and managing IoT systems in supply chain operations.

The government can also place a focus on reskilling and upskilling, either helping existing workers to adapt in their career path or moving to IoT as a replacement opportunity. In all cases, the industry will benefit if the U.S. promotes STEM education, including for early school ages.

The U.S. should establish performance metrics to measure and demonstrate progress on these fronts, as well.

The government can develop educational initiatives that focus on IoT, targeting workforce development and enhancing consumer privacy and trust. This can be achieved by increasing the understanding and safe use of IoT technologies developing a highly skilled workforce capable of addressing IoT privacy challenges, and boosting consumer trust and through adoption of IoT devices and services.

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

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

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

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

The justification for the recommendation to invest in education and workforce development in the is provided below:

1. Addressing skills gap: This is particularly evident for traffic engineers who are not familiar with these types of new technologies. They think of traffic engineering as concrete and asphalt

2. Enhancing competitiveness: A well-trained and skilled workforce is a key factor in the competitiveness of the sector. By investing in education and workforce development, the government can help businesses stay ahead of international competition and maintain a strong position in the global market.

3. Fostering innovation: A skilled workforce with a strong foundation in these technologies can drive innovations and development in new cutting-edge solutions.

4. Supporting digital transformation: The transportation sector is already undergoing a digital transformation and businesses need to adapt their operations and processes accordingly.

5. Encouraging job creation: As these new cutting-edge technologies are being developed in the transportation sector new jobs may be created-particularly as autonomous vehicles become more mainstream.

6. Outcomes Based Contracting: Solving transportation related issues and problems for those agencies that has an existing workforce with a limited knowledge or skill set for these types of technologies.

Implementation considerations for investing in education and workforce development include:

1. Identifying skill requirements: Conduct a thorough analysis of the specific skills and expertise needed.

2. Developing targeted curricula: Collaborate with educational institutions, industry stakeholders, and training providers to develop targeted curricula and training programs unique to the transportation sector.

3. Expanding access to education and training: Implement policies and programs that ensure broad access to this and training, including financial aid, scholarships, and online learning options to reach underserved communities.

4. Encouraging industry-academia partnerships: Promote partnerships between industry and educational institutions to facilitate real-world learning experiences, internships, and collaborative research projects.

5. Focusing on reskilling and upskilling: Implement programs to reskill and upskill the existing workforce, enabling them to adapt to the changing requirements of the transportation sector.

6. Establishing performance metrics: Develop performance metrics and evaluation methods to assess the effectiveness of education and workforce development initiatives and make data-driven improvements as needed.

7. Outcomes based Contracting: Outcomes based Contracting is a form of contracting comprised of four discrete characteristics: Identification, Alignment, Measurement, and Adjustment.

Key Recommendation 8.0: Precision Agriculture

[Key recommendation text is still being developed.]

Supplemental Recommendation 8.1: (Under Review) The U.S. should create a National Strategy for Agricultural IoT.

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

As IoT technologies continue to advance, their adoption in agriculture can significantly enhance productivity, resource efficiency, and environmental sustainability. However, without a cohesive national strategy, the potential benefits of agricultural IoT may be hindered by fragmented initiatives, limited interoperability, and a lack of clear direction.

To achieve success, the government can help to catalog and prioritize challenges in the sector, providing specific goals, timelines, and milestones for the integration of IoT in agriculture. This could be accomplished through an interagency task force that would engage with stakeholders across industry, develop the model, and help identify possible funding or other resources.

Supplemental Recommendation 8.2: The federal government should consider subsidizing the use of IoT in farms.

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

The federal government should encourage and promote partnerships among public, private-sector, and academia. This partnership should leverage Agricultural Extension Centers.

Supplemental Recommendation 8.3: The federal government should fund the deployment of a “farm of the future” setup in every land grant university nationwide.

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

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

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

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

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

Supporting recommendation 8.4 : (Under Review) The federal government should promote adoption of Generative AI applications for Agriculture IoT.

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.

By leveraging advanced algorithms and machine learning techniques, Generative AI can enable farmers to identify patterns, optimize resource allocation, and make better-informed decisions. This will result in benefits for various stakeholders, including farmers, policy makers, agricultural companies, and consumers.

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

Note: Additional recommendations regarding broadband and satellite connectivity are described in Recommendation 4.

Key Recommendation 9.0: Environmental Monitoring

[Key recommendation text is still being developed.]

Supplemental Recommendation 9.1: The federal government should establish or encourage IoT environmental data repositories in support of open, available data. Promoting the open availability of data would promote research, improve transparency, and encourage proactive improvement by industry participants. As described in other recommendations throughout this report, improved interoperability and competitiveness will help benefit all IoT adopters, and an open model for shared and consistent data will help take strides toward those objectives.

Supplemental Recommendation 9.2: The federal government should facilitate and support the research, development and deployment of low cost Air Quality sensors. (Could we expand to additional types of monitoring?)

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

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

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

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

Agencies should encourage automated and consistent measurement and can facilitate research in low-cost sensing technologies for criterial pollutants, such as optical particle scanning for particulate matter and M0x elements for gases and detection of other emerging chemicals of concern.

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

Key Recommendation 10.0: Smart Cities

[Key recommendation text is still being developed.]

Supporting Recommendation 10.1: The federal government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).

Some cities/agencies lack expertise, tools, and resources and small cities/agencies may be even more challenged. As referenced throughout this report, IoT can bring great economic and societal benefits to our cities, but specific smart city and sustainable infrastructure expertise in industry is limited and hard to attract. An SCSEP similar to existing partnerships (e.g., MEP, USDA) would be a worthwhile investment, and would provide an improved model over the current public procurement process to engage private sector resources.

Supporting Recommendation 10.2: (Under Review) The Federal Government should establish a Smart City Officer (SCO) within each of the twenty-four (24) CFO Act agencies.

This position would serve as a business executive and technology strategist, developing and governing a comprehensive strategic, tactical, and operational roadmap intended to communicate how existing and future projects are/can support organizational mission, inform resourcing decisions, and identify enterprise-wide investment opportunities. Once assigned via the Agency Head, e.g., Cabinet Secretary, the SCO will be required to develop a 90-day plan to include resources necessary to carry out the SCO program.

Supporting Recommendation 10.3: (Under Review) The Federal Government should establish a Smart Cities Program Office (SCPO) within the Executive Office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage smart city initiatives across the United States.

This central office will ensure that the federal government, state, and local government entities can effectively plan, implement, and manage smart city initiatives across the United States. The SCPO will align with the U.S. Chief Technology Officer Team to maximize the benefits of IOT and corresponding data for critical infrastructure sectors. The SCPO will develop a 360-day approach/plan addressing how the Federal Government can help cities develop a corresponding strategic roadmap for their smart city (and IoT) initiatives. This includes identifying goals, prioritizing initiatives, and developing a roadmap for implementation.

Supporting Recommendation 10.4: The federal government should consider the specification and utilization of IoT and "smart" technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.

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

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

Supporting Recommendation 10.5: The federal government should consider funding models for sustaining and support beyond the initial acquisition and building of new projects.

The federal government should consider funding models for sustaining and support beyond the initial acquisition and building of new projects. While many grants for projects help offset the initial cost of capital procurement, integration and development, the cost of operating the asset or system is left to the municipality or agency. Some municipalities may have the resources, funding models, or mechanisms to find the resources to sustain the operation and maintenance of this asset or system. However, many municipalities and agencies do not have these mechanisms (budget, taxes, etc.), and may forgo these types of projects.

The Board recognized that most American cities are small: 4,005 cities between 5K and 50K, 476 cities between 50K and 100K, and 238 cities between 100K and 250K

Agencies have an opportunity to provide equitable access to benefits for smaller cities. These cities are dependent on outside funding sources for many projects, as many do not have the same funding methods as larger ones. Cities may also benefit from working together on these projects, so the government is in a position to help provide a focus on regional projects that benefit multiple small cities and that cut across city borders.

Supporting Recommendation 10.5: The federal government should facilitate and support the development of smart city and sustainable infrastructure reference architectures.

There is no standardized definition of a smart city. Even among cities, a reference to a “smart city” varies. For example, some would say digitizing processes and doing transactions online makes them a smart city, while another may set up a public Wi-Fi network and call themselves a smart city. In general, most smart cities are a bunch of “point solutions” set up by different departments and agencies that don’t necessarily integrate or share common infrastructure.

Smaller cities have needs that may be different than their larger counterparts. The architectures they need may be different from those of larger cities. However, without a reference architecture, a piecemeal approach may lead to the situation where smart cities are built such that it would be difficult to integrate together or may lead to a city of smart solutions instead of a smart city of solutions working together.

The federal government can help establish a starting point vision or model that municipalities can begin to build with. For example, a true “smart city” is an interconnected system of cities, utilities (city owned or not), buildings, communities and businesses that interact. A broader reference model/architecture will help to identify potential areas of collaboration between entities, as well as identify areas of “sharing” and economies of scale.

Reference architectures may include a broader integration of entities that are not normally considered, such as utilities, smart regions, counties, and other communities (rural areas, etc.). They can also better support ecosystems in particular areas (e.g., communities, regions, counties, states).

The NIST GCTC has already established a structure and model to create, engage and support industry/academia/government partnerships. This infrastructure can be tailored to execute on this recommendation.

Supporting Recommendation 14.9: IoT Performance Metrics - The Sector Risk Management Agencies (SRMAs) should collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience. The expansive development and adoption of IoT assets and systems should map to IoT performance metrics intended to strengthen critical infrastructure security and resilience. Agency Chief Technology Officer and associated program office could serve as the nexus for convening peer stakeholders, e.g. CIO, CDO, CPO. Defining the performance metrics will need to be in conjunction with owners/operators of critical infrastructure assets/systems (both IT and OT).

Note: Smart city standards are covered in Recommendation 2

Key Recommendation 11.0: Health Care

[Key and recommendation text is still being developed.]

Supporting Recommendation 11.1: (Under Review) Raise Priority for IoMT to Healthcare Facilities' Executive Leadership Teams

Note: Data exchange for Internet of Medical Things (IoMT) is #2.8.

Key Recommendation 12.0: Public Safety

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

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

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

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

Similar to the HHS stockpiles of vaccines, PPE, etc., we recommend the US government add public safety devices to their procurement list.

Initial and ongoing funding is needed along with cooperation from manufacturers who wish to participate in the stockpile program develop APIs and interoperability to other competing and complementary devices.

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

Key Recommendation 13: Smart Traffic and Transit

[Key recommendation text is still being developed.]

Supporting Recommendation 13.1: The federal government should consider developing programs and grants to allow underserved and less developed communities as well as rural areas.

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

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

Supporting Recommendation 13.2: 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.

Conflicting Regulations/Legislations: With regulations/legislations that conflict there is a question of liability in the event of an accident involving a drone. There are also safety concerns.

Data/Privacy Framework is covered in Recommendation 1.

Industry-led Standards for AVs are covered in Recommendation 2.

Standards for interoperability and security are covered in Recommendation 2.

Education and Workforce are covered in Recommendation 7.

Key Recommendation 14.0: Supply Chain Logistics

[Key recommendation text is still being developed.]

IoT for Supply Chain is generally grouped into two segments: 1) the actual logistics of producing, transporting, and storing products (and providing services), and 2) the reliability and security of that chain of goods and services. Those segments are illustrated as “logistics” and “transparency” in Recommendation 14.

Augmented Supply Chain Logistics

Supporting Recommendation 14.1: National Strategy for IoT In Supply Chain Logistics - Establish a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.

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

Supporting Recommendation 14.2: Incentivize Adoption Of IoT in Supply Chain Logistics: Establish and provide financial incentives to encourage adoption of IoT technologies in supply chain operations by reducing initial investment costs and perceived risks associated with implementation of IoT solutions. Federal organizations should identify appropriate incentives and coordinate across agencies to support, monitor, and evaluate opportunities to incentivize IoT adoption in the supply chain.

Supporting Recommendation 14.3: 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 14.4: 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.

Global nature of supply chains; Harmonization of standards and regulations; Addressing global cyber threats; Leveraging global expertise; Fostering innovation; Building trust; Addressing social and environmental challenges; Establish bilateral and multilateral agreements; Participate in international forums and organizations; Share information and best practices; Collaborate on research and development; Promote capacity building; Identify key international partners; Leveraging existing diplomatic channels; Coordinate with relevant federal agencies

Standards encouraged by the federal government might encourage the use of Global Identifier Standards (e.g., GS1 (provide a link)) for supply chain traceability to improve security and supply chain transparency, reduce the risk of counterfeit or tampered goods, and enable creation of digital threads by tying workflow IDs to asset IDs.

Supporting Recommendation 14.5: Monitor And Evaluate IoT Adoption Progress in supply chain logistics - Monitor and evaluate progress to provide assurance that IoT adoption efforts in supply chain logistics are on track, effectively addressing identified challenges and opportunities, and delivering desired outcomes. Assess effectiveness and measure impact / Identify areas for improvement / Allocate resources efficiently / Enhance accountability / Facilitate knowledge sharing / Inform future strategies. Establish clear goals and objectives; Develop relevant performance indicators ; Implement data collection and reporting mechanisms ; Conduct periodic assessments ; Culture of continuous improvement ; Collaborate with stakeholders and assign responsibility ; Develop a monitoring and evaluation plan ; Allocate resources

Supporting Recommendation 14.6: Sustainable, Scalable Manufacturing Growth - The recommended policies, incentives and requirements are relevant to the transportation sector as it becomes increasingly connected, integrated, and ultimately autonomous. Rapid technological advances are further augmented by communication and IT, including IoT. Phase in domestic contract requirements.; Accelerate domestic manufacturing with investment tax credit for capital costs. Provide clear rules on domestic content requirements. Avoid rules that require determining the country of origin of subcomponents. Component test should include all costs associated with the manufacturing of a product. Allow 100% of manufacture value added (MVA) or substantial transformation to be classified as domestic content in component tests. Designate countries outside US for allowed procurement of components.

Smart Supply Chain Traceability

Supporting Recommendation 14.7: Trusted Architectures for Provenance & Traceability

Promote development and use of trusted hardware/software architectures for supply chain provenance, traceability, chain of custody and lifecycle mgmt.; Enhance supply chain security and mitigate risks relate to compromised components; Increase trustworthiness of critical systems for security, safety, and economic stability.; Increase consumer confidence, prevent supply chain attacks and data breaches ; Improve supply chain security, chain of custody and lifecycle management (SBOM-HBOM)

Supporting Recommendation 14.8: Incentivize IoT Systems Supply Chains to Adopt Trusted Traceability

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

- Improve confidentiality & integrity of IoT supply chain to prevent attacks, human/economic losses
- Accelerate IT/OT convergence, enhance efficiency in delivery of critical infrastructure services. • Create a competitive advantage, foster innovation, enable SMBs and large companies to monetize
- Enable suppliers of IoT devices to become smart-connected-secure IoT suppliers and service providers
- Enable the creation of connected ecosystems for end-to-end monetization and IoT growth
- Financial incentives to companies that market trusted products
- Require contractors and suppliers to follow traceability standards
- Establish a certification process for electronics products to meet trusted traceability standards
- Facilitate partnerships with industry associations develop guidelines and best practices

Supporting Recommendation 14.9: Promote traceable and trusted IoT network ecosystems made of devices, systems, networks, and personas operating in connected IoT environments

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

- Promote interoperability programs for networks to operate securely and reliably
- Encourage the development and adoption of secure, trusted and interoperable IoT solutions
- Work with industry, academia, promote innovation and R&D

Supporting Recommendation 14.10: Accelerate Evolution of Trusted Digital Threads Across Value Chains

Accelerate evolution of trusted digital threads across value chains by incentivizing companies to digitalize their workflows and link their data IDs to marketplaces. Increase visibility of a product's lifecycle and reduce risk of cyber attacks, counterfeits, recalls.

- Improve efficiency, reduce costs, manage vulnerabilities, increase differentiation, and promote innovation & data monetization.
- Enable data marketplaces that create business opportunities and drive new revenue streams
- Speed adoption by linking digital threads (DBOM, HBOM, SBOM) to protect proprietary IP but enable value chains to monetize
- Develop educational/training programs on digital threads
- Establish guidelines to create a digital thread data sharing.
- Incentivize companies to digitalize their workflows
- Promote collaboration PPPs for digital thread enabled apps
- Fund development of methods to ease digital thread evolution

Supporting Recommendation 14.11: Subsidize Digitalization of Enterprises in the Value Chain

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

- Improve management, efficiency and visibility in supply chains
- Increase security, reliability, and integrity of digital data
- Enable secure ecosystems, SMB opportunities, economic growth
- Accelerate creation of digital thread and IoT services growth
- Facilitate digital transformation over-the-air services & updates
- Enhance supply chain security, integrity of data which will the future digital economies.
- Develop guidelines and criteria for eligibility for the subsidies
- Streamline application/approval process for business subsidies
- Ensure that the subsidies are accessible to all businesses
- Provide incentives for SMBs to invest in digitalization and tools
- Encourage collaboration and community knowledge sharing

Supporting Recommendation 14.12: Promote Creation and Orchestration of Trusted Value Chains

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

- Maintain transparency, trust and accountability across value chain
- Grow economic value through collaboration and accountability among enterprises in value chain
- Protect against vulnerabilities, intrusions, and adversaries
- Ensure that IoT infrastructure is secure, transparent, trustworthy
- Enable shared monetization among stakeholders in the value chain and scalable economics
- Provide incentives for businesses to adopt transparent practices.
- Orchestrate networks of entities to maintain trust through collaboration and accountability.
- Establish guidelines for creating & upkeeping trusted value chains.
- Provide incentives for businesses to collaborate and adopt best practices for transparency

Supporting Recommendation 14.13: Subsidize Orchestrated Public-Private Partnerships Across Value Chains

Subsidize orchestrated Public-Private Partnerships working in parallel to speed adoption of traceability with consistent workflow & hand-off methods. Speed adoption of digital thread & complex supply chain traceability.

- Digitalize supply chains rapidly via PPPs working piecemeal in parallel for slices of the supply chain
- Create resilient and secure supply chains can help businesses drive economic growth.
- Improve supply chain traceability to help businesses reduce risk and increase resilience, which can lead to business and economic growth.
- Subsidize the orchestration of connected PPS across value chains.
- Promote consistent digitalization methods for "receivables-process-deliverables“ for digital threads
- Fund the development of digital infrastructure, training programs
- Provide support necessary for successful PPP implementation.

Supporting Recommendation 14.14: Facilitate Creation of Data-driven Business Ecosystems (Could move to Recommendation 1)

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

- Data-driven ecosystems enable new and scalable revenue streams
- Connected businesses, products and services fuel economic growth
- Data analytics provide insights to improve services and monetization
- Trusted data marketplaces promote data sharing and collaboration
- Platform-based ecosystems enable businesses to collaborate, innovate and scale with network effects
- Data regulations can ensure that businesses and marketplaces drive transparency and accountability
- Develop educational programs for businesses and individuals.
- Raise awareness via campaigns, conferences, and workshops
- Fund incentives for data-driven ecosystems and solutions PPPs
- Foster development of platform-based business ecosystems
- Encourage collaboration and innovation via network effects

Supporting Recommendation 14.15: Evaluate Opportunities, Risks of Using AI in Supply Chains

Evaluate opportunities, risks and regulations for using AI to accelerate supply chain security and resilience or prevent bad actors from tampering. AI-powered traceability can vastly improve supply chain security and resilience.

- AI can increase transparency and prevent counterfeits
- AI can detect supply chain disruptions and reduce risk
- AI used by bad actors in the supply chain can cause major disruptions and harm
- AI-powered attacks are more sophisticated and harder to detect than classic attacks.
- AI can target critical infrastructure
- Promote AI with IoT for end-to-end supply chain traceability.
- Encourage use of AI to analyze supply chain data to create value.
- Promote predictive analytics to anticipate & handle disruptions,
- Provide funding to research AI security and build tools to detect & respond to AI-powered attacks.

10. Conclusion

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

11. References

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

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

Global APEC Cross-Border Privacy Rules (CBPR)

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

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

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

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

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

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

12. Acknowledgements

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

13. Appendices

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

14. Compliance Matrix

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

The IoTAB herein advises working group in the following areas:

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

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

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