



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

January 22, 2024 Pre-Read Draft

IoT Advisory Board Members

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

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

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

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

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

Steven E. Griffith, Executive 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, LLC

Arman Shehabi, Staff Scientist, Lawrence Berkeley National Laboratory

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

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

IoT Advisory Board Members..... 2

Executive Summary 7

Introduction..... 8

Background..... 12

 Specific Applications of IoT..... 21

 The Current State of IoT..... 31

 The Future of IoT..... 38

Findings of the IoT Advisory Board..... 49

 General findings..... 49

 Industry findings..... 50

 General Findings – Specific Considerations 51

 Industry findings..... 90

 Smart Infrastructure..... 95

Establishing a National IoT Strategy..... 112

 Key Recommendation 1.1: The IoTAB recommends a strategic national approach for taking full advantage of the opportunity presented by the IoT. 112

Modernizing IoT Infrastructure 117

 Equitable and Responsible Data Sharing 117

 Key Recommendation 2.1: The government should foster policies that encourage responsible and equitable sharing of IoT data and thereby drive economic growth, societal benefits, and sustainability..... 117

 Consistent and Resilient Interoperability..... 121

 Key Recommendation 2.3: The government should establish methods to foster interoperability for IoT technology, including through the use of consistent models, protocols, application interfaces, and schemas..... 121

 Promoting Existing Methods..... 127

 Key Recommendation 2.4: The government should promote collaborative development across industries to adopt existing industry standards and protocols. 127

 Key Recommendation 2.5: The federal government should expand and improve programs that ensure availability, reliable and sufficient connectivity among and between IoT devices in all areas of the country. 132

Establish Trust in IoT 137

Cybersecurity Improvement..... 137

Key Recommendation 3.1: The Federal Government should provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach..... 137

Data Privacy Regulation..... 145

Key Recommendation 3.2: Congress should pass comprehensive federal privacy legislation. 145

Data and Privacy Policy..... 146

Key Recommendation 3.3: The White House and Congress should facilitate/support the development of a Data and Privacy Policy Framework..... 146

Privacy Protections and Transparency for IoT..... 151

Connected IoT-based Supply Chain Logistics 159

Key Recommendation 4.1: The government should monitor and evaluate progress of IoT adoption for supply chain logistics..... 159

Public and Private Partnership..... 161

Key Recommendation 4.2: The government should 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..... 161

Key Recommendation 4.3: The government should support trusted architectures and conduct a limited pilot to assess the value of trusted digital threads for provenance and traceability across the supply chain..... 168

IoT Leadership / Government capabilities..... 177

Establish Government Capabilities..... 177

Key Recommendation 5.1: The federal government should consider incorporating secure and updated IoT applications and systems into its own facilities, assets, and operations. 177

Enabling Recommendation 5.1.1: The government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems. 177

Leading by Example: Improved Use of IoT in Federally Funded Projects..... 180

Key Recommendation 5.2: The government should lead by example by promoting and enabling the use of IoT in those projects that are funded in full, or partially, by federal offices..... 180

Leverage Federal Grants And Programs To Improve IoT Technology Use..... 182

Key Recommendation 5.3: The government should consider new financial models for sustaining and supporting programs when considering IoT project feasibility. 182

Leading the Way for IoT Adoption in Agriculture..... 185

Key Recommendation 5.4: The federal government should implement sector-specific actions to further promote IoT adoption in the Agriculture sector..... 185

Leading the Way for IoT Adoption Through Smart Cities 195

Key Recommendation 5.9: Preliminary Text: The government should implement specific actions to further promote IoT adoption through smart cities.]..... 195

Leading the Way for IoT Adoption for Public Safety200

Key Recommendation 5.10: The government should implement specific actions to promote IoT adoption that will improve public safety.200

Leading the Way for IoT Adoption for Health Care.....200

Key Recommendation 5.10: The government should implement specific actions to promote IoT adoption in the health care industry.]200

Sustainability / Environmental Monitoring208

Key Recommendation 5.11: The government should implement specific actions to promote IoT adoption that will improve sustainability and environmental monitoring..... 208

Smart Transportation..... 216

Key Recommendation 5.12: The government should implement specific actions to promote IoT adoption in Smart Transit and Transportation..... 216

International Leadership 219

Key Recommendation 5.14: The government should lead international efforts related to the adoption, implementation, and promotion of IoT. 219

Small Business Leadership.....223

Key Recommendation 5.15: The government should accelerate IoT technology adoption as well as manufacturing for small businesses and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them.....223

Research to Support the Future State of IoT 227

Key Recommendation 5.16: [Preliminary Text: The government should consider research in the following areas to support the future state of IoT. [For Board Review - Proposed by Benson]..... 227

Fostering an IoT-Ready Workforce..... 231

Key Recommendation 6.1: The government should invest in and promote IoT-related aspects of education and workforce. 231

Conclusion 239

References.....240

Acknowledgements.....240

Appendices 241

 Appendix A: IoT Stakeholders..... 241

 Appendix B: Leveraging the CHIPS Acts and IoT for Supply Chain Traceability247

Table of Abbreviations 267

Compliance Matrix..... 271

Executive Summary

[this will be drafted after other sections are complete]

Introduction

The United States is undergoing a profound transformation - one that is driven by economic, societal, technological, and cultural innovations brought about by the advancement of the Internet of Things (IoT). This fourth industrial revolution intertwines connectivity and digital innovation with the opportunity to drive a revolutionary transformation across our nation.

We begin with three different stories all illustrating a possible future glimpse into industry sectors that could be radically transformed by the evolution of Internet of Things (IoT) technologies today. These stories offer glimpses into a future transformed by the IoT - a future where agriculture thrives in harmony with nature, supply chains operate with unimaginable efficiency, public safety is bolstered by intelligent systems, transportation flows seamlessly through smart cities, and healthcare becomes personalized and preventive.

These stories are illustrative yet showcase the scale of today's technologies into a vastly transformative edge for the benefit of our society tomorrow. We then peer into the impacts of such transformations and the incredible areas of US economic prosperity such advancements could provide our future nation for all Americans.

Future Glimpse into Agriculture and Environmental Monitoring

The year is 2060. A rural farmer in the Midwest of the US stands amidst her thriving fields, despite the local effects of climate change over the last decade. This is a seemingly testament to the transformative power provided by the advancement of IoT in agriculture over the last few decades. Gone are the days of mostly manual labor and unpredictable weather without efficiency to risk management.

Invisible sensors provide real time inputs about the soil on moisture levels, nutrient composition, and the balance of microbial life. Drones, no longer mere tools of observation, scatter across farm sky, equipped with advanced bio-scanners that identify potential threats and optimize resource allocation with pinpoint accuracy. Self-driving tractors zig zag across the field in full automation guided by AI algorithms that orchestrate every aspect of the farm with meticulous precision. This is not just a farm; it's a living laboratory, a model of sustainability that thrives in harmony with the natural world.

Looking back from today, how do we embrace the evolution of today's early-stage IoT technology like sensors and drones to achieve this tomorrow land farm? The widespread adoption might come slow at first but then with accelerating possibility given the proliferation of affordable sensors across every aspect of farm operations, the rise of robust data networks to enable seamless communication and remote

monitoring, and the convergence of data driven decisions from AI automating outcomes in real time. These technologies, once seen as mere concepts, are poised to revolutionize the way we grow our food and bring food to the table from farms, making the supply chain itself more sustainable, efficient, and personalized.

Future Glimpse into Public Safety and Smart Transit

The year is 2065. An urban officer patrols the streets of the large metropolitan city where public safety and smart traffic are more autonomous to the interconnected nature of technology. Gone are the days of slow response times, limited situational awareness, and unpredictable traffic patterns. In their place, a network of intelligent sensors and AI algorithms work tirelessly to keep the city safe and flowing smoothly.

Embedded sensors embedded in roadways monitor traffic flow in real-time, automatically adjusting traffic signals and optimizing routes to minimize congestion. Smart cameras and drones alert law enforcement towards suspicious activity and traffic incidents in real time. The live feeds from nearby cameras and other IoT devices can even communicate directly within a larger ecosystem and give coordinated responses to law enforcement and public safety organizations in the vicinity.

Today, a fire has erupted in a high-rise apartment building, trapping residents on the upper floors. The building itself is encased with smart technology. Sensors within the building detect the blaze, automatically activating its integrated fire suppression system and activating sprinklers. Drones equipped with heat sensors arrive to the building and scan for trapped individuals to guide firefighters to their location. Additionally, all law enforcement and public safety personnel have on their advanced smart suits with their own sensors for their localized vicinity and as they join together they receive in unison real-time data on the fire's location, the location of the trapped individuals and each other, and the actions currently underway from all parties displayed on their artificial reality displays embedded in their helmets and information in their earpieces.

Looking back from today, the transformation of today's skyline seems like science fiction. Yet, it was built upon the proliferation of today's low-cost sensors across city and traffic ecosystems, the converge of hyperconnected IoT ecosystems of different types of devices monitoring different types of data processed by AI algorithms for automated real time responses. These technologies, once seen as futuristic concepts, have now become the backbone of a safe, efficient, and sustainable city, fostering unprecedented levels of security and mobility.

Future Glimpse into Healthcare and Medicine

The year is 2070. A doctor interacts with a holographic display, analyzing real-time data flowing from her patients' embedded biosensors. Strides in technology have empowered healthcare professionals to see the unseen, intervene before the symptoms, and personalize medicine with unparalleled precision.

Biosensors are tiny, intelligent devices that continuously monitor vital signs, blood sugar levels, and even hormonal balances, providing a real-time snapshot of individual health. Microscopic pressure sensors embedded in the heart monitor its function and rhythm, detecting potential issues before they manifest as symptoms. Bio-implants in the brain track neurotransmitter activity, offering insights into mental well-being, sleeping patterns, and personalized interventions for anxiety, depression, and age-related issues like cognitive decline.

Predictive algorithms flag potential health concerns before they even manifest, allowing for preventative measures and early interventions into what were once considered chronic illnesses. In-home robots assist with medication adherence and provide personalized care instructions, empowering patients to manage their own health more effectively with optimism lessening the strain on the medical field to more serious issues for physical doctor office visits. These same data streams if consented provide real-time data feeds to researchers in the medical field looking to run at scale optimized AI algorithms and models to spin studies on predictive treatment protocols and insights for pharmaceutical companies to develop new classes of drugs, both at scale.

Looking back from today, the early stages of IoT devices like wearables and sensors, coupled with the rapid advancement of AI and data analytics, and the evolutionary integration of embedded biosensors enable human-machine interaction evolution to healthcare delivery. These technologies, once in their infancy, have now woven themselves into the very fabric of healthcare, transforming it from a reactive system to a proactive and preventative field at scale.

Areas of US Economic Prosperity

While these scenarios still seem futuristic, they are embedded in the fabric of innovating today's infrastructure with evolving IoT technology. Today's IoT technology has not yet reached its pinnacle of potential nor are its benefits realized at scale. We recognize three impacts to be made:

- There must be a larger vision to enable a more resilient nation with advanced technological capabilities to provide economic prosperity to Americans.

- There must be continued research and funding into these IoT technologies and their applications across market sectors to innovate into tomorrow's nation and societal benefits.
- There must be a collective action and a nationwide commitment to bridge the gap between the present and a promising future.

In our global ecosystem, all developed nations seek these same advantages. Consequently, the adoption of IoT is not just an option, it is an imperative for the United States. It is a call to action to embrace a future where connectivity transcends boundaries, propelling our economy to new heights, fostering societal well-being, and ensuring that America remains at the forefront of global innovation.

Despite the unlimited potential and benefits of this transformation, a number of significant challenges and barriers stand in the way. It is imperative that we embrace the potential of IoT, acknowledge and overcome the challenges, and act with deliberation and urgency to realize its benefits for our economy and society. We must act with the same characteristics that built our nation - lead with vision and innovation, execute with passion and relentless tenacity, and persevere with unwavering commitment for the betterment of all Americans.

This report contains our findings and groups actionable recommendations under overarching themes that serve to guide the US towards an IoT-empowered future. This includes experiences and perspectives from a cross-section of industry, local government, academia and other private-sector experts. We urge the Federal Working Group to study our recommendations and adopt those that will best serve the needs of this nation.

Background

In January 2020, 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 Committee 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). Specifically, this charter requires the following:

4. Description of Duties. The Board shall advise the Working Group with respect to --
 - a. 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;
 - b. 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;
 - c. 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;
 - d. 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;

- 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;
- e. the opportunities and challenges associated with the use of Internet of Things technology by small businesses; and
- f. 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.

In addition, the charter provides for the following:

- The Board will submit to the Internet of Things Working Group a report that includes any of its findings or recommendations. The report will be administratively delivered to the Internet of Things Working Group through the Director of the National Institute of Standards and Technology (NIST).
- The Board shall set its own agenda in carrying out its duties. The Working Group may suggest topics or items for the Board to study, and the Board shall take those suggestions into consideration in carrying out its duties.
- The Board will function solely as an advisory body, in accordance with the provisions of FACA.
- The membership of the IoTAB consists of sixteen members (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.



Introduction to the Internet of Things

The Internet of Things (IoT) is composed of devices embedded with sensors and actuators that are connected to the internet to react to and influence physical actions in the real world. As a result, the IoT can be seen as a collection of disparate technologies that work together to create innovative outcomes.

From a technology perspective, IoT have sensors that collect real world data and actuators that perform actions in the physical environment based on the processing of the data collected. IoT data is either processed locally on the device, by an on-premises processor, or sent over the internet to be handled off-premises. For example, simple commands for a device's physical actions, such as “increase temperature” or “unlock the door,” may be generated locally or sent down from the central processing. The infrastructure of the internet is extended to individual devices through various existing technologies including Bluetooth, Wi-Fi, LoRaWAN, and traditional cellular and mobile broadband solutions.

A high level IoT technical architecture is shown below in Figure 1.

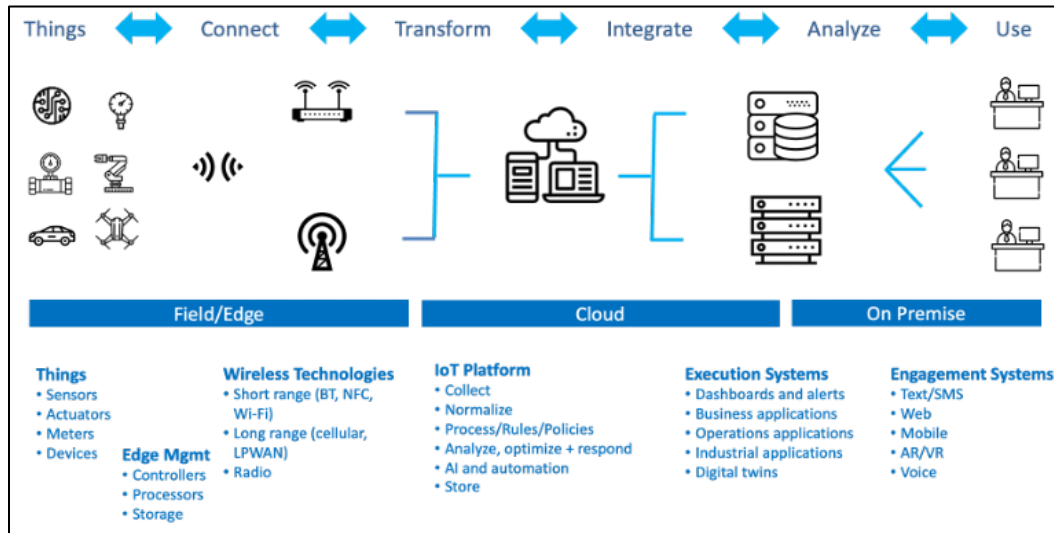


Fig. 1 - High Level Internet of Things Architecture

From an economic perspective, adding sensors and actuators to the internet yields value from doing old things in new ways and seeing new things done in ways that were not possible before. For example, a systematic literature review of 122 different descriptions for IoT in 'Revisiting IoT definitions: A framework towards comprehensive use'¹, found that focus largely centered on a technological standpoint. Yet the authors emphasized that the better viewpoint would be to start with the user (or needs) and the value that could be created by the IoT (application to business ecosystems).

The authors also highlighted that some value is created in part by 'things' themselves and that value created could be monetary or non-monetary. The diagram below highlights the user and services represented at the bottom. The authors emphasized that the first step is to define the value to be exchanged by describing the services offered and then to analyze what kind of information is needed to create value and what physical object can obtain it. Above that you have the data and the data exchange and management protocols over the internet that would handle the specifics from a technological perspective as examined in the earlier architectural diagram.

¹ <https://www.sciencedirect.com/science/article/pii/S004016252200155X>

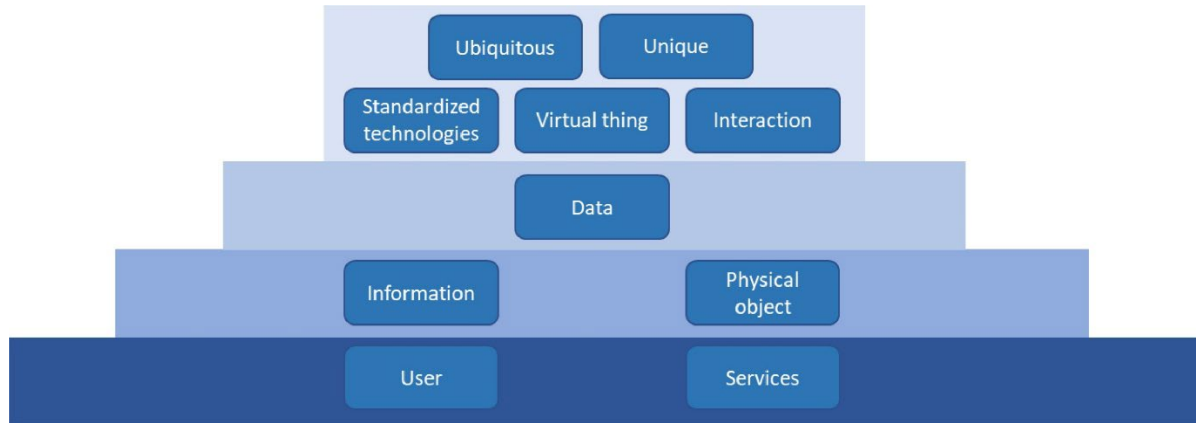


Figure X - Design flow for a value-based IoT system

The benefits from IoT in this way would be realized from the value created downstream closer to the device and the value created upscale as processed at scale resulting in better decisions and value outcomes for localized applications and applications at scale to the collective needs of the users (as provided by the services rendered). In looking at IoT in this perspective of driving value by creating new opportunities, we can see cost avoidance, increased efficiencies and productivity, reduced variability and waste, and the creation of new classes of data-enabled products and services.

Figure 2 below shows an example of how this is possible with the example of a product manufacturing process enhanced by IoT.

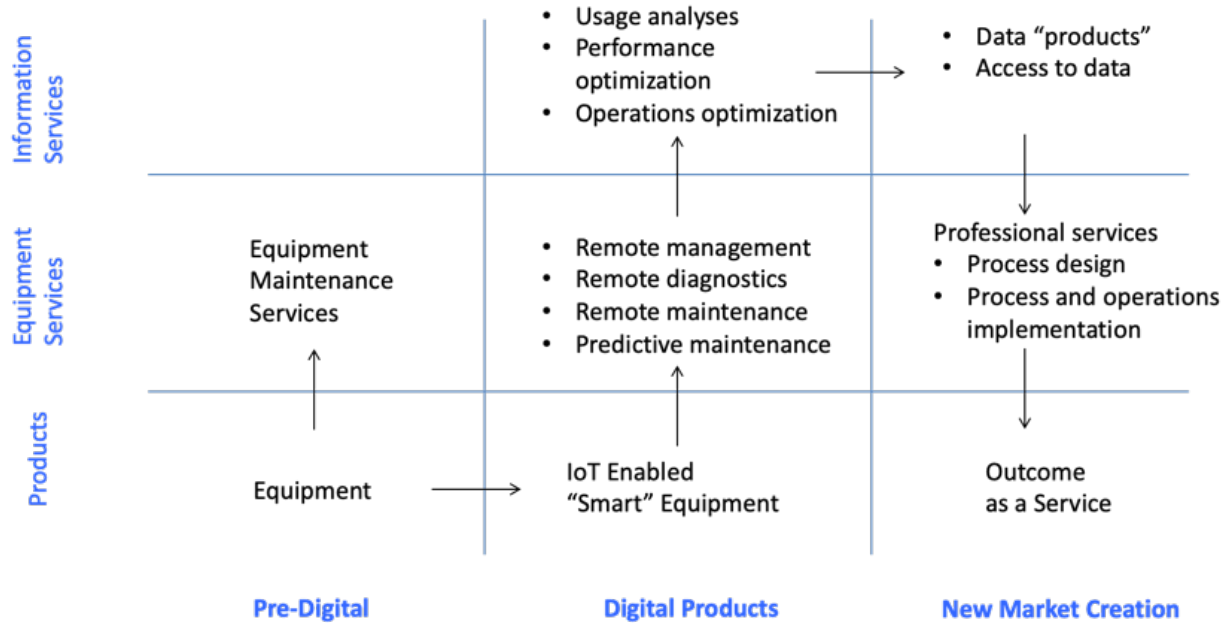


Figure 1: IoT Example: IoT-Enhanced Manufacturing Process and Resulting Opportunities

Prior to IoT, equipment dealers traditionally sold machinery, spare parts, warranties, maintenance contracts and installation and repair services.

The addition of IoT to the equipment creates new capabilities and value for both buyers and dealers. These "smart machines" allow dealers to offer new services and existing services in new ways. For example, onboard IoT sensors allow a dealer's technicians to monitor and diagnose their customers' machinery remotely and avoid an onsite visit. Predictive algorithms driven by IoT sensor data alert technicians when maintenance and repairs are needed, order a replacement part and then schedule a technician to replace the part. This helps the customer avoid unplanned machinery downtime and maintain operational productivity.

At the same time the IoT sensors collect large amounts of data, including machinery usage data from its entire customer base which is aggregated by the manufacturer to understand how their machines are used. This information is analyzed by company engineers to create new services and applications that are sold to the customers. For example, the information can be used to create performance optimization software and consulting services. Customers purchase these new information products and services because it further enhances their operational productivity, reduces inefficiencies and enables them to take on larger jobs.

For example, in a manufacturing context, the data and insights collected from "smart machines" can be aggregated, packaged and sold to lubricant vendors, who use the information to create more effective premium formulations. The data can also be

purchased by insurance companies who use it in a way that minimizes on-the-job accidents. Consultants use the same data to help the factories plan and implement operational process improvements.

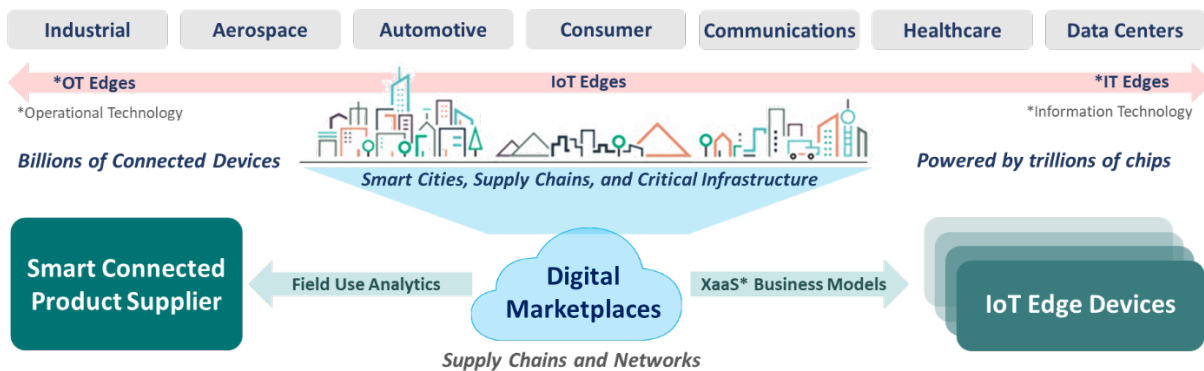
Finally, “smart machines” provide factories with the capability to create innovative new businesses, such as “Manufacturing as a Service”. With full visibility into the actual utilization of their production equipment, factories can offer excess capacities and capabilities to customers. The “uberization” of factories turns manufacturers into “manufacturing utilities” to offer contract manufacturing at agilities, scales and efficiencies unmatched by traditional factories.

IoT Can Transform Business Models

[Note: this is some content inserted from Tom’s findings/edits. There may be some duplication, but Tom’s content has a lot of detail, some of which can substitute and/or complement some of the content above. It is placed here for editor review and possible use. I think we can use his content to answer the question What can or does IoT do?]

IoT connectivity changes product economics. To take advantage of the IoT potential, product suppliers must transform their business to become smart-connected product suppliers enabling new services models and revenue streams.

The 2021 McKinsey report classification of IoT Applications as “settings” (or environments) indicates that IoT vertical markets should be considered in the broader context of connectivity among **smart cities, critical infrastructure, and supply chains**. From an IoT edge use case perspective, the types of enterprises and personas dealing with IoT use cases vary across various vertical markets that serve these environments.



For example, in **Industrial IoT** connected devices and process sensors are managed by information technology (IT) and operational technology (OT) professionals. In **Consumer IoT** connected devices with embedded sensors are managed by users or device makers. And in **Compute IoT**, connected devices in data centers are exclusively managed by IT professionals.

Connectivity creates opportunities for product suppliers to change their mindset about growing their business. Instead of viewing their business as being suppliers of smart-connected products, IoT leaders view their business as **being smart-connected suppliers** to their customers using their products. Being a connected supplier, provides several benefits:

1. **High Visibility on Product Field Use:** IoT connectivity provides real-time insights into how customers use products, allowing suppliers to gather valuable data on usage patterns, performance, and potential issues.
2. **Remote Lifecycle Management:** Over-the-Air (OTA) updates enables remote management of devices and software, allowing suppliers to deliver improvements, security patches, and new features without physical intervention.
3. **Reduced Support Costs and RMAs:** IoT-connected devices enable proactive issue detection and troubleshooting, reducing the need for customer support and costly returns Return Merchandise Authorizations (RMAs).
4. **Lower OPEX, Higher Differentiation:** Operational expenses (OPEX) can be minimized as suppliers gain greater control over product performance and maintenance. Moreover, IoT capabilities help them differentiate products and increase market share.
5. **Hardware as a Service² Business Model:** IoT facilitates the introduction of new revenue streams through subscription-based models, offering services like remote monitoring, predictive maintenance, and data analytics as value-added services.

IoT Can Transform Business Ecosystems

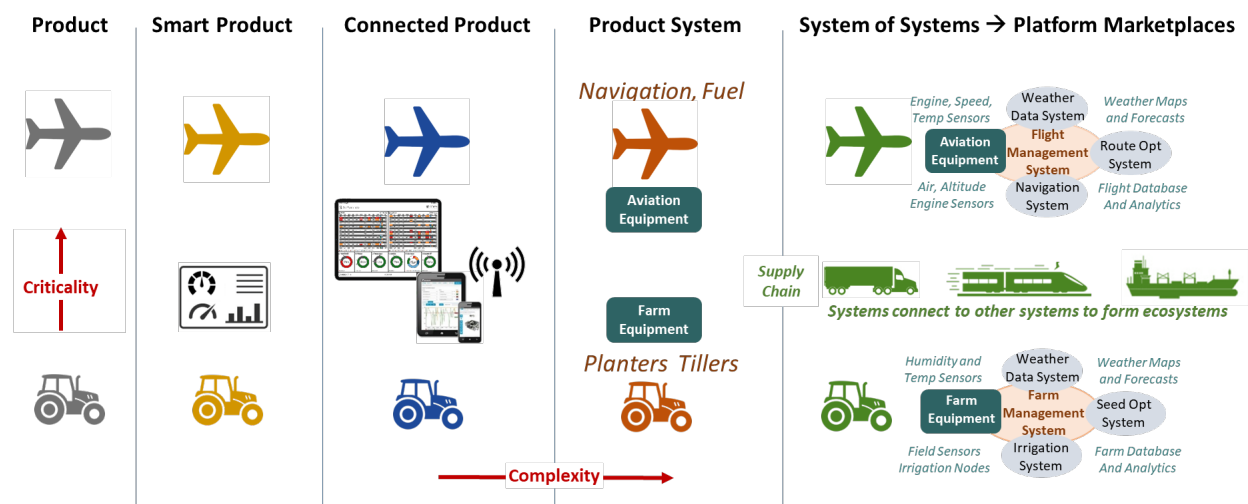
[This section below also came from Tom's findings edits. This section is more visionary, and we should have some statement saying this is one possible, but speculative and visionary view of where IoT can take the economy.]

² Deloitte - <https://www.linkedin.com/pulse/unlock-limitless-possibilities-empower-your-customers-rochak-sethi/>

Finding: Connectivity changes product-based businesses to platform-based businesses with smart-connected products and ecosystem partners delivering higher value end-to-end solutions compared to individual parts sold separately.

Connectivity changes products and businesses by enabling the evolution of solutions and partner ecosystems. Technology adoption rates vary based on vertical market sophistication and ability of enterprises to embrace new technologies and “Cross the Chasm³” that creates new markets (Innovators, to Early Adopters, Early Majority, Late Majority, Laggards).

Connectivity accelerates adoption of IoT. Smart, connected products reshape competition within industries and expand industry boundaries. The basis of competition shifts from discrete products to product systems to systems of systems, to platform ecosystems and marketplaces⁴.



Businesses evolve products into platforms by combining existing products with technologies from other suppliers and forming partnerships for end-to-end solutions. Complex system-of-systems and solutions require collaboration and business connectivity platforms that incentivize businesses to participate and share the innovation burden and economic value delivered.

Smart-connected product businesses evolve into solutions platforms. The similarities of how connected product businesses evolve into platform businesses are striking. Just replace the tractor with a plane, and the peripheral capabilities follow the same principles. Only the application software changes and partnerships with

³ https://en.wikipedia.org/wiki/Crossing_the_Chasm

⁴ <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition>

application experts accelerate adoption. Companies that deliver smart-connected solutions with ecosystem partners capture high value.

Companies whose product platforms connect to other systems will capture more value with ecosystem partnerships by expanding industry boundaries. For example, a coordinated approach across supply chains in transportation and logistics ecosystems will speed adoption, across connected industries accelerate supply chain resilience and enable new solutions.

IoT connectivity drives business transformation for continuous improvements to deliver customer benefits, increase retention, boost differentiation, manage complexity and creating higher value and economies of scale with ecosystem partners.

Specific Applications of IoT

There are several specific applications of the IoT. Each application has its own unique set of use cases, benefits and challenges. This section will highlight a few in greater detail.

IoT for the Consumer

Internet of Things (IoT) technology is becoming increasingly prevalent in consumer products, from smart TVs and wearable devices (fitness trackers, smartwatches), to products that are typically not thought of as “consumer electronics”, such as refrigerators and door locks. These “smart” products connect to the internet and used data create new functionality and enhance existing features and functions to create benefits to consumers in new and better ways. Adoption can bring many benefits to the consumer in many areas, such as:

- **Convenience:** Tracking tags attached to keys, purses and luggage, help locate and recover lost items no matter where they are. Smart appliances can be monitored and operated remotely, allowing consumers to control them from anywhere and anytime. Smart refrigerators monitor grocery quantities, and create weekly shopping lists.
- **Safety:** Connected baby monitors and security cameras monitor activity to protect people in and around the home. Smart doorbells and smart door locks prevent unauthorized access to homes. Security systems, integrated with cameras, monitors, smart doorbells and locks, are connected with call centers to protect the physical safety of residents.

- **Maintenance/Monitoring:** Connected devices can report on their own status, such as an air purifier alerting of the need for a filter change. They can monitor conditions; for example, a smart water leak detector senses water flow through pipes and can send an alert for even small water leaks.
- **Cost Savings:** Smart irrigation controllers can incorporate data about weather conditions and sensor inputs on soil moisture, to optimize the frequency and amount of lawn watering. Connected thermostats monitor and maintain home temperatures while minimizing energy usage.
- **Health:** Wearable devices such as fitness trackers and smartwatches encourage users to track their health data and increase their physical activity, often “game-ifying” the experience to promote regular use. Other connected devices such as body scales, blood pressure monitors, and CPAP machines allow consumers to see trends in their data, improve compliance, and optionally report back to the health provider.
- **Entertainment:** Consumers stream a wide selection of video and audio content on their smart TVs and wireless speakers, and connected cameras inside the home can provide hours of entertainment watching and interacting with house pets remotely.

Despite these potential benefits, IoT is uncharted territory for many consumers. The connected nature of IoT products, the collection of data, and subscription pricing present challenges for the consumer:

- **Cybersecurity:** The number of devices connected to a home network increases the potential cyber-attack surfaces, and as a result, the security of the home router and of all the devices connected to the network becomes a critical link. There are particular concerns around child safety, such as intruders on baby monitors or smart speakers.
- **Privacy:** IoT devices collect sensitive and non-sensitive user data. IoT device cybersecurity vulnerabilities may allow this data to be accessed by cyber-criminals. The collected data may also be used by product manufacturers and other third parties in an undisclosed or unauthorized manner, or in a manner that may lead to adverse outcomes for the consumer.
- **Usability:** Not all consumers are technically or digitally tech-savvy, and many current IoT products are difficult to set up, use, troubleshoot and maintain without technical knowledge. In some cases, the user experience and user interfaces are not intuitive, making the product hard to use and realize benefits from.

- **Subscription pricing:** Consumers are accustomed to buying a product and paying once. Some IoT products offer a limited set of features that is available on a one-time purchase price, while other features are only available on a subscription basis.

Making a traditional “dumb” product “smart”, such as a door lock, adds complexity, risk and cost to a product that consumers possibly felt “was working well before”.

Robust adoption and realization of its associated benefits will depend on consumer understanding, trust and perception of value of IoT. Continued efforts by industry and government to support initiatives, such as the U.S. Cyber Trust Mark labeling, help to alleviate consumer concerns and facilitate adoption.

IoT in the Smart Home

Today’s homes are becoming increasingly digital and connected. Digital networks and telecommunications systems join HVAC (heating, ventilation and air conditioning), plumbing, and electrical systems as essential infrastructure of a functioning home. Broadband Internet connects these homes with a variety of services, including news, entertainment, business and government services, education, and healthcare.

The connected home contains a variety of disparate digital systems, including audio/video (television, receivers, DVD players, media servers, etc.), security and access (alarms, cameras, electronic doorbells, digital door locks, etc.), HVAC (thermostats, fans, etc.), energy management, and automation (lighting, windows, blinds, garage doors, irrigation, etc.). These systems operate as individual systems, and sometimes in an orchestrated fashion through a central home control and automation system.

IoT adds intelligence to this connected home in multiple ways. Sensors monitor a variety of conditions around the home, while the data collected is routed to a cloud data center and analyzed by software algorithms to create optimized responses. Homeowners can access the information and interact with the home remotely through a website or a mobile app. IoT-enabled home systems provide significant improvements in energy efficiency, occupant comfort, security, and other functions.

Smart home technology is diverse. The capabilities of IoT-connected products for a smart home can generally be classified into four main functions: monitor, control, optimize, and automate. Some smart home applications perform one function, while others do more.

The potential benefits include greater comfort, convenience and security with reduced energy consumption. Other benefits include:

- **Increased awareness of home condition and activities through monitoring.** IoT-connected devices monitor the condition of a home and inform the

occupant of abnormal conditions or take appropriate automated responsive actions. For example, pool safety is a concern for families with young children. Connected video cameras monitor the swimming pool, alerting residents to unaccompanied children entering the restricted area. Another important smart home application is the use of IoT to monitor the health and safety of elderly residents living alone. In-room microphones detect the sound of falls or cries for help, notifying family members and caregivers. In-room proximity sensors paired with algorithms monitor resident movements throughout the home, and alert caregivers of unusual patterns of activity or inactivity. Another common smart home IoT application is an outdoor air quality monitor. These monitors detect the pollution levels of the outside air and share that information on a website. This allows the community to understand the current air quality and take the necessary precautions, such as staying indoors or refraining from heavy physical activity.

- **Remote access, control and autonomous operation.** The connected nature of IoT technologies allows users to remotely control and operate smart home devices and equipment. For example, a resident can unlock a smart door lock remotely to allow a guest into the home. A resident can turn house lights on and off through a control panel in the home, or remotely through a mobile phone app. Smart home applications can be controlled manually, or autonomously in response to pre-set threshold conditions or intelligent algorithms that learns from specific patterns in data. A smart irrigation system turns off the garden sprinklers when it senses rain or delays operation if soil moisture levels are high. A IoT-enabled HVAC system automatically resets to lower setpoints when it senses no occupants at home.
- **Optimize home operations through intelligence.** The use of data collected from IoT connected devices have made homes more livable, safer, convenient, and economical to maintain. Algorithms analyze the data to optimize the use of home systems. For example, smart HVAC systems can be optimized based on patterns of use, automatically turning on thirty minutes in the morning before first activity and turning off thirty minutes before occupants go to bed, based on historical data. Similarly, a home with a solar panel and battery system optimizes the mix of electricity stored, discharged to the grid, and used by the home users based on past data.
- **Automate functions to increase convenience and simplify tasks.** Home automation platforms integrate various systems together, such as lighting, energy management, blinds, audio video, IoT-enabled systems (appliances, thermostats, etc.) and others. This integration enables the various systems to orchestrate and work together. Combining monitoring, control, and optimization capabilities permits home systems to operate autonomously with little human input. For example, smart home algorithms know when occupants

return each day, and what rooms they used in the house. Sensors detect the resident's car entering the driveway and initiates an automated sequence to open the garage door, turn on the lights in the areas of the house used by the resident, turn on the HVAC systems, turn on the oven, and turn on the television system to the right channel. As the evening progresses, lights in the sleeping portions of the home are turned on while the common areas are turned down. Select appliances, such as the dishwasher and the laundry appliances activate at midnight when the electricity rates are the lowest.

While smart home technologies provide a variety of benefits to residents and homeowners, there are some challenges to using these technologies. These include:

Interoperability. Modern homes are comprised of a variety of mechanical and electrical systems, electronics, appliances, and other equipment. While any single system can be optimized to improve efficiency or reduce operating costs, the real value is when these individual systems are linked together, combined with sensor and external data sources, and then managed as an integrated system. The lack of interoperability between the different systems, as well as similar systems from different vendors, hinders integration and data sharing. Further complicating matters are competing smart home standards that make operating all the IoT connected devices challenging. Recent industry collaboration has resulted in the Matter standard. While the Matter 1.0 standard officially launched in 2022 and promises the potential for interoperability between various smart home devices, there are still many existing devices and systems in the market that are not interoperable and compatible.

- **Privacy.** Smart home technologies collect a lot of information that may be private to a resident. For example, the collected data may contain both personally identifiable information (PII) as well non-PII information. While some data collection is unavoidable in order to offer personalized and relevant experiences and outcomes, smart home users are concerned with how that data is used, stored, and secured, as well as who has access to it.
- **Cybersecurity.** Smart home technologies create new vulnerabilities and attack surfaces in the home network. While home networks are smaller and simpler compared to their enterprise network counterparts, they are also less secure. Enterprise networks are well maintained and updated frequently. In contrast, home networks are seldom updated, configured correctly, and maintained. The integration of IoT devices into this network greatly increases cybersecurity risks. Cybercriminals can penetrate these networks through vulnerable IoT devices and gain access to sensitive homeowner information, as well as plant malware into the devices and network. In other cases, cybercriminals can access IoT devices and intercept the data streams, such as a video feed from a camera system.

- **Subscription Plans.** Many smart home technologies are offered as a hardware purchase and a subscription service. For example, one manufacturer sells a smart doorbell and an accompanying subscription service to access stored video. Because IoT and smart home technologies collect a lot of data, storing growing amounts of data over a period of time is expensive. Many manufacturers, especially smaller ones, are unable to “absorb” that cost and must pass it on to the consumer and homeowner. In other cases, smart home technology manufacturers offer “premium” features on a subscription basis. While there may be justification for these subscription costs, buyers are accustomed to paying once and feel that they are “nickel and dimed” by these subscription services.
- **User Experience.** Smart home and IoT technologies offer benefits to its buyers, but those benefits may not be equally accessible to all. Complex configuration and setup processes hinder less sophisticated owners and require 3rd party installers. It may lead to improperly configured devices that function poorly. In addition, some devices are poorly designed with little thought for user experience. These poorly designed user interfaces (UI) and experiences (UX) discourage users with limited digital literacy from fully accessing and using the technology to its fullest. For example, smart home technologies that are controlled by voice commands can be challenging. The commands must follow a specified format and not in a “natural language” and have trouble accurately recognizing accents.
- **Maintenance and Upgrades.** Smart home technologies must be maintained and updated frequently to stay current, secure and functional. However, some users are hesitant to do so because in an integrated smart home, software upgrades to one component in a system may “break” the integration with other components in the same system or other systems. Repair of this breakage may require reconfiguring of select components in the system and are beyond the capabilities of most users. These “breaks” are more likely between components from different brands. Not all upgrades are performed “over the air” as some must be done in-person. These “truck rolls” are expensive and may hinder upgrading firmware.

IoT in the Industrial Sector

Industrial operations are heavily monitored and controlled in a variety of industries, including energy mining, chemicals, and transportation. These technologies are also prevalent in manufacturing, monitoring, process control and operations, and supply chain management. Many equipment manufacturers use Industrial Control Systems, (ICS), that are used to control processes like manufacturing, product handling, production, and distribution. ICS includes Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and programmable logic controllers that incorporate IoT technologies. These technologies are often also referred to

Operational Technologies (OT). OT is comprised of hardware and software that detects or causes a physical change through the direct monitoring and/or control of industrial equipment.⁵ OT devices are as distinct from ‘consumer IoT’ due to their usage in commercial operations and are not available or readily available for sale to the public.

IoT systems are used in conjunction with existing OT systems to enhance and improve operations. For examples, IoT brings sensors, data storage and integration, data analytics, and machine learning, can be applied to SCADA systems to improve interoperability and coordination among different machines. The sensors collect new data from various equipment and continuously feed the data into the analytics. This way, machine learning algorithms can learn from past data and fine-tune the settings on different machines for thousands or even millions of cycles to reach the optimal point of the entire system. Harnessing IoT in industrial markets brings several benefits:

1. **Increased efficiency in manufacturing operations.** IoT gives manufacturers and industrial operators the ability to automate and optimize their operating equipment efficiency and/or utilization. The use of robotics and automated machinery can boost productivity and help manufacturers streamline productions, reducing unplanned equipment downtime. Using sensors, manufacturers and utilities gain valuable insight into operational performance of pieces of equipment as well as entire systems.
2. **Reduction of errors.** Through digitalization, manufacturers can reduce operational and manufacturing errors generally associated with manual labor. IoT can help reduce errors in operations, even in those operations that are automated like in continuous manufacturing operations. For example, IoT sensors can detect anomalies and/or variabilities in a chemical processing operation and adjust certain parameters to reduce process waste and increase yields. AI and machine learning can do much of the required computing and data analysis and make subsequent predictive recommendations which can improve a manufacturing process.
3. **Predictive maintenance.** IoT technologies can alleviate issues and unplanned machine downtime associated with reactive maintenance. By monitoring equipment performance consistently, industrial operators are able to identify issues before they occur and allows them to schedule maintenance prior to any downtime.

⁵ Wikipedia https://en.wikipedia.org/wiki/Operational_technology

4. **Improved safety.** A fully functioning manufacturing operation that incorporates sensors and other IoT technologies can use the collected data to bolster worker and product safety. Integrated systems can protect workers by providing alerts which could automatically and safely cease operations if an accident is predicted or until an incident is resolved. Safety can be improved with sensors monitoring hazardous conditions and sending alerts when necessary, such as detecting chemical leaks or equipment malfunctions, reducing the risk of accidents.
5. **Cost reduction.** The data provided to manufacturers through Industrial IoT technologies is giving them the knowledge and tools to reduce costs and increase marginal revenue. By using data-driven insights into operations, production, marketing, and sales manufacturers can steer their business into a more profitable direction.
6. **Enhanced Productivity & Quality:** IoT technologies can improve productivity by providing workers with real-time data and insights. Continuous monitoring of product quality can automatically adjust processes to maintain consistent quality levels.
7. **Data-Driven Insights, Reporting, Compliance:** The data collected by industrial devices incorporated with IoT technologies can be analyzed to gain valuable insights. This data-driven decision-making can lead to innovations, process improvements, and a better understanding of customer needs. It can also simplify regulatory compliance by automatically recording and reporting data required for compliance purposes.

The Industrial sector has many existing applicable standards and best practices., As an example, this sector utilizes the ISA/IEC 62443 series of standards and conformity assessment programs that provide a systematic, practical, and holistic approach to address cybersecurity in product development and across the overall product lifecycle, starting at its inception. It's also important to consider how the use cases of IoT technologies in the industrial sector are distinct from IoT technologies used in other sectors. There are a number of reasons for this listed below.:

- **Use/Scope:** IoT in industrial devices are used in settings for manufacturing, transportation, energy, and other critical infrastructure.
- **Utility:** IoT in industrial devices are used for enhancing productivity, improving efficiency, quality and reducing costs in industrial processes.
- **Applications:** IoT in industrial devices are used for industrial applications such as monitoring and control of machinery, inventory management, and supply

chain optimization. These operations may be in harsh environments, require low latency and may operate in long time scales before replacement.

- **Impact:** Cybersecurity breaches in industrial devices with IoT technologies can cause significant damage to critical infrastructure, including production downtime, supply chain disruptions, and safety risks.
- **Life Support:** Some industrial devices with IoT technologies such as medical devices and aerospace systems may involve human safety, and their cybersecurity vulnerabilities can lead to fatal outcomes.
- **Automation:** Industrial devices with IoT technologies are often automated and may interact with other machines and systems.,
- **Reliability:** Industrial devices with IoT technologies must operate reliably and continuously in harsh environments.
- **Privacy and Confidentiality:** Industrial devices with IoT technologies may collect sensitive data, but the privacy concerns may differ based on the application. The data being transmitted and processed in Industrial IoT environments can be highly sensitive and critical to business operations. This includes manufacturing data, process control information, supply chain data, and proprietary intellectual property. Confidentiality in Industrial IoT extends beyond personal information to safeguard critical industrial processes and trade secrets.
- **Interoperability:** Industrial devices with IoT technologies are often part of larger systems and must be interoperable with other devices and systems, including legacy equipment and other operations technologies.
- **Scalability:** Industrial systems with IoT technologies often involve a large number of devices and must be scalable to accommodate growth., whereas consumer systems with IoT technologies may be smaller in scale
- **Attack Surface:** Industrial devices with IoT technologies have a larger attack surface due to their connectivity and may be vulnerable to various types of cyber threats such as hacking, malware, and ransomware.
- **Criticality:** The cybersecurity of industrial devices with IoT technologies is critical for the operation of critical infrastructure.

The advancement of IoT technologies in industrial applications can further amplify the efficiencies of the manufacturing process, allowing for production goals and

outcomes to reach levels of scale that are previously unimaginable and physically attainable. And when properly and responsibly governed and applied, these technologies can achieve these efficiencies while enhancing workers safety and privacy while fostering energy and environmental stewardship.

The Current State of IoT

The adoption of IoT is growing in the United States. One industry analyst estimated the value of the U.S. IoT market to be \$56.3 billion in 2022, growing at 15.6% CAGR and projected to reach \$270.2 billion by 2033.⁶ Research published in the 2021 Microsoft IoT Signals found that 94% of business decision-makers, IT decision-makers and developers at U.S. enterprise organizations (1000+ employees) surveyed are “IoT adopters”⁷, meaning that they are either learning about IoT, conducting a trial or proof of concept, purchasing IoT, or using IoT.⁸ Of this, 27% have projects in the “use” phase, while 78% reported that they are planning to use IoT more within 2 years.⁹

However, this growth is below expectations. Adoption of IoT is hindered by a variety of industry-specific challenges. For years industry projected 10's of billions of IoT units in use by ca. 2022. And in 2014 the World Economic Forum and McKinsey & Co. projected that IoT, and adjacent technologies (analytics, cloud computing, big data and ML/AL) will produce \$9.6 to \$21.6 trillion of value for the global economy by 2022. And Verizon's State of the Market: Internet of Things 2016 report noted, *“The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019, hitting 30 billion in 2020.”* ¹¹ Verizon was by no means an outlier at that time; while numbers varied, most analysts expected this kind of growth over the next few years.

But in 2021, McKinsey & Co. revised the IoT forecast drastically downward, projecting global value of only \$5.5 to \$12.6 trillion, and not reaching those targets until 2030. While the new projection was focused on the top nine categories, it is clear that adoption is not as anticipated. The firm clarified that the 2014 projection was off mainly due to headwinds related to change management, cost, talent, and cybersecurity. They additionally noted factors of slow market adoption of digitalization and cyber-resilience, particularly in enterprises.

And compared to analysts' ca. 2016 estimates, the IoT is nowhere near on target. Verizon said in 2022, *“By the end of 2022, it's estimated that there will be 14.4 billion connected IoT devices worldwide, an increase of roughly 18% over last year alone, with numbers climbing to 27 billion by 2025.”* ¹² Comparing the 2022 estimate of 14.4 BN to the estimate just six years earlier of 30 BN in 2020, clearly something happened.

¹¹ <https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>

⁶ “United States IoT Market is expected to surpass revenues worth U.S.\$ 270.23 billion by 2032: Persistence Market Research Report,” Persistence Market Research Press Release, May 24, 2023. [Link](#)

⁷ “IoT Signals - Edition 3|October 2021”, Microsoft, October 2021. Exhibit 3. [Link](#)

⁸ Ibid. Exhibit 2.

⁹ Ibid. Exhibit 3.

¹² <https://www.verizon.com/about/news/5g-iot-together-changing-our-world>

Analysts a decade ago saw the incredible potential for IoT growth, but could not foresee the barriers to deployment that would significantly slow that growth. Still, the difference is between incredible growth, and moderate growth, as IoT adoption is definitely rising—just not as quickly as predicted.

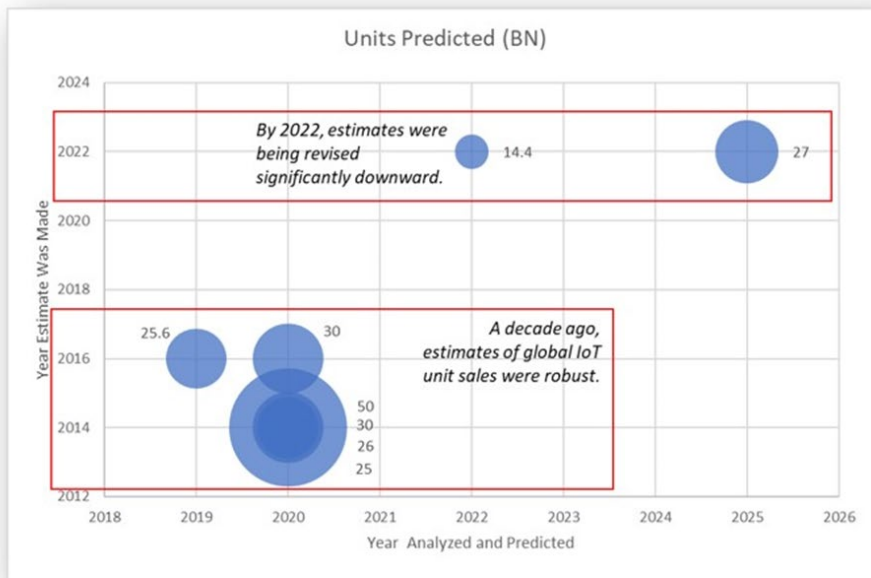


Figure 2: Impact of barriers and other factors ("headwinds") on IoT adoption, based on industry forecasts. Size of bubble is proportional to the estimate.

IoT is used across a variety of industries for different reasons. For example:

- Manufacturing.** The top three reasons for small manufacturers with less than 500 employees (which make up 98.3% of manufacturing companies in the United States), are performance improvement of operational processes, achieving production cost efficiencies and filling labor shortages.¹⁰ A 2022 CESMII survey of manufacturers found that the top five smart manufacturing goals were better manufacturing capacity utilization (65%), lower production costs (63%), improved on-time delivery (62%), operational excellence (61%) and improved quality/reduced quality risks (60%).¹¹

¹⁰ "The Manufacturing Institute–BKD Small and Medium-Sized Manufacturers Survey", The Manufacturing Institute, September 2021. [Link](#).

¹¹ "2022 Smart Manufacturing Market Survey Executive Summary", CESMII, May 2022, Page 4. [Link](#)

- **Agriculture.** IoT helps lessen the impact of labor shortages and augment existing labor resources. A 2018 study estimated that 250,000 farms across the United States were using IoT solutions, with most of those in livestock and crop management. The study also found that up to half of all U.S. farms were interested in purchasing IoT solutions, representing 1.1 million farmers and a potential agricultural IoT solution market opportunity of \$4 billion dollars.¹²
- **Retail.** A 2022 industry survey of 104 large American retailers (with sales of \$500 million and above) by RSR Research reported that the top business challenges driving interest in IoT included competitive differentiation (43%), maintaining margins (41%), operations cost reduction (40%) and operations speed and agility (34%). The top IoT use cases deemed as “very important” centered around inventory accuracy and stock management (82%), fraud and loss prevention (80%), fulfillment center process automation (65%), supply chain process automation (63%), loyalty and personalization (62%) and brand protection and anti-counterfeiting (62%).¹³
- **Transportation and logistics.** One way IoT technologies help create a resilient supply chain is by tracking the real-time locations and quantities of goods and inventory across a network of warehouses and distribution centers, enabling inventory and logistics planners to draw from the most appropriate locations to minimize disruptions.¹⁴ Approximately 95 million telematics devices have been shipped worldwide as of 2021, and is expected to grow at a CAGR of 10.9% reaching nearly 160 million units by 2026.¹⁵ It is also estimated that there are over 130 million units of embedded car OEM telematics units in operation globally as of 2020, and 375 million embedded units by 2026.¹⁶

Adoption Barriers

Although IoT offers the potential for significant economic and societal benefits to the United States, its overall adoption and deeper integration into the economy and daily

¹² [“Nearly 250,000 U.S. Farmers Already Using IoT Technology, Study Finds”, J. Tomas, May 16, 2018. Enterprise IoT Insights. Link](#)

¹³ “A Deep Dive into Retailers’ Views About Rfid and the Internet of Things”, B, Kilcourse and S. Rowen, Retail Systems Research Benchmark Report, April 2022. [Link](#)

¹⁴ “How telematics and the IoT work together to improve fleet management,” Verizon Connect, June 29, 2021. [Link](#)

¹⁵ “Outlook on Vehicle Telematics Hardware Global Market to 2026...”. Global Newswire, July 15, 2022, [Link](#)

¹⁶ “Number of embedded auto telematics units n operation worldwide in 2019 and 2020...”, Martin Placek, Statista, March 23, 2023. [Link](#)

lives of Americans in a larger way has been slow. There are a myriad of contributing reasons, including:

- A lack of national coordination...*[This Finding section is incomplete but has Board members tasked to fill it out]*
- A need for suppliers to adopt new smart-connected-product business models with new services models and revenue streams.
- Various existing policies and regulations at local, state and federal levels.
- An unsustainable inequitable share of access, opportunities, benefits and outcomes from IoT.
- Lack of interoperability hinder integration and communication with other IoT devices and existing systems and processes
- Limited and outdated infrastructure, such as connectivity and legacy systems, to support, operate and scale IoT systems.
- A variety of network connectivity challenges particularly in remote communities.
- Concerns about IoT cybersecurity vulnerabilities that may lead to an intrusion of the user's network, theft of sensitive and proprietary data, unauthorized control of systems, and loss of network access.
- Concerns about privacy involving the unauthorized collection and use of information collected from IoT devices and systems. This information may be used in an adverse and discriminatory manner, limit choice, and create negative outcomes for the user.
- A slow adoption of enterprise digital transformation elements that enable and accelerate IoT benefits.
- A shortage of workers with expertise, digital and data science skills to develop, integrate and operate IoT and IoT enabled systems.
- And a variety of sector-specific challenges

Market Consolidation

There is no “one size fits all” IoT technology. The market is an organically-developing but fragmented ecosystem of sensors, chips and processors, modules, devices and software platforms¹⁷. For example, there were 613 IoT software platforms in the market in 2021, down from 620 in 2019, but up from 450 in 2017.¹⁸ The fragmented nature of the market has created confusion for IoT buyers who have struggled with

¹⁷ ^[1] “IoT platform” is an application or service that provides IoT product suppliers with tools and capabilities that they would otherwise need to develop in-house. Platforms ease development and assist with the product lifecycle after the product is shipped by providing such features as automated software updates or data analytics.

¹⁸ “IoT platform companies landscape 2021/2022: Market consolidation has started,” P. Wegner, IoT Analytics, November 23, 2021. [Link](#)

understanding, selecting and integrating hardware and software from a vast array of technology providers to meet their specific requirements.

Today, this large and fragmented IoT market is consolidating in order to create value for buyers, scale and profitability at the current market levels. Some recent mergers in the news include:

- IoT module maker Telit acquires Thales cellular IoT products company (2022)¹⁹
- Semiconductor manufacturer Semtech acquires IoT technology provider Sierra Wireless²⁰
- Kore acquires Twilio's IoT business (2023)²¹
- Renesas acquires IoT chip and module provider Sequans Communications (2023)²²
- Unabiz acquires IoT connectivity provider Sigfox (2022)²³

Other market players have not achieved the level of success envisioned and have exited the IoT market or cut staff. Notable announcements include:

- Google exiting the IoT services business (2022)²⁴
- Ericsson sells IoT business (2022)²⁵
- IBM shuts down Watson IoT (2022)²⁶
- SAP retires IoT platform (2022)²⁷
- Cisco exits smart city market (2020)²⁸
- Hologram lays off 40% of workforce (2022)²⁹

[This section below is from Tom's findings document. Although Tom calls it a finding, I don't consider it a finding, but commentary that belongs here instead. I just cut and pasted his content verbatim. There is some good content here that supports and complements the above content on consolidation and industry state. Some

¹⁹ "Telit acquires Thales' cellular IoT products to establish Telit Cinterion," R. Daws, IoT News, August 1, 2022. [Link](#)

²⁰ "Semtech Corporation to acquire Sierra Wireless," Semtech press release, August 2, 2022. [Link](#)

²¹ "Twilio Sells Its IoT Business Unit to Kore," J. Stephen, CX Today, April 3, 2023. [Link](#)

²² "Renesas to broaden IoT offering through Sequans acquisition," L. Redins, Edge Industry Review, September 5, 2023. [Link](#)

²³ "IoT firm Sigfox acquired by UnaBiz," A. Wooden, Telecoms, April 22, 2022. [Link](#)

²⁴ "Google to shut down its IoT Core Services from Aug 2023; users seek options," Business Standard, August 18, 2022. [Link](#)

²⁵ "Ericsson quits IoT - agrees sale of loss-making IoT accelerator business to Aeris," J. Blackman, RCR Wireless Business, December 7, 2022. [Link](#)

²⁶ "IBM to fire Watson IoT Platform from its cloud," L. Clark, The Register, November 15, 2022. [Link](#)

²⁷ "SAP IoT Retirement and SAP Asset Performance Management," S. Lee, SAP, October 5, 2022. [Link](#)

²⁸ "Cisco Systems pulls back from smart city push," A. Tilley, Wall Street Journal, December 28, 2020. [Link](#)

²⁹ "Hologram lays off 40% Workforce – 80+ Employees," Layoffs Tracker, June 9, 2022. [Link](#)

duplicate what is here, but there are some new information as well that we could use. There is too much content and some can be cut out].

Commercial IoT platforms are consolidating while partnerships among companies using IoT platforms for end-to-end solutions are growing. New models of platform-based public private partnerships and business ecosystems emerge.

The IoT platforms landscape is consolidating, as reported by IoT Analytics³⁰, with a growing trend in forming end-to-end solutions partnerships using these platforms. This approach accelerates IoT technology adoption by offering incentives to partners who utilize these platforms, which benefits their businesses, creates new workforces, and fuels economic growth.

IoT Platforms are software systems used to develop or manage solutions. IoT platforms are classified into five types: application enablement and management, device management, data management, telco connectivity and management, and IoT-based Infrastructure-as-a-Service (IaaS). Platforms have revolutionized the way we conduct business, have disrupted traditional business models, and have become an important force in the global economy.

Number of IoT Platforms Consolidating

2015	2016	2017	2018	2019	2020	2021
260	360	450	535	620	617	613

Typical IoT Platforms Capabilities

- Application Management
- Data Management/Analytics
- Connectivity management
- Device management
- Application Management
- End-to-end Platforms

Since 2019, IoT Platform companies are transitioning into solutions. Some companies folded, some pivoted their business models, and some transitioned from IoT software tools to IoT solutions. The total number of IoT platforms based in Asia-Pacific (APAC), especially China, grew rapidly from 2019 to 2021, while the number of platforms in all other major regions decreased. IoT solutions partnerships almost always include the top 10 platform companies.

The market for IoT Platforms continues to consolidate with Hyperscalers dominating. In 2023, the top 10 companies controlled 65% of the market, compared to 58% in 2019 and 44% in 2016. Leading Hyperscalers (Microsoft, AWS, Alibaba) continued to outgrow the market with growth rates of 50%+ per year since their platforms enable business ecosystems and scalable revenue streams. Platform-based partnerships successful collaborations for various markets.

³⁰ <https://iot-analytics.com/iot-platform-companies-landscape/>

IoT Solutions Partnerships for Specific Use Cases

John Deere is creating an ecosystem of connected farm machinery, for new **solutions & services** in precision farming and asset monitoring.



Port of Rotterdam is using Watson IoT to connect port Sensors and find more efficient **ways to manage port logistic operations.**



Volkswagen is partnering with AWS & MindSphere to create its Industrial Cloud, **connect its supply chain** and enhance it with a **digital marketplace**



Enel, an Italian multinational Energy company, used C3 AI platform and achieved a 2X performance increase by identifying unbilled energy



Technology Maturity

The technology enabling IoT continues to evolve. IoT is an evolving set of disparate technologies at various levels of maturity. While some are mainstream and mature, others are emerging ~~and immature~~. Technologies such as cloud computing, IoT platforms, containers, supervised machine learning, IoT streaming analytics, cellular IoT and Low Power Wide Area Networks (LPWAN) have reached a certain level of maturity.³¹ Others are “coming up”, including edge data and app platforms, serverless/Function-as-a-Service, cloud-connected sensors, edge AI chips, and low code/no code development platforms and satellite IoT connectivity.³² Still others like data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, QRNG chips, biodegradable sensors, 6G and quantum computing are only just hitting the market or are still in research labs. ~~still “years-out” and require continued research investments.~~³³

Figure out what to do with this content – delete or move somewhere.

Emerging trends for digital platforms require a change in partnership models.

Moving forward, interconnected ecosystems are expected to drive integration between IoT and AI that enables circular economies for sustainability, connected manufacturing, and challenges such as value creation, regulation, and misinformation. Partnerships that serve specific needs like the ones shown here will no longer be scalable. New Public Private Partnerships (PPPs) that align business incentives and industry standards for broader hyper-connected use cases will emerge.

Platform-based business ecosystems driven by Hyperscalers can create enormous value. The key challenge is how to drive scalable collaboration among ecosystem partners in ways that help Small Medium Enterprises (SMBs) grow, instead of their value-add being exploited.

³¹ “55+ emerging IoT technologies you should have on your radar (2022 update),” S. Sinha, IoT Analytics, April 6, 2022.

[Link](#)
³² *ibid.*

³³ *ibid.*

The Future of IoT

From a device deployment perspective, as the physical environment is equipped with more and more sensors, the way those sensors and devices are used will evolve. Many of the devices deployed today largely operate in isolation or “islands”. However, as IoT matures and interoperable technology platforms emerge, the “islands” of devices integrate to form systems of connected devices and larger ecosystems of benefits for a plethora of users.

From an ecosystem perspective, systems of connected devices integrate with other systems to form broader and bigger “systems of IoT systems”. In a smart factory example, individual IoT applications in a factory integrate to create a smart factory. These smart factories connect with others to share data and create a network of smart factories. These smart and connected factories form a virtual factory network that offers “production as a service”. Customers find available factory capacity online and route files and orders to open factories for production. The data from these smart factory networks integrate with IoT applications across industries, such as freight and logistics providers, to coordinate the delivery of raw materials to factories and finished products to distributors and retailers. Finally, the integration of data and operations within and across industries leads to the formation of the fully autonomous factory and supply chain.

From scaling technology from today to tomorrow, we can envision new innovative business models which require partnerships and incentives for growth for all participating stakeholders. Value generated can provide future opportunities through parallel ecosystems or rather the ecosystem at the largest scale to provide better economic outcomes for society. This transformation has already seen things become ‘smart’ and as the data of things is becoming more utilized through the systematic integration of algorithms and analytics. The future is more predicated on the advancement of emerging technologies, the utility and outcomes of those future integrations, and at large a hyperconnected economy with full autonomy by machines. IoT enables new innovative business models which require partnerships and platform-based business and technology ecosystems that incentivize growth for all participating stakeholders across diverse disciplines.

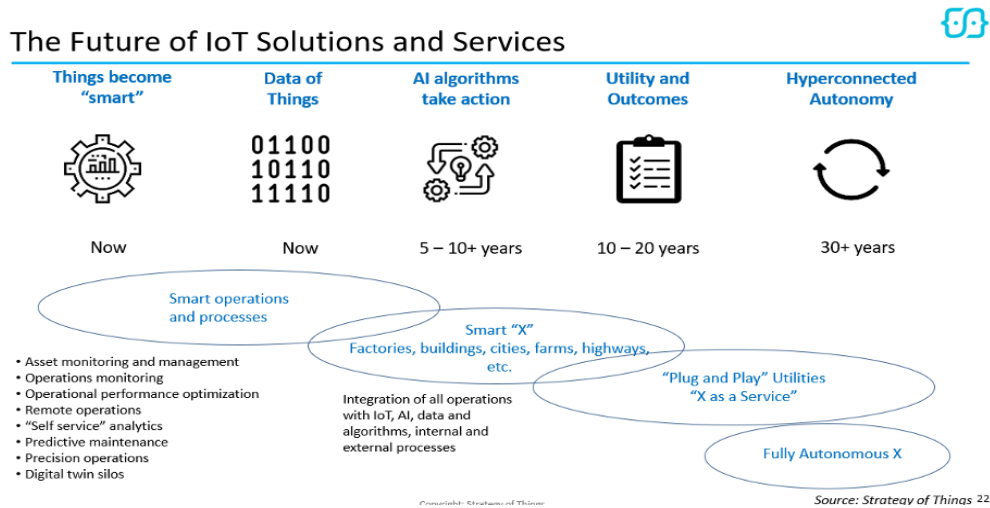
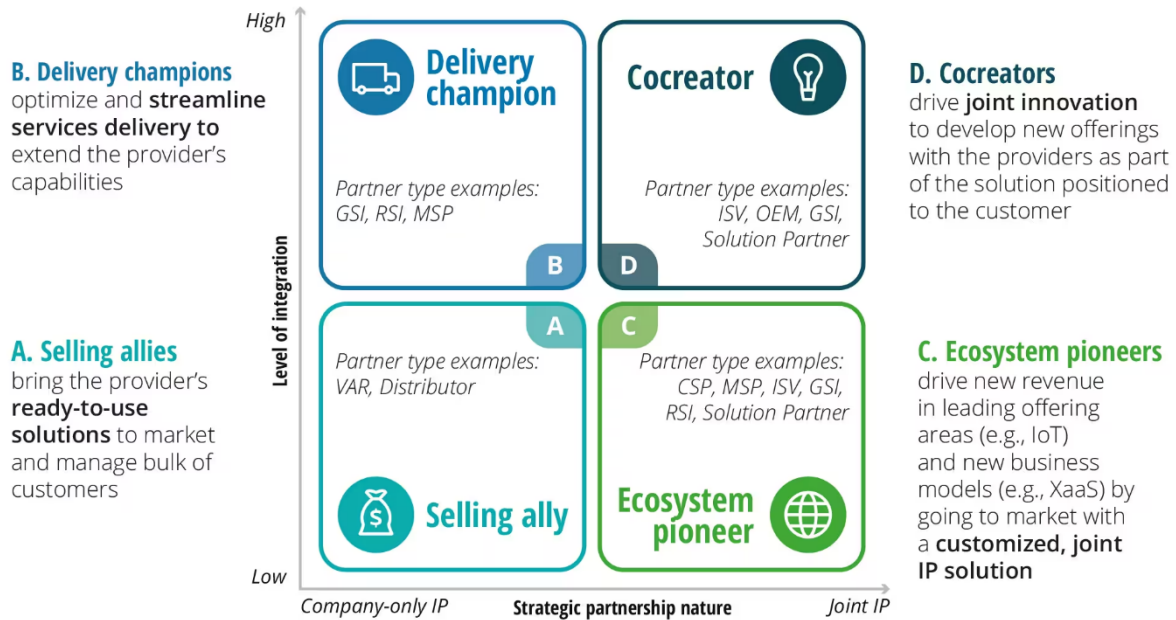


Figure 2: The future of IoT Solutions and Services

IoT enables new innovative business models which require partnerships and platform-based business and technology ecosystems that incentivize growth for all participating stakeholders across diverse disciplines.

Platform-based business ecosystems are proven to grow rapidly and create enormous value. IoT provides opportunities to evolve partner ecosystems that promote business collaboration.

Partner archetypes



Notes: CSP: certified service partner; GSI: global systems integrator; ISV: independent software vendor; MSP: managed service provider; OEM: original equipment manufacturer; RSI: regional systems integrator; VAR: value-added reseller. Solution Partner examples: cloud platform, data management and analytics, IoT.

Source: Deloitte analysis.

IoT solutions require orchestrated business ecosystems with clear roles. Private Public Partnerships (PPPs) including broadline suppliers, innovative startups, and application domain experts can be a catalyst to growth. Orchestration requires re-thinking the roles of ecosystem participants as proposed by Deloitte³⁴, which must be clearly defined to support a collective mix can bridge the gaps between legacy infrastructure and IoT markets to accelerate IoT adoption.

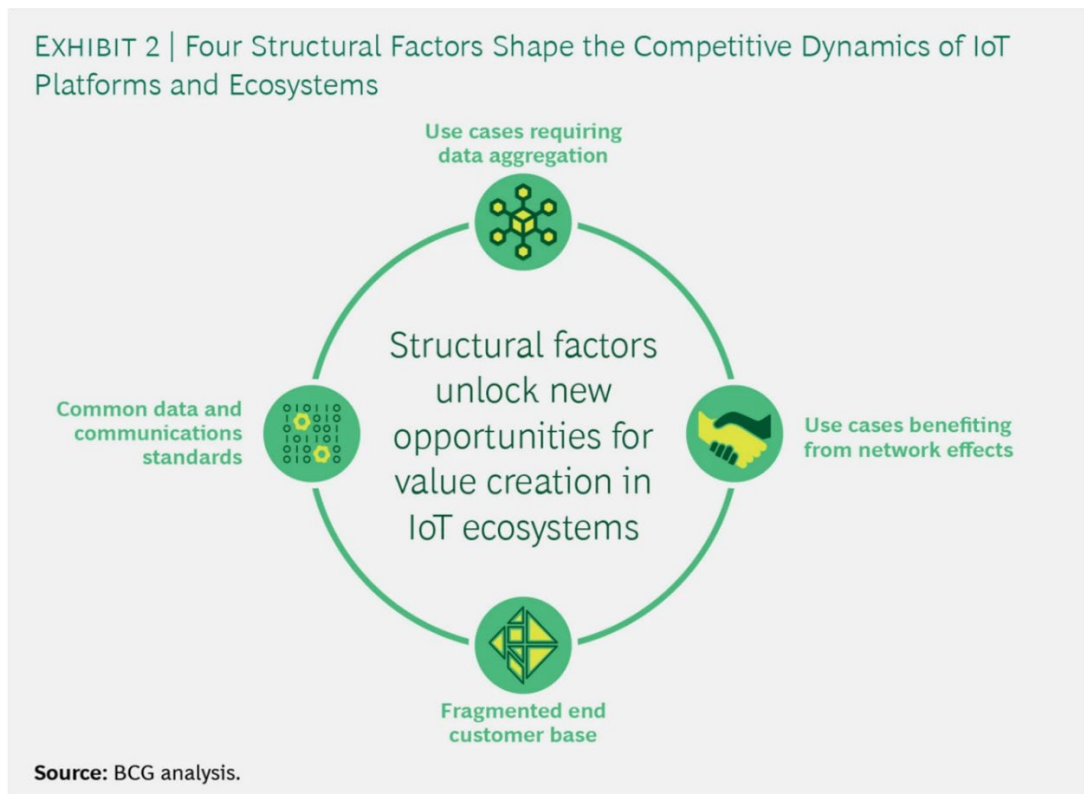
Platform Ecosystem Orchestration Transforms Linear Supply Chains to Value Chains. Boston Consulting Group has published an analysis on how IoT offers a transformative opportunity to shift from traditional linear supply chains to multi-industry value chains³⁵. By aggregating data from products or business processes, industries can create IoT platform³⁶ businesses and ecosystems that serve diverse user bases. These platforms invite contributions from other companies, fostering

³⁴ <https://www2.deloitte.com/xe/en/insights/focus/industry-4-0/partner-ecosystem-industry-4-0.html>

³⁵ <https://www.wallstreetmojo.com/supply-chain-vs-value-chain/>

³⁶ <https://www.bcg.com/publications/2020/value-in-iot-platform-based-business-models>

collaboration and the exchange of data, products, and services, ultimately breaking down industry silos and creating rapid growth driven by network effects³⁷.



Digital platform network effects are key to accelerating growth of business ecosystems. A platform-based digital marketplace can be established by identifying numerous high-value use cases within a single industry or across industries that benefit from network effects. Such marketplaces connect buyers and sellers. As more customers and a wider range of equipment join, the value of the platform grows with more stakeholders and applications. Once a strong market presence of suppliers and buyers is established, third parties introduce digital services.

Tech innovation hubs³⁸ are key for orchestrating ecosystems that accelerate adoption. They provide the ability to orchestrate the right mix of partners for Proof of Concept (PoC) pilot projects that can show the economic value before investing to deploy at scale. Broadline suppliers bring platform orchestration capabilities, startups push the boundaries of IoT with innovation, and domain experts provide real-world relevance optimizing for practical use. Innovative startups and SMB's, especially the ones that are domain experts in specific market applications and application

³⁷ <https://www.wallstreetprep.com/knowledge/network-effects/>

³⁸ <https://www.eda.gov/funding/programs/regional-technology-and-innovation-hubs>

environments, must be incentivized to use Hyperscalers' platforms in ways that help them attract skilled personnel, innovate, and grow open business ecosystems

Tech hubs enable innovative ecosystems to fuel economic, financial, and social benefits. Public-private partnerships (PPPs) led by tech hubs effectively manage risks and deliver scalable solutions that promote economic growth. Innovation hubs bring together diverse stakeholders like R&D institutions, venture capital, incubators, startups, and businesses, fostering innovation, attracting talent, and creating economic opportunities. Tech hubs can lead innovation ecosystem orchestration, emphasizing priorities such as talent attraction, capital investment, strengths identification, and comprehensive support.

Finding: Orchestrated Business Ecosystems enabled by collaborative platforms with appropriate mix of large companies, innovative startups, SMBs and end market domain experts can accelerate IoT adoption and fuel economic growth.

Successful innovation ecosystem development relies on network effects for relationship-building, addressing business gaps, and meeting the needs of small and large businesses through collaboration. Orchestrated innovation ecosystems must be driven by business use cases that provide business incentives for all participating stakeholders. The U.S. federal government must promote initiatives to operationalize such ecosystems with few Hyperscalers to use their platforms to accelerate growth of the many SMBs, instead of using their value-add to increase monopoly. Below are business use case examples that can be accelerated with orchestrated PPPs consisting of **large companies**, **innovative startups**, and **domain experts**.

Smart Connected Cities: IoT systems collecting data on traffic, pollution, etc. to improve city lifestyle.



- Cisco
- Qualcomm
- AWS
- Siemens
- UrbanData
- City Planners

Platform-based business ecosystem partnerships may include broadline chip suppliers (e.g., Qualcomm), device makers (e.g., Cisco), Hyperscalers (e.g., AWS), PLM vendors (e.g., Siemens), innovative startups (e.g., UrbanData Analytics), and city planners.

For collaboration, broadline suppliers lead the way with foundation IoT platforms, cloud vendors offer data storage and processing, PLM vendors assist in managing city assets, startups and domain experts add value by providing innovative applications for traffic management, pollution reduction, or urban planning and city governments facilitate data access and policy implementation. The economic value proposition for

stakeholders includes enhanced city services, reduced traffic congestion, improved air quality, and a higher quality of life and improved city lifestyle and future economic growth.

Smart Connected Manufacturing: Factories using sensor data to improve efficiency, automation, and quality.



- Schneider
- NVIDIA
- Azure
- PTC, GE
- QualitySense
- IT/OT Experts

Platform-based business ecosystem partnerships may include chip suppliers (e.g., NVIDIA), device makers (e.g., Siemens), cloud vendors (e.g., Azure), PLM vendors (e.g., PTC), OEMs (e.g., GE), innovative startups (e.g., QualitySense) and manufacturing experts.

For collaboration, large companies like Shneider, ABB, Siemens, PTC and GE offer industrial IoT platforms, while innovative startups like QualitySense provide specialized solutions for quality control and process optimization. Chip suppliers like Nvidia contribute AI and IoT hardware, while domain experts in manufacturing processes collaborate on real-time data analytics and automation. The economic value proposition for all stakeholders, centers on increased efficiency, reduced downtime, improved product quality, and cost savings, benefiting both large and small enterprises that jointly offer unique solutions.

Smart Connected Buildings: Sensors monitor activity and manage power or find doctors in hospitals.

Platform-based business ecosystem partnerships may include device makers (e.g., Honeywell, Johnson Controls), Hyperscalers (e.g., Google Cloud), innovative startups (e.g. EcoSensors) that offer energy-efficient sensor technology and domain experts in building management and energy efficiency. Chip suppliers like Intel, ST and NXP can power smart buildings apps.



- Honeywell
- Johnson Controls
- Intel, ST, NXP
- Google Cloud
- EcoSensors
- Bldg. Experts

For collaboration device makers provide sensors and automation systems, cloud vendors handle data analytics and storage, and building experts. Innovative startups ensure that the sensor data collected is effectively utilized to optimize building management such as power consumption and occupancy

tracking. The economic value proposition for participating stakeholders includes reduced energy consumption, cost savings, and optimized building management, with all stakeholders benefiting from better efficiency and enhanced building functionality.

Smart Connected Transportation: Connected EVs becoming Autonomous and integrated with city infrastructure.

Platform-based business ecosystem partnerships may include Automotive OEMs (e.g., Tesla, VW), infrastructure providers (e.g., Siemens), Chip suppliers (e.g., AMD, Infineon), innovative startups like AutonomyTech focusing on autonomous vehicle software development and city municipalities.



- Tesla, Rivian
- Siemens
- AMD, Infineon
- Azure, AWS
- AutonomyTech
- Urban Planners

For collaboration, EV manufacturers develop connected vehicles, infrastructure providers create charging stations and autonomous infrastructure, and city governments facilitate integration with urban planning. Large EV manufacturers and infrastructure providers pave the way with platforms, while startups focus on

software development and integration, enabling a transition to autonomous vehicles applications integrated with city infrastructure. The economic value proposition for stakeholders includes reduced traffic accidents, enhanced mobility, and efficient transportation systems, benefiting all stakeholders through safer and more efficient transportation options.

Smart Connected Energy: Utility companies use Smart meter analytics to balance energy supply and demand.



- E.ON, PG&E
- Schneider
- Landis+Gyr
- Renesas, SAS
- Bidgely
- Energy Experts

Platform-based business ecosystem partnerships may include leading utility companies (e.g., E.ON, PG&E), OEMs (e.g., Schneider), Smart Connected meter suppliers (e.g., Landis + Gyr), data analytics firms (e.g., SAS) and chip suppliers (e.g., Renesas), and startups (e.g., Bidgely).

For collaboration, utility companies license and deploy software platforms from innovating startups offering analytics into energy consumption and managing energy demand and supply of the overall grid. Meter suppliers provide hardware, data analytics firms offer insights, and energy experts optimize the grid for supply and demand balancing of the Connected Energy ecosystem. The economic value proposition for stakeholders revolves around reduced energy waste, lower costs, and improved grid reliability, benefiting utility companies, analytics providers, and consumers.

Smart Connected Healthcare: Wearables collecting health data and provide analytics to prevent emergencies.

Platform-based business ecosystem partnerships may include large consumer tech companies (e.g., Apple), data analytics providers (e.g., IBM Watson Health), innovative startups on medical data analysis (e.g., HealthTech Insights), healthcare institutions, and medical expert networks.



- Apple
- IBM Watson
- Amazon
- OMRON
- HealthTech
- Medical Experts

For collaboration, large companies deliver wearables and data analytics tools that capture health data, while startups contribute specialized medical data analysis, healthcare institutions utilize insights, and medical experts provide guidance to help prevent emergencies through early detection and proactive health

management. The economic value proposition for stakeholders includes improved health outcomes, reduced healthcare costs, and early intervention where all parties benefit from proactive healthcare management.

Smart Connected Agriculture: Sensors and drones help increase crop yield and reduce spoilage in storage.

Platform-based business ecosystem partnerships may include agriculture leaders (e.g., John Deere) drone manufacturers (e.g., DJI), Hyperscalers (e.g. Azure, AWS) innovative startups of drone sensors data analytics (e.g., PrecisionHawk) or spoilage sensors and analytics (e.g., Centaur Analytics) and agronomist experts.



- John Deere
- DJI Drones
- Azure, AWS
- PrecisionHawk
- Centaur Analytics
- Agronomists

For collaboration agriculture technology firms supply sensors and solutions, drone manufacturers offer aerial monitoring technology, startups provide drone-based monitoring solutions to increase crop yield and sensor-based solutions to reduce spoilage in storage, while agronomists leverage data for

crop management and optimization. The economic value proposition encompasses increased crop yields, reduced spoilage, and sustainable farming practices, benefiting all stakeholders with better agricultural capacity and reduced waste.

Smart Connected Supply Chain: Tracking sensors on boxes & containers reduce costs and strengthen resilience.

Platform-based business ecosystem partnerships may include logistics giants (e.g., UPS), sensor technology providers (e.g., Bosch, TI, ST Microelectronics), innovative startups offering real-time visibility (e.g., Resilinc), and supply chain experts. Ecosystem partnerships vary by vertical market as shown below.



- UPS, FedEx
- Bosch
- TI, ST Micro
- PrecisionHawk
- Resilinc
- Market Specific

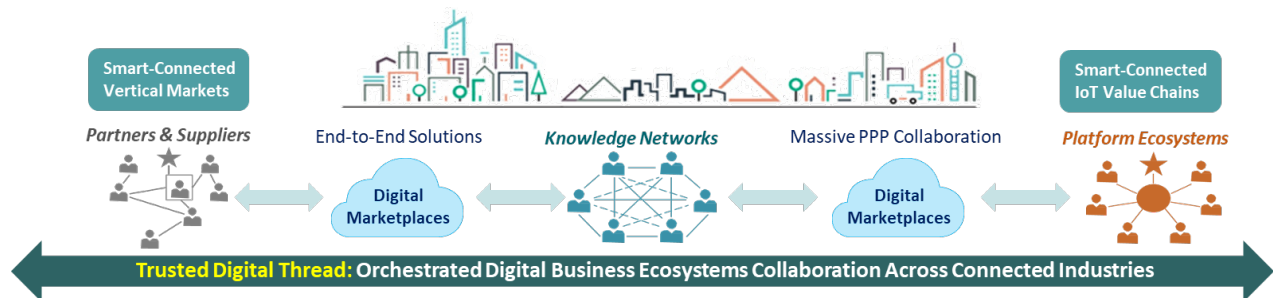
For collaboration, logistics companies deploy tracking sensors, sensor technology providers supply IoT hardware which connects to company IT infrastructure, and supply chain experts optimize logistics based on real-time data and technology startups offer real-time visibility into supply chain events and helps

organizations proactively identify and mitigate risks. The economic value proposition includes cost reduction, improved supply chain resilience, and enhanced efficiency, benefiting all participants through reduced operational costs and improved supply chain reliability.

Platform-based business ecosystems driven by orchestrated PPPs are crucial for IoT adoption and growth due to its complexity and critical need for integration and interoperability of many components. Collaboration among stakeholders with a joint business objective involves clear communication, trust-building, alignment of incentives, network affects and the establishment of governance to ensure that all parties work together toward a common goal.

Finding: IoT can have a positive impact on our GDP by leveraging platform giants to lead the development of orchestrated digital business ecosystems linking industries, environments, and digital marketplaces into a hyper-connected planet.

In an age of unprecedented technological advancement, the Internet of Things (IoT) emerges as a transformative force with the potential to reshape our GDP. IoT can positively impact our economy by harnessing the prowess of digital platform giants like Apple, Microsoft, Google, and Amazon. Their collective value represents a major portion of the U.S. GDP. Their collective might and platform experience can be leveraged to lead the evolution of a hyper-connected planet connecting industries, environments, and digital marketplaces.



Void in orchestrated platform-based business ecosystems. While the platform giants have excelled in various domains, there remains a noticeable void on multi-stakeholder collaboration platform across industry ecosystems. One of the main strategies for achieving hyper-connected growth is to create orchestrated platform-based business ecosystems linking IoT value chains. This approach recognizes that the digital landscape is evolving rapidly, and that legacy business models are being reshaped by the advent of IoT technologies. With appropriate orchestration and incentives, the few trillion-dollar giants can multiply the growth of the many SMBs.

The journey from partnerships to knowledge networks, to digital ecosystems. Digital ecosystems are not limited to the exchange of goods and services. They encompass a broader spectrum, starting with partnerships where entities collaborate to achieve shared goals. Over time, partnerships evolve into knowledge networks, emphasizing the importance of sharing expertise and insights among stakeholders. Knowledge networks mature into collaborative platform-based business ecosystems leveraging the collective IQ and digital threads across value chains to surge in new XaaS revenue streams with amplified network effects.

Strategy for giants to empower SMBs to scale with massive collaboration. Platform-based business ecosystems that span across IoT ecosystems amplify network effects exponentially, setting the stage for a dynamic and collaborative business landscape. To unlock this potential, the platform giants should spearhead orchestrated platform-based business ecosystems in ways that strengthen national security and fuel economic growth. Rather than exploiting SMB value-add in their own ecosystem to increase their monopoly, they should be incentivized to amplify and multiply the value-add of SMBs to create the next generation of trillion-dollar giants.

Harnessing data for national security and economic Growth. By motivating the platform giants to orchestrate multi-stakeholder digital business ecosystems and hyper-connected marketplaces driven by trusted digital threads, the treasure trove of data generated by digital twins and AI applications will be unlocked. This data will fuel a plethora of digital services, enhancing national security and propel our economy into the future of a hyper-connected digital planet. Large and small businesses will be able to access a vast marketplace where they can not only offer their products and services but also tap into a wealth of data and insights.

Leveraging circular value chain ecosystems for sustainability. Platform-based business ecosystems in circular value chains play a pivotal role in driving sustainability and accelerating the convergence of physical and digital worlds with digital twins. Digital twins being replicas of physical systems integrated into circular ecosystems, will contribute to collective ecosystem IQ amplified by network effects evolving new

layers of digital twins. The convergence of physical and digital worlds, fueled by digital twins within circular business ecosystems, fosters efficiency, innovation, and environmentally responsible practices that will take economies to the next level.

The convergence of IoT and platform giants leading the development of orchestrated business ecosystems represents an unparalleled opportunity to grow our GDP. Through collaboration, amplification of SMB value, and the adept leveraging of hyper-connected digital threads, the U.S can usher in an era of prosperity and innovation. It is incumbent upon us to leverage the core strengths of the giants and harness the full potential of IoT and lead the charge toward a future of orchestrated digital business ecosystems that unite digital marketplaces, industries, and environments and a hyper-connected planet that holds untold promise for us all. By embracing this strategic transformation, we secure our place at the forefront of the digital revolution, ensuring a brighter future for generations to come.



Findings of the IoT Advisory Board

The major findings that informed the board on the development of the recommendations are listed in this section. These findings are grouped in general findings (affecting everyone) and industry-specific findings.

General findings

1. Industry adoption is slower than expected and is hindered by a variety of challenges.
2. A lack of coordination at the national level is hindering IoT adoption and operation across the economy and industry sectors.
3. The adoption and operation of innovative IoT applications are hindered by various existing policies and regulations at local, state and federal levels.
4. Equity in access, opportunities, benefits and outcomes is necessary for the sustainable integration of IoT into all aspects of the national economy and civil society.
5. Small businesses can reap significant benefits from IoT, but significant barriers hinder adoption.
6. Small companies and startups are instrumental in developing many innovative and disruptive technology solutions and services but face a variety of barriers in getting adoption.

7. IoT enables new innovative business models which requires new business and technology platforms and ecosystems to support and scale it.
8. Interoperability is a key challenge for IoT across multiple industries
9. A variety of connectivity challenges is hindering IoT adoption, operation and scaling.
10. A lack of trust in IoT is a major barrier to widescale adoption.
11. Artificial Intelligence (AI) is critical to unlocking and accelerating the value of IoT.
12. There is an insufficient number of people in the current workforce with the technical, digital and analytic skills required to develop, integrate and deploy, operate and maintain IoT devices and IoT-enabled systems and applications.

Industry findings

1. Precision Agriculture: IoT brings significant value to agriculture, but adoption is slow.
2. Smart cities and infrastructure: The development of smart cities in the United States is limited, uneven and slow to develop.
3. Transit and traffic: IoT is transforming transit systems and traffic management with real-time data analytics, intelligent traffic management, and predictive analytics to enhance efficiency, reduce congestion, increase safety, and improve overall transportation experiences.
4. Healthcare: IoT is transforming healthcare, and is poised to revolutionize it but significant challenges need to be addressed.
5. Environmental Sustainability: IoT supports environmental sustainability through real-time monitoring, optimizing resource usage, and facilitating data-driven decision-making across infrastructure and multiple sectors of the economy.

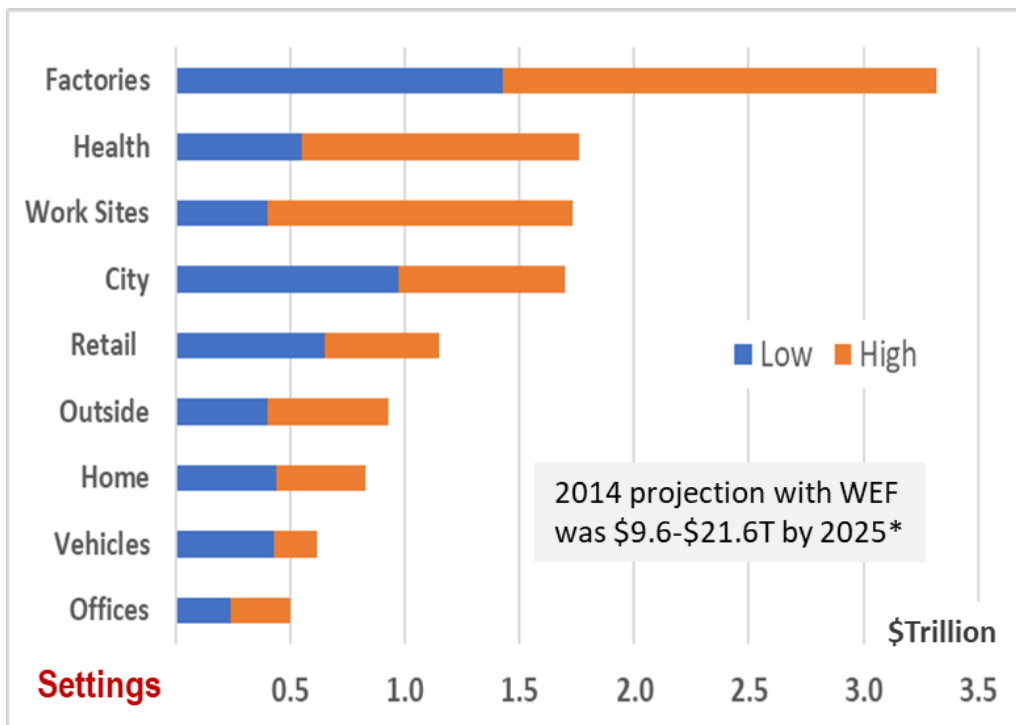
General Findings – Specific Considerations

Finding: Industry adoption is slower than expected and hindered by a variety of challenges.

In 2014 the World Economic Forum and McKinsey & Co. projected that IoT, and adjacent technologies (analytics, cloud computing, big data and ML/AL) will produce \$9.6 to \$21.6 trillion of value for the global economy by 2022³⁹.

In 2021, McKinsey & Co. clarified in a new report⁴⁰ that the above projection was off mainly due to The IoT has faced headwinds related to change management, cost, talent, and cybersecurity, and slow market adoption of digitalization and cyber-resilience particularly in enterprises.

Global IoT Economic Value \$5.5-\$12.6 Trillion by 2030



The 2021 report revised the IoT forecast to \$5.5 to \$12.6 trillion by 2030 concentrated in certain settings as shown above. For each setting, it provided a min-max range for projections factoring **adoption rates, impact, and scale**. Each setting was analyzed

³⁹ www.weforum.org/press/2014/01/increased-cyber-security-can-save-global-economy-trillions/

⁴⁰ www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

for tailwinds and headwinds, opportunities and risks and the settings were ranked based on size and growth rates as shown in the chart above. The convergence of physical and digital worlds was cited as a fundamental trend underlying the digital transformation of businesses that can fuel the global economy.

Despite the significant value of IoT and projections about its potential to accelerate economic value the rate of adoption and growth is still slow. However, some key barriers to adoption across value chains are economic, such as upgrading legacy infrastructure, handling enterprise silos, optimizing fragmented supply chains delivering solutions requiring broad partnerships. To compete, the U.S. must leverage existing strengths and experience of the few trillion-dollar companies and replicate across the many smaller companies and SMBs.

The adoption of IoT technologies has been growing in the United States, but that growth has been gradual and slower than expected. As a result, several major technology companies have pivoted away from IoT. Despite its potential, there are several challenges and barriers that have contributed to the slow pace of adoption across the economy and society.

- **Complexity and Integration.** IoT is a set of disparate technologies offered by a fragmented ecosystem of hardware suppliers, software platforms and connectivity service providers. It is not a “one size fits all” and components must be assembled together to create a solution that meets the specific requirements. In addition, IoT implementations often require integration with existing systems and infrastructure. Integrating IoT devices and platforms with legacy systems is a significant barrier, costly, and requires technical skills that is in short supply, especially for industries with established processes.
- **Cybersecurity Concerns.** IoT introduces a vast number of potential attack surfaces, leading to very real concerns that hinder adoption. Many industries, particularly those dealing with sensitive data or critical infrastructure, are cautious about the potential vulnerabilities associated with IoT devices. Significant progress has been made in IoT security but many manufacturers have not yet moved to secure by design/ secure by default cultures. Policies must focus on ensuring adoption of best practices and ensuring regular updates to IoT devices.
- Cyberattacks may disrupt the operation of IoT devices and services, or lead to a breach of back office and enterprise systems that the IoT devices connect to.
- **Interoperability.** The inability for devices to communicate with each other or to the broader enterprise, legacy systems and operations technology systems, is a major barrier. In some cases, the lack of interoperability is caused by a lack

of standards and protocols. In other cases, there are multiple competing standards as each solution provider creates “walled gardens” or “walled ecosystems”. One major challenge is the integration of IoT devices with legacy and operations technology systems, which are commonly found in many industrial and enterprise environments.

- **Data Privacy and Compliance.** Concerns related to data privacy and regulatory compliance are significant barriers to IoT adoption. Industries must navigate complex legal frameworks and ensure that IoT implementations comply with data protection regulations, which can slow down the adoption process. While privacy concerns cut across multiple markets and industries, certain markets are more sensitive to privacy issues, including smart cities, retail, insurance and healthcare.
- **High Implementation Costs.** The upfront costs associated with implementing IoT solutions, including the purchase of devices, infrastructure, and integration expenses, can be a deterrent for many potential adopters, especially for those operating on tight budgets. It is estimated that the cost of the IoT solution represents 30% of the total cost, while implementation and deployment accounts for the other 70%.
- **Lack of Skilled Workforce.** Implementing and managing IoT technologies require a skilled workforce with expertise in wide variety of areas such as cybersecurity, data analytics, application development, cloud operations, and system integration. The shortage of professionals with these skills hinder adoption, particularly in industries that have not traditionally require digital talent. In addition, the ongoing labor shortage contributes to the struggle to attract and retain such talent.
- **Uncertain ROI and Business Value.** Some industries are more hesitant to adopt IoT technologies due to uncertainty about the return on investment (ROI) and the overall business value. This is particular true for industries, such as mining, construction and agriculture, that have not traditionally incorporated digital technologies into its operations. There is a lack of clear use cases and success stories demonstrating tangible benefits are essential for convincing businesses to invest in IoT.
- **Resistance to Change.** Resistance to change within organizations is a common challenge. Many potential adopters have limited awareness and education of IoT, and what it can do. Employees and management may be accustomed to traditional processes and may resist adopting new

technologies. Complexity, industry regulations and structure, and organization culture are additional barriers hindering the adoption of IoT.

- **Reliability and Stability Concerns.** IoT is still considered a new or emerging technology for many industries, particularly those in sectors like healthcare, manufacturing, energy and smart cities. In these sectors, reliability, stability and longevity are important characteristics. The failure of a smart healthcare device may result in the death of the patient. Failure of an intelligent traffic signal may lead directly to accidents and injuries. Failure of such systems may result in the adopters incurring financial liability. In sectors like cities, maintenance and operations are a top requirement, and IoT devices are expected to last decades. In these sectors, adopters often forgo the “latest and greatest” technologies for older generation “tried and true” systems.

Finding: A lack of coordination at the national level is hindering IoT adoption and operation across the economy and industry sectors.

[dan, pete to supply content]

Finding: The adoption and operation of innovative IoT applications are hindered by various existing policies and regulations at local, state and federal levels.

Technology advancements create intended and unintended outcomes that are both positive and negative. Government policies and regulations help inform, facilitate and reduce the impact of unintended consequences. While the outcomes of regulations and policies on mature technologies have been studied and understood, new and emerging technologies often outpace the effectiveness of policies and result in unintended consequences.

While IoT offers the potential for disruptive transformation and value, there are instances where policies and regulations at various levels of government hamper the benefits it provides. Policies and regulations are generally well-intentioned and crafted to protect users and the community from harm, or to comply with standards and norms. Conflicts arise because the development and use of technology is moving and changing fast, and used in ways that have never been used or studied before. These well intended policies may conflict with one another, resulting in barriers to adoption, use, compliance and commerce of IoT. Government policies and regulations play a critical role in advancing or stifling the use, the beneficial outcomes and the scaling and evolution of IoT.

Examples of policies affecting the use of IoT include

- Facial recognition algorithms running on a city's network of video cameras helps to deter and solve crimes but may lead to privacy violations when it is used outside of its intended purpose or provide inaccurate results. Many cities have enacted laws restricting the use of video cameras and facial in smart city applications.
- Autonomous drones can perform a variety of labor-saving tasks on large farms, including monitoring plant health and crop spraying. However, FAA regulations require one operator per drone, and it must be operated within line of sight. This limits the utility and value that can be obtained from the use of drones in agriculture.
- Telematics devices generate a lot of information about a car and driver's behaviors. This information can be used by automobile insurance companies to create personalized insurance products and set premiums. Insurance is regulated at a state level, and each state determines what information can be used. For example, California only allows insurance companies to use mileage data.

Finding: Equity in access, opportunities, benefits and outcomes is necessary for the sustainable integration of IoT into all aspects of the national economy and civil society.

Although IoT offers the potential for significant benefit to people, communities, businesses and organizations across the United States, those benefits are not equally distributed or shared. Conversely, IoT may create adverse outcomes, with some communities disproportionately receiving more harm than others. Equity in access, opportunities, benefits and outcomes is necessary for the sustainable integration of IoT into all aspects of the national economy and civil society. Policymakers, regulators, and financiers must understand and consider equity when planning initiatives to accelerate and increase the adoption of IoT into the economy and society. Similarly, builders, developers and operators of IoT products and services should take equity in consideration to create offerings that are relevant, effective, and sustainable.

Equitable access to connectivity. Connectivity is necessary for the operation of IoT. However, many communities today do not have access to connectivity, or to service at the levels necessary to support their needs. This lack of access may be due to a lack of infrastructure, lack of access to affordable service, or insufficient infrastructure. For example, rural and remote communities lack broadband infrastructure, while lower socioeconomic communities in urban areas suffer from a lack of affordable service.

Other communities may have old infrastructure that must be upgraded to support advanced IoT applications and services. Equity in connectivity is necessary to enable equity of benefits from IoT.

Equitable benefits for rural communities and economies. Rural communities face challenges that their urban counterparts do not. For example, many rural areas are “medical deserts”, a term used to describe locations with inadequate access to one or more kinds of medical services. Approximately thirty million Americans, many in rural communities, live at least a sixty-minute drive from a hospital with trauma care services.¹ In these communities, IoT-enabled telehealth services are of great benefit, especially for those with chronic health conditions requiring frequent doctor visits. However, rural regions lack not only the connectivity infrastructure, but the workforce and resources to support IoT operations. From maintaining connectivity to developing, integrating and servicing IoT applications and equipment, a lack of local expertise and trained resources is hindering the ability of rural economies to sustain and extend its benefits from IoT.

Equitable opportunities for small cities and communities. Small cities and communities lack the capital, resources and capabilities that their larger city counterparts enjoy. IoT and other innovations offer the potential of helping these smaller cities and communities “do more with less” and to do it more effectively to serve the needs of their constituents. However, these smaller cities and communities are often less aware of IoT and other innovations, lack the budget and access to funding sources, and in-house expertise and capabilities to plan and deploy these technologies. Furthermore, the lack of innovation offerings, enablement programs, and funding sources is hindering these smaller communities from accessing the same opportunities and benefits that their larger counterparts receive.

Equitable outcomes from data. IoT devices collect vast amounts of private and non-private data to make decisions, drive actions and create outcomes. However, the use of this data may lead to negative outcomes intentionally or unintentionally. For example, the use of facial recognition on people of color has been found to have a higher probability of error and lead to inaccurate results. Because of this, people of color have been negatively impacted at higher rates than other demographic groups. Similarly, vehicle telematics data can be used by insurance companies to determine risk and set personalized premiums. However, while this leads to good drivers receiving lower premiums, bad drivers may be relegated to a class of “uninsurables” who are unable to get insurance at any premium. In the past, these drivers would have been placed into a larger risk pool, where their higher risks may be offset by others with a lower risk. Equity considerations and protections must be incorporated in using data to create beneficial outcomes for the economy and society.

Equitable access to IoT for small businesses. Small businesses are the heart of American commerce and stand to benefit from the integration of IoT into their businesses. However, these small businesses lack the staff and technical expertise, resources, and the funds to afford and buy and integrate these IoT technologies. For example, many small farming businesses have limited appetite and funds to invest in IoT technologies with an “unknown” outcome. Instead, they prefer to invest those funds into inputs (seeds, fertilizer, herbicides, etc.) which they know will lead to something tangible (“produce”) even if it was produced inefficiently. Similarly, small retail businesses have limited free cash available, and prefer to invest that limited in inventory which they know will convert to profits. These day-to-day realities “trap” many small businesses into an endless cycle and hinders their ability to buy and use IoT to obtain its associated benefits.

Equitable access to opportunities for small business and start-up IoT innovators. Start-ups and other small businesses create many of the innovations that bring disruptive new value to the economy and society and keep America strong and resilient. However, many of these companies face challenges in bringing these innovations to reality. For example, many businesses and government agencies are often unaware of these innovations and have limited funds, policies and processes ability to evaluate and validate them. Innovations often face the “valley of death” from successful completion of pilot or proof of concept to contract. Procurement policies and processes, designed for well-established mature products and services, do not work well for innovative solutions. As a result, many innovative offerings from small businesses and start-ups fail not because of their offering, but because they face access barriers to market that larger businesses don’t have.

Equitable access to workforce development and employment opportunities. The integration of IoT into the economy and society creates new types of jobs and employment opportunities. Some of these jobs will require new skills, while others may be extensions to existing skills. For example, some IoT jobs will require digital skills, such as integration, programming, cloud application development, cybersecurity and data science. At the same time, other jobs will be needed to manufacture, install, service and maintain IoT devices and IoT-enabled equipment. These employment opportunities are at risk of bypassing socioeconomically challenged and rural communities, whose residents may not have the language proficiency, digital literacy, access to education and development opportunities, and broadband service, to be included. Labor shortages exist in many industries today and hinders the American economy. Similarly, the inequitable access to employment opportunities created by IoT will hinder the country’s full realization of the economic and societal benefits.

Finding: Small businesses can reap significant benefits from IoT, but significant barriers hinder adoption.

IoT brings significant value and outcomes for both small and large businesses. Small business enterprises lack the resources and scales of economy that their larger counterparts have, and the adoption of IoT into their operations can have a significant and immediate impact. For example, soil moisture sensors help farmers direct irrigation to those specific areas where the soil needs watering most. Small farming operations are cash flow constrained, and the money saved on watering can be immediately redeployed to help pay for other things. In manufacturing, IoT sensors continuously monitor the condition and performance of production equipment, helping factories optimize production, reduce scrap, and minimize unplanned downtimes. This has an immediate impact on small factories, helping them to meet customer commitments, expand their business and profits, and overcome cash flow constraints.

A number of barriers hinder the adoption of IoT in small businesses. These include:

- **Financial.** The initial cost associated with purchasing and implementing IoT solutions may be beyond the means of small businesses. These businesses have limited financial resources, and many have cash flow constraints, hindering their ability to invest in IoT, hire skilled resources or contracting with service providers.
- **Skills and Expertise.** Integrating IoT technologies into existing business processes can be complex. Small businesses lack personnel with the expertise to successfully deploy and manage the integration. They face challenges in finding and retaining these employees. Training existing staff or hiring skilled workers can be difficult due to budget constraints and market competition for the same talent.
- **Infrastructure.** Small businesses often lack the infrastructure to support the integration, operation and scaling of IoT. Existing infrastructure may need to be modernized. Networks may require upgrading to ensure consistent and stable connectivity for their IoT implementations. Software applications may be upgraded to integrate data from IoT sensors. Some businesses employ legacy systems, adding further complexity to integrate with IoT solutions.
- **Cybersecurity and privacy concerns.** Cybersecurity breaches are extremely disruptive to small businesses, who often lack the resources and expertise to implement and keep up with robust security measures, and mitigate the impacts of cyber-attacks. The collection of data from sensors adds further complexity. Small businesses are concerned on how their proprietary data is

used and shared, as it is their source of competitive advantage. They also lack the expertise, knowledge and tools to navigate complex regulations and ensure compliance with data protection laws on customer data collected from IoT.

- **Limited Awareness.** Many small businesses have very limited to no awareness and understanding about IoT solutions. These businesses have limited time and budget for exploring and staying updated on the latest technologies. Small businesses have limited exposure to industry conferences, trade shows, or forums where IoT trends are discussed. Many IoT solution providers focus their marketing efforts on larger enterprises, leaving small businesses unaware of available solutions that could benefit them. Small businesses may have difficulty finding relevant case studies or success stories that demonstrate the practical benefits of IoT in their specific context.
- **Adoption resistance.** Small businesses, especially those in survival or growth phases, prioritize immediate operational needs over exploring new technologies. IoT may be perceived as complex and technical, especially by individuals who are not well-versed in IT. Small business owners and decision-makers may feel overwhelmed by the technicalities associated with IoT, leading to a hesitancy to explore further. Small business owners may be unfamiliar with the potential advantages of IoT technologies and may hesitate to invest without a clear understanding of the return on investment. Misperceptions about the cost of adopting IoT technologies discourage exploration and investment in IoT solutions.

Finding: Small companies and startups are instrumental in developing many innovative and disruptive technology solutions and services, but face a variety of barriers in getting adoption.

Many disruptive technology and market innovations come from small companies and start-ups. However, start-ups face a variety of challenges in developing and bringing innovative offerings to market. As a result, many promising innovations never reach commercialization. Some of these challenges include:

- **Access to Funding and Investment.** Securing funding is challenging for IoT start-ups and small businesses. Funding is necessary for the research and development of innovative offerings, but investors are risk-averse when it comes to “unproven” and emerging technologies. Customers have limited to no budgets for funding pilot and proof of concept projects. While larger and established companies can afford to fund development projects and do free pilots, smaller companies and start-ups cannot. Many more start-ups and smaller businesses fail to navigate the “Valley of Death” (the period between

initial successful pilot/prototype development and contracting) because they are unable to secure the bridging funds.

- **Customer procurement processes are not designed to purchase innovative offerings.** Existing government and enterprise procurement processes and policies are designed for sourcing established and mature products from established companies. These processes are not well-suited to buy “risky” offerings from start-ups with limited to no proof of performance, limited operating history, and innovative commercial models. Some larger companies address this by offering deep discounts or free proof of concepts to alleviate risk concerns, but small companies do not have the luxury to do so.
- **Legacy regulations and standards.** Certain industries, such as energy, healthcare and transportation, are subject to regulations and standards that were established for legacy systems and operations. The capabilities offered by IoT and other disruptive emerging technologies may deliver the desired outcomes in innovative ways, but may do it in ways that conflict with these existing industry standards and regulations. For example, drones are subject to FAA regulations specifying one drone, one operator. In addition, drones must operate within the line of sight of the operator. This prevents the development and operation of autonomous drones in farming, where drones could be used to collect imagery information of plant health, or conduct crop spraying.
- **Market incumbents.** Many start-ups offer technologies and solutions that disrupt and compete against existing incumbent legacy solutions. Incumbents are well established, and hinder market adoption of innovative solutions in a variety of ways. This includes limiting access to infrastructure and systems and creating “walled garden” ecosystems. For example, one equipment manufacturer “maliciously complies” with an industry standard for communications, but encrypts the data traffic going through it, which effectively blocks access to the data by other machines.
- **Low market awareness.** At this early stage, there is very limited market awareness of innovative IoT technologies and solutions. Start-ups often invest considerable resources and time to establish credibility and educate their target market about the technology, approach, benefits and value proposition of their innovative solutions. In addition, many start-ups lack the market credibility compared to larger and more established companies. Government adoption and use of innovative IoT solutions helps start-ups establish credibility, and more importantly, credibility of IoT.

Finding: IoT enables new innovative business models which requires new business and technology platforms and ecosystems to support and scale it.

[Update with information from TomKat's findings and opportunities.]

Finding: Interoperability is a key challenge for IoT across multiple industries.

Interoperability allows heterogeneous devices and systems to integrate, communicate and share information with each other and automate. For example, information collected from one IoT device is used as input data by another different device, or devices from different brands may communicate and work together in a system. While interoperability is enabled by standards, it is challenging to achieve for a variety of reasons. In some areas, IoT technology is still new and rapidly evolving. There are many areas of IoT technology to be standardized and attaining agreement on a standard takes time. While open standards provide the potential for seamless interoperability, the current market is filled with products with proprietary standards, “walled garden”⁴¹ device ecosystems and differing international standards and protocols. Some vendors believe their proprietary standard is technologically superior, some were first to market before standards developed, while others are concerned with commoditization of their offerings. For IoT to evolve, interoperability and standards across devices, industries and countries are critical. (source: NIST IoT report draft)

Here we add some stories.

Example – highlight automobile industry report highlighting lack of interoperability and value lost.

Finding: A variety of connectivity challenges is hindering IoT adoption, operation and scaling.

The availability of connectivity service coverage is a necessary prerequisite for IoT adoption and operation. The COVID-19 pandemic highlighted the impact of the digital divide and the need for connected communities. Several government and private sector initiatives offer the potential to make connectivity ubiquitous. For example, a portion of the \$65 billion in the federal Bipartisan Infrastructure Law will build infrastructure in underserved areas. California is building a \$6 billion middle mile

⁴¹ A “walled garden” ecosystem is one in which a vendor or a group of vendors together form an ecosystem where their products are compatible with each other.

fiber network to facilitate the creation of last mile services to underserved areas.⁴² The FCC is considering the potential use of the frequencies in the TV white space for connecting IoT devices over wide expanses of rural areas. Several satellite operators are planning or have launched next generation Low Earth Orbit (LEO) broadband and IoT connectivity services to rural and underserved areas. These initiatives are supplemented by private enterprises establishing LTE and 5G private networks to connect campuses, factories and other facilities augment commercial telecommunications services. (source: NIST IoT research report draft)

Despite these efforts, more work needs to be done to overcome the various challenges IoT adopters and operators face. These include:

- **Lack of fixed and wireless connectivity infrastructure.** While urban areas have the infrastructure to offer different connectivity service options, rural areas and remote regions lack the same. This may be manifested in the lack of fiber infrastructure, as well as a lack of sufficient wireless infrastructure. Limited infrastructure, low population and population densities, terrain challenges and poor economic returns limit industry connectivity investments in these areas.
- **Future use cases require higher bandwidth symmetric services.** Future IoT use cases, such as drone and remote machinery operation applications in agriculture, require higher bandwidth symmetric connectivity services. The FCC's current 25/3 broadband service level definition is insufficient to support those applications.
- **Insufficient spectrum to support future needs of IoT at scale.** As the number of devices and IoT-enabled services continue to grow, additional wireless spectrum is needed to minimize performance issues. These issues include interference, latency, quality of service and reliability. IoT devices supporting first responder and medical applications, are especially vulnerable. Urban and metropolitan centers, having a large number of building structures, high wireless device density, are most susceptible to disruptions and issues.
- **Sunsetting of connectivity technologies.** There are millions of IoT devices that are connected through 2G and 3G networks in the United States. As 4G and 5G networks enter into service, these older networks are turned off or "sunsetting" over a period of time. For example, the various carriers started turning off their 2G networks between 2017 (AT&T) to 2022 (T-Mobile). Similarly, carriers turned

⁴² State of California Middle-Mile Broadband Initiative,

off their 3G networks between 2021 and 2022.⁴³ In many cases, it is not possible on a practical basis to replace and update the transmitters in the devices to newer protocols, rendering the devices useless. Managing the sunset and replacement of the devices is a major task and cost burden for IoT users and owners.

Finding: A lack of trust in IoT is a major barrier to widescale adoption.

The IoT raises several cybersecurity and data privacy concerns. Cybersecurity is top of mind with developers, adopters and privacy advocates. IoT devices expose new attack surfaces that can be exploited to enter the network, steal information and disrupt operations. Data collected from IoT devices can be stolen, improperly accessed, or used for purposes outside its initial design. Algorithms can be biased or tricked to produce incorrect or unintended outcomes. While interoperability, connectivity and compute provide the technical infrastructure for IoT to scale, a trust infrastructure is necessary for IoT market adoption to evolve and scale.

Building trust and transparency is imperative in the IoT ecosystem. Initiatives like Privacy Transparency for IoT aim to make privacy practices more visible and understandable to consumers. In specific applications such as automobiles, introducing IoT Privacy information on Automobile Monroney Stickers and Location Tracking Notice in IoT e-labeling are key measures to inform consumers about the privacy features of IoT-enabled vehicles.

[highlight stories to follow – stories from Debbie and Mike and TomKat]

Envisioning Privacy in the Internet of Things (IoT) Era

As we delve deeper into the digital age, the Internet of Things (IoT) 's impact on privacy brings exciting opportunities and significant challenges. A comprehensive vision to address privacy in the IoT realm is critical, encompassing various aspects such as regulation, policy, trust and transparency, security, compliance, and education and innovation.

Regulation

Central to this vision is the support of robust regulatory frameworks. The endorsement of a Comprehensive Federal Data Privacy Regulation is vital to setting uniform privacy standards across the United States. Furthermore, developing a Federal IoT Privacy

Link

omplete Overview of 2G & 3G Sunsets," A. Worth, IOT, August 29, 2019. [Link](#)

Policy Framework is crucial to provide specific guidance for IoT technologies. Equally important is the Inclusion of IoT in Federal Privacy Regulations, ensuring comprehensive consumer protection under privacy laws.

Policy

Policies form the foundation of privacy in IoT. Implementing Plain Language in Privacy Policies is essential to make privacy terms understandable for consumers. Additionally, well-defined Third-Party Data Sharing Policies are necessary to regulate the sharing and use of IoT data, thus protecting user privacy. In specific applications such as automobiles, introducing IoT Privacy information on Automobile Monroney Stickers and Location Tracking Notice in IoT e-labeling are key measures to inform consumers about the privacy features of IoT-enabled vehicles.

Security and Compliance

Security and compliance in IoT require a multifaceted approach. Universal Opt-Out Signals for IoT offer consumers a simple method to control their privacy settings. Promoting Privacy-Enhancing Technologies (PETs) is crucial for advancing secure IoT solutions. Adhering to NIST Sanitization Standards for Used Automobiles and Government Automobiles Resell also ensures proper data erasure before vehicle resale. Under this umbrella, 'Privacy by Design' for IoT is essential. This approach integrates privacy considerations into every stage of IoT product development, ensuring that privacy safeguards are built into IoT technologies from the ground up.

Education and Innovation

Finally, educational initiatives for the IoT-savvy workforce are key to providing professionals with the skills and knowledge necessary to navigate and influence the future of IoT and privacy. This education will drive innovation, ensuring privacy considerations evolve alongside technological advancements.

This vision for privacy in the IoT era aims to establish a balanced ecosystem where innovation thrives alongside robust consumer privacy protection, achieved through comprehensive regulation, effective policies, enhanced trust and transparency, stringent security measures, and continuous education and innovation.

IoT has promised a revolution in connectivity and automation, offering immense potential for enhancing our daily lives and industries. However, a significant barrier hindering the widescale adoption of IoT technologies is the pervasive lack of trust. Trust is the cornerstone of any successful digital transformation, and without it, the promise of IoT remains unrealized. Trust in IoT must be addressed holistically through

trusted devices, supply chains, data, partnerships, networks, digital threads, digital marketplaces, digital twins and business ecosystems.

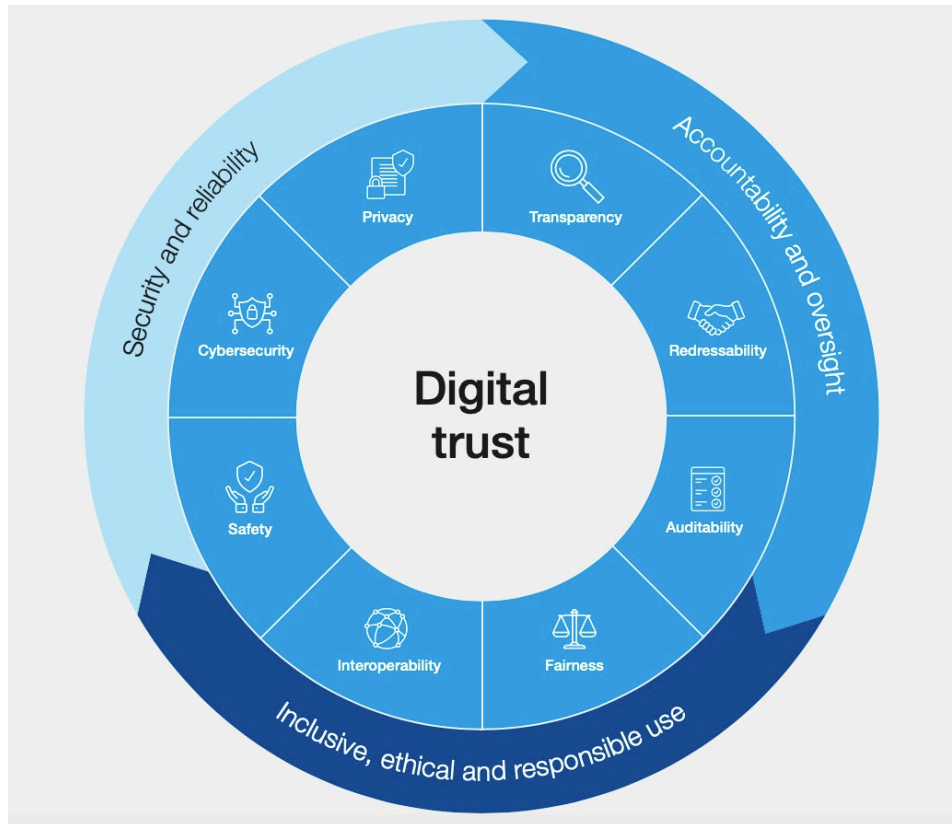
The Importance of Trust in IoT

1. **Begin with Trust**⁴⁴: Trust is fundamental to any technological advancement, including IoT. Without trust, consumers and businesses are reluctant to embrace IoT solutions due to concerns about data security, privacy breaches, and reliability. Trust forms the foundation that alleviates barriers to adoption of any technology and the basis upon which IoT ecosystems can thrive, fostering confidence among users and stakeholders.
2. **Trust Trumps Technology**⁴⁵: Trust holds more significance than technology itself in the context of digital transformation. Trusting the devices, systems, and networks that underpin IoT is paramount to its acceptance. Despite IoT's technological advancements, building trust is vital for its successful implementation. Trust in devices, systems, and networks is paramount to the acceptance of IoT technologies.
3. **The Significance of Digital Trust**⁴⁶: Digital trust is a critical factor in today's digital age. IoT devices are central to digital transformation. Their reliability and security determine the degree of trust placed in them. Ensuring trustworthiness is key to speeding adoption, proliferation and growth. Building and maintaining trust is essential, from manufacturers to end-users, as it unlocks IoT's potential for informed decision-making, and innovation.

⁴⁴ <https://hbr.org/2020/05/begin-with-trust>

⁴⁵ <https://www.industryweek.com/leadership/corporate-culture/article/21146077/trust-is-more-important-than-technology-in-digital-transformation>

⁴⁶ <https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters>



4. **Holistic Digital Trust Framework**⁴⁷: Digital trust is the belief that digital technologies and the organizations behind them will safeguard everyone's interests and adhere to societal values. Recent failures in various digital domains have severely undermined trust. To address this, the World Economic Forum brought together tech giants, government officials, and consumer advocates to establish a framework for earning digital trust. This framework emphasizes leadership commitment to cybersecurity, privacy, transparency, fairness, and other key factors to enhance trust in technology and the responsible use of new technologies. The Forum's report offers both a framework and guidance for building trustworthiness in technology development and deployment.

Holistic Approaches to Building Trust in IoT

- **Trusted Devices**⁴⁸: Trust in IoT starts by creating awareness about trustworthiness of IoT devices. Device makers prioritize security, data protection, and standards, driven by the "U.S. Cyber Trust Mark" which helps

⁴⁷ <https://initiatives.weforum.org/digital-trust/about>

⁴⁸ <https://techcrunch.com/2023/08/23/the-us-cyber-trust-mark-finally-gives-device-makers-a-reason-to-spend-big-on-security/>

them differentiate. The mark fosters consumer awareness and trust simplifying identification of secure IoT devices. Recognition of the trust mark enhances consumer confidence and conveys devices are secure and trusted.

- **Trusted IoT Partnerships:** Building trust within IoT ecosystems involves establishing trusted partnerships. Collaborative relationships among stakeholders should prioritize data security, privacy, and adherence to ethical standards. Trustworthy partnerships contribute to the overall reliability of IoT solutions.
- **Trusted Networks⁴⁹:** Securing Telco infrastructure and wireless networks, reinforced by encryption, authentication, and monitoring, are vital for trusting connected IoT devices and applications. Intrusion detection and network segmentation add extra layers of protection, instilling confidence in users and organizations. Trust in network integrity is key to preventing breaches, ensuring smooth operations, and driving IoT adoption.
- **Trusted Supply Chains⁵⁰:** Ensuring the integrity of the supply chain is essential. Organizations should employ transparent and secure supply chain practices, from component sourcing to device assembly, to minimize the risk of tampering or vulnerabilities introduced during production. Digitalization, Blockchain and distributed ledger technologies are key enablers for creating trusted supply chains.
- **Trusted Digital Transformation⁵¹:** Digital trust in operations and business is a key enabler for IoT adoption. The role of trust in data privacy, cybersecurity, and ethical AI, emphasizing that trust-building is essential for successful digital transformations. Teams and organizations must prioritize trust through robust data protection, secure technology, and ethical practices to gain a competitive edge in the digital era.
- **Trusted Data for Privacy⁵²:** Emphasizing the protection of personal user data and privacy rights is key for trusting IoT. It involves compliance with stringent data privacy regulations like GDPR and transparent data handling practices. Users have the right to control their data and its usage, necessitating clear consent mechanisms, robust encryption, and secure storage. Trust is essential

⁴⁹ <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value>

⁵⁰ <https://hbr.org/2020/05/building-a-transparent-supply-chain>

⁵¹ <https://www2.deloitte.com/xe/en/insights/topics/digital-transformation/digital-trust-for-future.html>

⁵² <https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/securing-the-future/consumer-privacy.html>

to assure users that their data, including health information and personal preferences, won't be misused.

- **Trusted Data for Confidentiality:** Safeguarding enterprise data for IoT is critical to operations and competitiveness, including securing data transport, storage, access for devices and edge applications, etc. Confidentiality measures include encryption, access controls, secure communication, and identity management. Trust assures businesses that their confidential data will remain secure in all settings.
- **Trusted Digital Threads for Traceability:** Digital threads are the backbone of IoT ecosystems, enabling traceability and transparency in data flows. Trust in these digital threads is crucial to ensure data integrity, accuracy, and reliability. Accountability and transparency across the entire IoT landscape depend on these trusted digital pathways.
- **Trusted Analytics and AI:** Analytics and AI drive insights and decision-making in IoT applications. Trust in the data used for analytics and training models that drive AI algorithms and the algorithms themselves is paramount. Users need assurance that AI systems provide accurate, unbiased, and ethical insights. Building trust in analytics and AI fosters confidence in IoT's ability to deliver valuable outcomes.
- **Trusted Digital Twins⁵³:** Digital twins serve as virtual replicas of physical objects, used in simulations, predictive maintenance, and more. Trust in the data used in digital twins is key for reliability and integrity. Users rely on real IoT data to represent real-world objects and situations, ensuring their usefulness and effectiveness in applications.
- **Trusted Digital Marketplaces:** In digital marketplaces, trust is vital for users to make informed choices. Trustworthy marketplaces offer transparent product information, user reviews, and secure transactions. Users need to trust that the products and services they find in digital marketplaces are of high quality and safe to use.
- **Trusted Business Ecosystems:** Trust in business ecosystems requires organizations to invest in building and maintaining trust among ecosystem partners through ethical practices, transparency, and strong governance to foster trust⁵⁴. Trust can be expanded as a fundamental part of ecosystem

⁵³ <https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/digital-twins-the-key-to-smart-product-development>

⁵⁴ <https://www.bcg.com/publications/2021/building-trust-in-business-ecosystems>

design that promotes collaboration, innovation and trust-based decision-making and the creation of trusted platforms. Industry stakeholders, regulatory bodies, and end-users should prioritize methods for trusted ecosystem.

In conclusion, the lack of trust poses a significant barrier to the widescale adoption of IoT technologies. As underscored by various sources, trust holds paramount importance in digital transformation, especially in IoT. To overcome this trust deficit, a holistic approach is imperative, encompassing trusted devices, supply chains, partnerships, networks, digital marketplaces, traceability using digital threads, digital twins, and business ecosystems. These elements must be fortified with security measures, traceability, and ethical practices. By addressing trust holistically, we can unlock the full potential of IoT and build a safer and more connected future.

Finding: Artificial Intelligence (AI) is critical to unlocking and accelerating the value of IoT.

Data collected from IoT devices is invaluable for creating insights and driving positive outcomes. For example, data from condition sensors is used to inform on the current status of an operational process or to diagnose a problem. Historical data may be used to identify trends and predict an outcome. Artificial intelligence automates the processing and analysis of vast amounts of data quickly and accurately.

Some of this data is used to train and build machine learning (ML) and artificial intelligence (AI) algorithms. Once trained, these algorithms are deployed in the cloud or on the devices where they are used to analyze newly collected sensor data to generate insights, inform decisions and support autonomous actions. For example, cameras in fruit picking robots analyze images of fruit in a field and identify those ripe fruits for picking.

Latency, connectivity and processing requirements determine where the algorithm resides on the device, local processing servers (“the edge”) or in the cloud. A current trend is that more and more algorithm processing is occurring on the device and the edge, instead of the cloud. Facilitating this trend is the development of AI-capable semiconductors.

As more sensors and devices are deployed, the quality of the data used to train the algorithms improves, leading to more refined models, the extension of those models to more use cases and more accurate model outcomes. Continuing advancements in algorithm development create new models that service more complex and computationally intensive applications, as well as enable more efficient processing on existing resource constrained microprocessors.

As connectivity and processing infrastructure expand, IoT will scale with new use cases that are ML/AI enabled. Continuing advancements in interoperability and development of low-cost devices will eventually lead to an environment with ubiquitous intelligence. This state, called ambient intelligence, is reached when intelligence is embedded and integrated transparently into the physical environment and human interactions. Intelligence, interoperability, connectivity and computing are interdependent. Developments in low-cost devices lead to more IoT devices, which increases the need for more connectivity service and coverage. As the number of devices scales, the amount of data collected grows. The need to process these data drives advancements in computing infrastructure and algorithms, to create outcomes. These outcomes increase the need for more devices to be integrated into the physical environment and the day-to-day interactions with humans. (source: NIST research report).

Artificial Intelligence (AI) Considerations

The IoT and Artificial Intelligence (AI) are two very distinct concepts that complement each other. When operational, IoT devices create and gather data. In turn AI analyzes the data to provide insights, interpretation, and decision making that can then and improve items on the IoT device such as its efficiency and productivity. Artificial intelligence (AI) can be defined as a collection of technologies and approaches that allow a machine to perceive its environment and take actions towards a specific goal. It encompasses several different technologies that give computers human-like abilities of perception.

Most of the AI systems today are machine learning (ML)-based systems, which allow computers to learn data patterns in a supervised or unsupervised manner, and then apply these learnings to make predictions, classify data, recognize objects or images, and understand speech or text. Other techniques that are often used in AI systems include deep learning (DL), natural language processing/understanding (NLP/NLU), computer vision (CV), and machine reasoning (MR)

Within the manufacturing industry, AI is being used in a variety of environments. These range from the factory floor, where it improves the production and distribution of manufactured goods and enhances safety, to the back office, where it streamlines administrative tasks and bolsters customer service efforts. AI is also being incorporated into manufactured goods to allow others along the value chain, including distributor, retail, and service partners, to leverage the intelligence provided by the technology to provide better customer service. In addition, these partners can use AI to improve aspects of product design and lifecycle management.

IoT technologies in industrial markets together with components like sensors, data storage and integration, data analytics, and machine learning, can be applied to SCADA systems to improve interoperability and coordination among different machines. The sensors collect new data from various equipment and continuously feed the data into the analytics. This way, machine learning algorithms can learn from past data and fine-tune the settings on different machines for thousands or even millions of cycles to reach the optimal point of the entire system. The use of AI within the manufacturing sector is being driven by specific enabling market factors that include the digitization of data, the development of IoT networks, and the steady improvements in ML and DL algorithms. AI technology introduces scale and efficiency and is best applied to two types of problems:

1. Data analysis and subsequent predictive recommendations and actions: ML and DL technologies excel at analyzing massive datasets very quickly. They can complete data analysis computations much more quickly than manual human analysis or hardcoded computer analysis.
2. Routine, redundant tasks: AI technologies are successfully handling redundant, linear thought-focused tasks (clerical work, order taking, food service), freeing up human resources to focus on higher value, human-exclusive skills (creative thinking, problem solving, interpersonal skills, emotional intelligence, reasoning, negotiation, and decision-making).

Within specific vertical markets (manufacturing, health care, energy, and transportation) there are several use cases that leverage the power of AI to deliver ROI while employing ML, DL, NLP, and CV approaches that are commonly used across vertical segments. These use cases include:

- **Digital Twins:** A digital twin is a digital representation providing the elements and the dynamics of how a device or ecosystem operates and lives throughout its lifecycle. Digital twins combine sensor data with ML and software analytics, which are then used to create spatial graphs that provide a digital simulation model that is updated and changes in real time in tandem with their physical counterparts.
- **Energy Management:** Within manufacturing, the consumption of energy remains a primary cost and concern for plant managers and the key decision makers of the company. While the cost of energy may be variable a company's energy use is fully within its control. However, in order to better assess and control energy consumption within a manufacturing environment, machines must be equipped with sensor technology. Energy usage must be tracked at a granular level in order to assess key ratios, such as energy consumption versus

productivity. The use of AI can make this tedious and data-intensive process much more efficient and effective.

- **Medical Image Analysis:** Analyzing images is a strong application for DL and CV within the realm of patient data processing. DL is now being applied to automate the analysis and increase the accuracy, precision, and understanding of images down to the pixel. Some of the more common applications include 3D CV (images analyzed and rendered into detailed 3D models), auto grading of eye diseases, and detection and segmentation of radiology images.
- **Safety Enhancement in Buildings:** Employers have an incentive to ensure better compliance with safety standards and protocols. One example of how DL is being used to help ensure better compliance includes tools that allow employers to leverage photos and videos to identify workers who are missing hard hats, gloves, or other safety equipment.
- **Street Lighting:** Street lighting is an essential element for any city. In addition to providing better visibility for pedestrians and motorists, it adds a feeling of safety and security and can often deter criminal activity. Smart cities are adding AI capabilities to street lighting, which is designed to not only provide lighting, but also perform other tasks by incorporating CV, ML, and IoT connectivity. Streetlights can be equipped with an array of sensors to monitor traffic flow, as well as send signals to traffic lights and other traffic control devices.

Manufacturers that have successfully incorporated AI technology generally have been able to achieve the following:

- An understanding of how analytics and AI can work together: Data analytics can and should be used to augment and support AI.
- An understanding of the goals and benchmarks needed to assess AI use cases: AI leaders need to be able to review the output from AI use cases and ensure that proper processes are in place for confirming or overriding questionable results.
- A modicum of trust in AI: All stakeholders need to have confidence that AI can deliver benefits if properly deployed.
- A strong culture of oversight: Regular oversight over the use of AI is critical to ensure that algorithms are delivering the benefits they should, while also remaining in compliance with applicable regulations, is a major key to success. Because the technology is still relatively new, stakeholders are much more likely to stay engaged if they are confident that there is proper oversight occurring on a regular basis.

Generative AI

Traditional AI is trained on large data sets with human input, conversations, user queries and responses. Generative AI is trained on different sets of data to learn patterns to create content with predictive patterns. Generative AI can produce various types of content, including text, imagery, audio, and synthetic data. It is particularly valuable in creative fields and for novel problem solving, as it can autonomously generate many types of new outputs. ChatGPT, DALL-E, and Bard are examples of generative AI applications that produce text or images based on user-given prompts or dialogue.

According to a recent McKinsey Global Survey (<https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year>), 2023 is listed as a breakout year for Generative AI. The survey describes the most commonly reported uses of Generative AI tools to be in marketing and sales, product and service development and service operations such as customer care and back-office support. Inaccuracy, cybersecurity, and intellectual property infringement are the most cited risks of generative AI adoption.

As AI continues to move forward it's important to note the distinction between traditional AI and generative AI. Policies and regulations that are developed need to take this into account.

Finding: There is an insufficient number of people in the current workforce with the technical, digital and analytic skills required to develop, integrate and deploy, operate and maintain IoT devices and IoT-enabled systems and applications.

A significant challenge in scaling IoT into the national infrastructure and economy is the development of a IoT ready workforce. The current workforce lacks many of the key digital, technical and data science skills and expertise required to support IoT. In addition, IoT involves the convergence of various disciplines, including information technology, data science, hardware development, and cybersecurity. Building an IoT-ready workforce requires a workforce with interdisciplinary knowledge who can understand the complexities of both hardware and software components. Integrating these diverse skill sets within a single workforce is a considerable challenge.

The need for a more digital and technical skilled workforce is driven by:

- **IoT requires different skills.** Despite its connected nature, IoT is not IT. IoT is a disparate set of technologies requiring an interdisciplinary combination of existing and new technical, digital and analytic skills. The workforce must

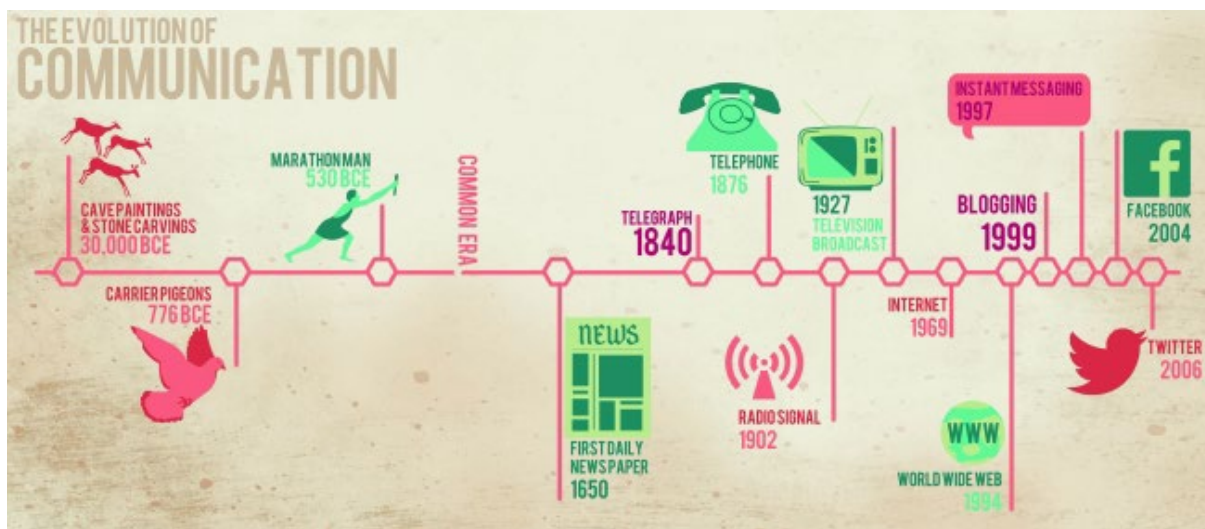
develop expertise in working with new connectivity technologies, such as LoRaWAN and 4G/5G, integration of IoT devices into internal and external networks, and the cloud. In addition, the workforce must develop skills in working with the cloud, and application development. Finally, the amount of data collected required data professionals to manage the data and analyze it to create optimal outcomes.

- **Non-digital industries and systems go digital.** Many pre-digital industries required limited technical and digital skills. For example, the installation and integration of HVAC systems into a building requires mechanical, electrical and ventilation expertise. However, smart HVAC systems incorporating IoT and other technologies now require technicians with networking skills to integrate them into the building's IT network, and systems integration skills to interoperate with building and energy automation systems. Furthermore, smart HVAC systems collect vast amounts of data that must be studied by analytics-savvy operators to optimize occupant comfort and system performance, minimize operating costs and plan maintenance activities.
- **The convergence of IT, OT and IoT systems.** Industries such as manufacturing, energy and transportation employ operations technologies (OT), including supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLC), to monitor and control physical processes. On the other hand, business operations are supported by Information Technologies (IT) systems that process data and communications. In these industries, IT and OT systems operate independently of each other and are maintained by separate organizations. The incorporation of IoT into industrial processes require OT and IT systems to come together. This convergence requires a workforce with a specific set of digital skills, including understanding of IT and OT protocols and processes, cybersecurity, systems integration, cloud computing, programming and application development, IoT integration, data analytics.
- **The value of data analytics.** IoT collects vast amounts of data that can be used to create beneficial and innovative outcomes. Unlocking that value requires a variety of skills, including data management and governance, analysis, and development of insights. In addition, there is a need for the development of algorithms and the application of machine learning and AI tools. While the value of data analytics is understood, there is a current shortage of data savvy practitioners, analysts and scientists across all industries.
- **Interdisciplinary collaboration.** IoT involves the convergence of various disciplines, including information technology, data science, hardware development, and cybersecurity. Building an IoT-ready workforce requires

individuals with interdisciplinary knowledge who can understand the complexities of both hardware and software components. Integrating these diverse skill sets within a single workforce can be a considerable challenge.

Finding: Many barriers to IoT adoption due to legacy infrastructure, security, and interoperability require multi-stakeholder platform-based business ecosystem partnerships that align business incentives on high value end-to-end solutions.

Communication has been transformative for markets and illustrates the potential of connectivity. From carrier pigeons to marathon sprint, to paper, to newspaper, to telegraph, to telephone, to radio, to television, communication have been transformative and drove major market shifts⁵⁵.



Internet connectivity has been even more disruptive. It began with ARPANET followed by the world wide web, commercializing Internet, instant messaging, etc. Facebook and Twitter leveraged connectivity to develop scalable social platforms and reach huge valuations rapidly. However, unlike social platforms that leveraged the growing Internet infrastructure, it will be harder to evolve scalable IoT platforms on top of legacy hardware and software infrastructure.

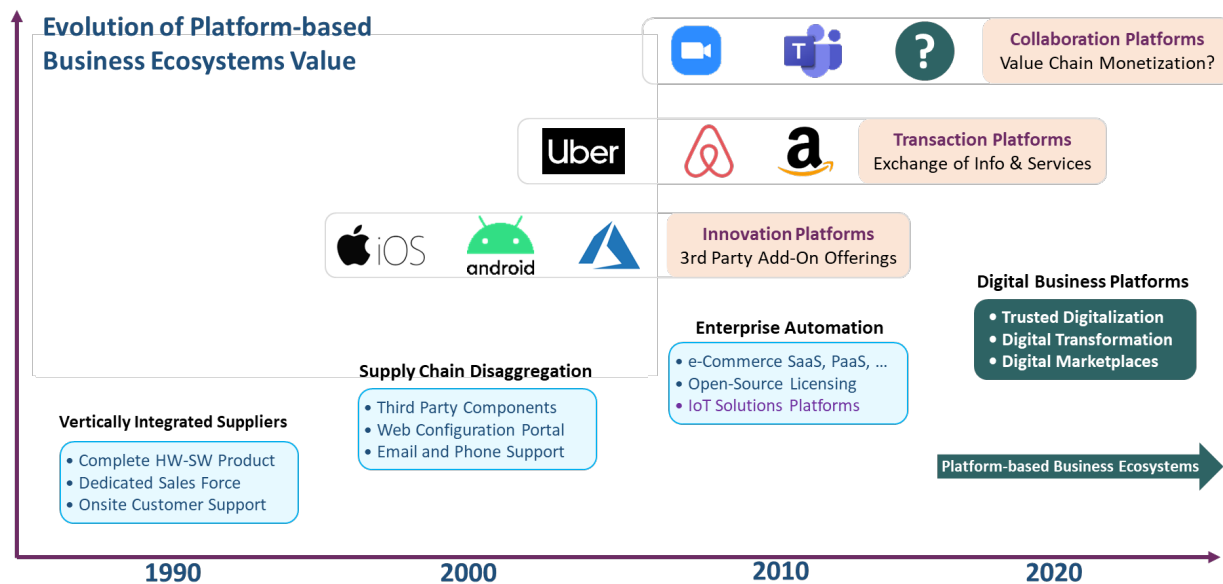
Foundational platforms accelerate evolution of technology ecosystems. History shows that innovative businesses can't evolve in a vacuum. They must attract resources of all sorts, drawing in capital, partners, suppliers, and customers to accelerate growth through cooperative networks and ecologies of competition⁵⁶.

⁵⁵ <https://sci10sectionm.wordpress.com/2013/12/08/the-evolution-of-communication-effects-on-the-world-of-science/>

⁵⁶ <https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition>

Hardware and software value chains evolve from foundational platforms (e.g. *Intel Inside*) into partnerships and scalable business ecosystems.

Partnerships driven by connectivity gave rise to internet business platforms. Since the 90s disruptions, go market strategies, business platforms and revenue models advanced along with new generations of technologies on top of legacy infrastructure. In the new age of ecosystem partnerships⁵⁷ value creation reflects a networked and dynamic collaboration and exchange among partners, which was accelerated with internet-based business platforms.



Platform-based business ecosystems created trillion-dollar valuations. Business scholars have advocated platform-based business ecosystems and their potential to fuel economic value driven by architecture, governance, and network effects⁵⁸. Architecture platforms like Apple iOS and Android enable third parties to add apps to smart phones. Transaction Platforms like Airbnb and Uber enable supply-demand matchmaking for the exchange of goods, or services. Future Hybrid Platforms⁵⁹ combine the advantages of both. Collaborative platforms like MS teams and Zoom which grew rapidly during Covid-19, facilitate innovation, but not business orchestration.

Multi-stakeholder collaborative business platforms failures offer lessons for strategy. The IBM-Maersk TradeLens blockchain platform was taken out of the market⁶⁰ because it was not open and failed to gain stakeholder support in the

⁵⁷ <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ecosystem-partnering>

⁵⁸ <https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/>

⁵⁹ <https://sloanreview.mit.edu/article/the-future-of-platforms/>

⁶⁰ https://www.theregister.com/2022/11/30/ibm_and_maersk_tradelens_shutdown/

maritime supply chain. Collaborative platforms and ecosystems emerge as new organizational forms that provide distinct ways to cope with market failures (e.g. fragmented supply chain) or organizational failures (e.g. silos). Distributional and functional failures arise from self-interested actions by members, undermining the overall value structure⁶¹. Recognizing these failures is crucial for designing effective collaborative multi-stakeholder platforms across the IoT value chain, as they can inform strategies to prevent or mitigate failures, create value, and accelerate adoption.

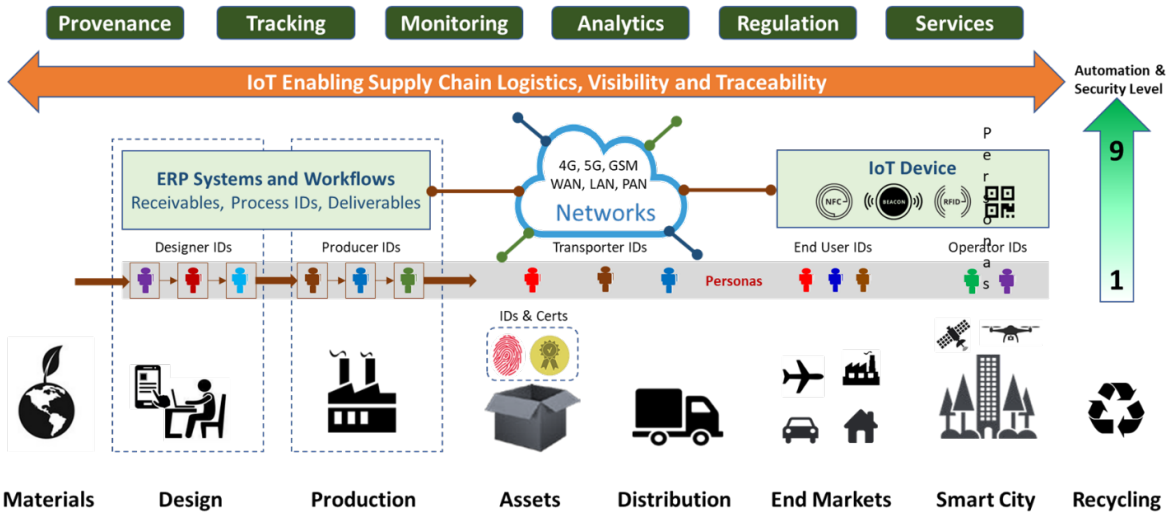
IoT creates opportunities for digital collaboration of orchestrated business ecosystems. As noted before, IoT provides the potential to transform linear supply chains and silos workflows to dynamic value chains and workflows. Transformative IoT platforms enable scalable business ecosystems⁶² where enterprises collaborate to provide coherent end-to-end solutions that benefit all stakeholders. Platform-based business ecosystems based on Digital Orchestration, Governance and Network Effects will fuel Digital Marketplaces to drive economic growth.

Finding: Disconnected supply chains with multiple stakeholders involved pose IoT adoption barriers. Industry specific partnerships using IoT for augmented supply chain logistics reduce risks, speed adoption and fuel economic growth. I don't understand this finding.

Disconnected supply chains can be digitally connected by leveraging IoT technology for global supply chain logistics focused on tracking goods from design, production, distribution, delivery, and end use. The logistics process will consider varied levels of automation relative to the capability maturity of enterprises all the way up to digitalization of logistics workflows.

⁶¹ <https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3Dihub>

⁶² <https://sloanreview.mit.edu/article/how-healthy-is-your-business-ecosystem/>



Logistics for tracking scope will extend to include provenance and traceability of physical objects and data linked to identifiers to deliver assets with trusted information and security for the benefit of suppliers, consumers, distributors, operators, logistics companies, businesses, and all stakeholders in the value chain and industry ecosystems.

Varied levels of security and trust for traceability will be considered for enterprises and global markets, in ways that maximize national security and economic prosperity. Traceability scope will be extended with digital threads to regulate market preference, access, and usage of goods, enable trusted data producers/consumers, marketplaces, and AI applications to fuel growth.

Platform-based business ecosystem partnerships for supply chain logistics tracking, monitoring, and risk management can significantly benefit vertical markets. In each market, these ecosystem partnerships leverage IoT technology to enhance supply chain visibility, transparency, security, and resilience, leading to increased efficiency, reduced costs, and improved customer satisfaction. Exemplified of ecosystem partnerships and value include:

- Automotive Supply Chain Partnerships:** OEMs (e.g., Ford, Toyota), IoT hardware providers (e.g., Bosch), logistics companies (e.g., DHL), data analytics firms (e.g., IBM Watson). OEMs integrate IoT sensors into vehicles and parts. Logistics companies track shipments using IoT-enabled containers and vehicles. Data analytics firms provide predictive maintenance insights. This partnership can optimize supply chain visibility, reduce inventory costs, and improve vehicle maintenance.

- **Industrial Supply Chain Partnerships:** OEMs (e.g., Siemens), IoT sensor providers (e.g., Honeywell), logistics and transportation companies (e.g., FedEx), industrial automation firms (e.g., Rockwell Automation). OEMs embed IoT sensors in machinery. Logistics companies offer real-time tracking of industrial goods. Automation firms use data for predictive maintenance. This partnership enhances supply chain efficiency, reduces downtime, and lowers operational costs.
- **Healthcare Supply Chain Partnerships:** Medical device manufacturers (e.g., Medtronic), IoT solution providers (e.g., Philips), healthcare logistics companies (e.g., UPS), telemedicine platforms (e.g., Teladoc). Medical device manufacturers incorporate IoT sensors for tracking. Logistics companies provide temperature-controlled transportation. Telemedicine platforms offer remote monitoring. This partnership ensures the safe and timely delivery of critical medical equipment and enhances patient care.
- **Communications Supply Chain Partnerships:** Telcos (e.g., Verizon), IoT connectivity platforms (e.g., Sigfox), logistics and distribution networks (e.g., FedEx), supply chain visibility solutions (e.g., Savi Technology). Telcos offer IoT connectivity. Logistics companies use IoT for asset tracking. Supply chain visibility solutions provide real-time insights. This partnership enhances the management of communication equipment and ensures seamless connectivity.
- **Maritime Supply Chain Partnerships:** Shipping and maritime companies (e.g., Maersk), IoT sensor manufacturers (e.g., Inmarsat), maritime logistics firms (e.g., Kuehne + Nagel), weather monitoring services (e.g., The Weather Company). Shipping companies install IoT sensors on vessels and containers. Logistics firms offer real-time tracking. Weather monitoring services provide maritime weather forecasts. This partnership optimizes maritime logistics, reduces delays, and enhances risk management for cargo shipments and can be enhanced with digital collaboration and sharing of data across the maritime ecosystem⁶³.
- **Consumer Supply Chain Partnerships:** Consumer electronics companies (e.g., Apple), IoT device makers (e.g., Fitbit), e-commerce giants (e.g., Amazon), last-mile delivery services (e.g., Postmates). Consumer electronics companies integrate IoT in products. E-commerce platforms use real-time tracking. Last-mile delivery services provide precise delivery windows. This partnership

⁶³ https://thetius.com/wp-content/uploads/2023/10/Common_Interest_Report.pdf

improves customer experience, reduces returns, and minimizes shipping costs.

Top of FormIn each industry, these ecosystem partnerships leverage IoT technology to enhance supply chain visibility, tracking, monitoring, and risk management, ultimately leading to increased efficiency, reduced costs, and improved customer satisfaction. For more detailed information refer to the section on augmented supply chains. Many industries with associations serving common business interested and facilitating partnerships. By leveraging platforms creating network effects⁶⁴ they attract new members, broaden ecosystem IQ and accelerate adoption.

Finding: Digitalization of Enterprise Workflows is Foundational in Creating a Trusted Digital Thread for a Continuous Flow of Data Connecting Business Processes, Products, Assets, and Digital Marketplaces Across Value Chains.

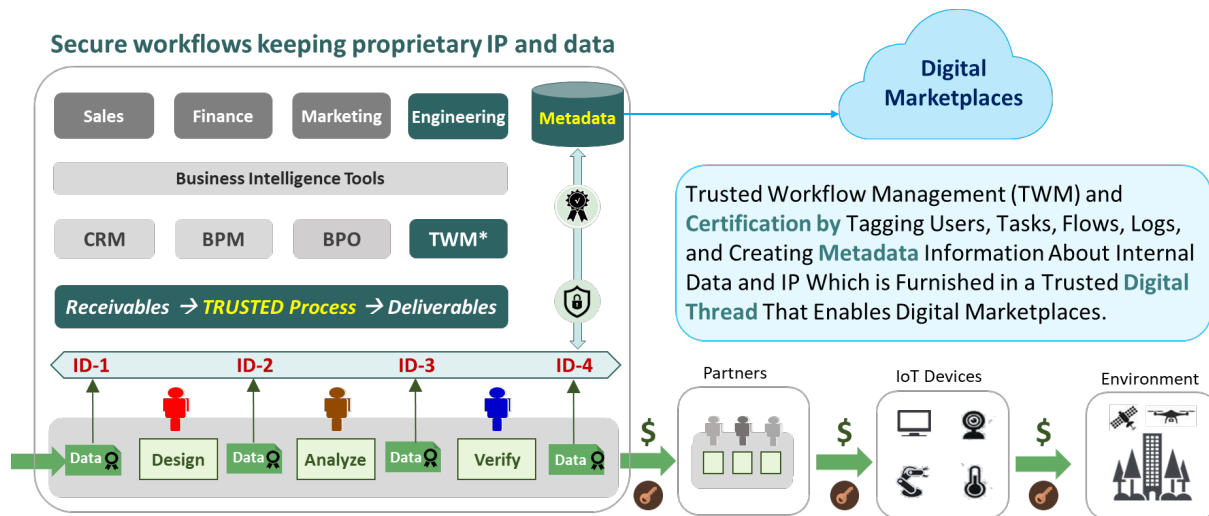
As stated before, IoT provides opportunities to transform linear workflows and supply chains to dynamic value chains.

Supply chain refers to the sequence of activities and processes involved in the production, distribution, and delivery of a product or service to consumers. It primarily focuses on the logistics and flow of goods and services, where IoT can accelerate adoption and add value in improving logistics, automation, and operational efficiency.

Value chain refers to the entire range of activities from the conception of a product or service to its delivery to the end applications. It includes activities related to supply chain logistics, and more. It aims to identify and create value at each stage of the process and provide benefits to all stakeholders that can be realized with digitalization. Digitalization enables digital value chains.

Enterprise Workflow Digitalization for operating functions (Sales, Finance, or Marketing) using tools for Customer Resource Management (CRM), Business Process Management (BPM) and Business Process Optimization (BPO). These tools are used for production planning, procurement, logistics, inventory management coupled with personnel databases.

⁶⁴ <https://www.cornerstoneondemand.com/resources/article/why-network-effect-secret-formula-your-associations-success/>



Trusted Digitalization extends the business process change to design and manufacturing creating products, assets with data linked to operations. Trusted Workflow Management (TWM) can be used to trace and tag users, tasks, data, logs and digital assets to produce metadata and information that can be shared without sharing the proprietary data or IP of the enterprise. By digitalizing the receivables, workflow process, and deliverables, enterprises can participate in value chains, and ultimately digital marketplaces.

Design, manufacturing, physical asset data IDs for part codes, SKUs, serial numbers, etc. can be furnished into a trusted (certified) *Digital Thread* used by data producers, consumers, and partners to share metadata and information about physical and digital assets and workflows about across value chains. Digital marketplaces enable consumers to send queries to producers about which offerings and related data to license and what value-add to create from it.

Trusted Digitalization coupled with secure IoT technology can help trace the movement of assets and data across supply chains, provide transparency to stakeholders and ensure that any information related to products and services is readily available and can be shared securely with relevant parties. Secure enterprise digitalization as discussed in this proposal to NIST⁶⁵ is essential for multi-stakeholder collaboration on supply chain traceability security and resilience.

Digitalization coupled with Digital Transformation is key for accelerating IoT adoption. Digitalization enables automation of manual processes and collaboration among suppliers and consumers. Digital platforms automate order processing, device onboarding, in-field monitoring, and predictive maintenance during field use which

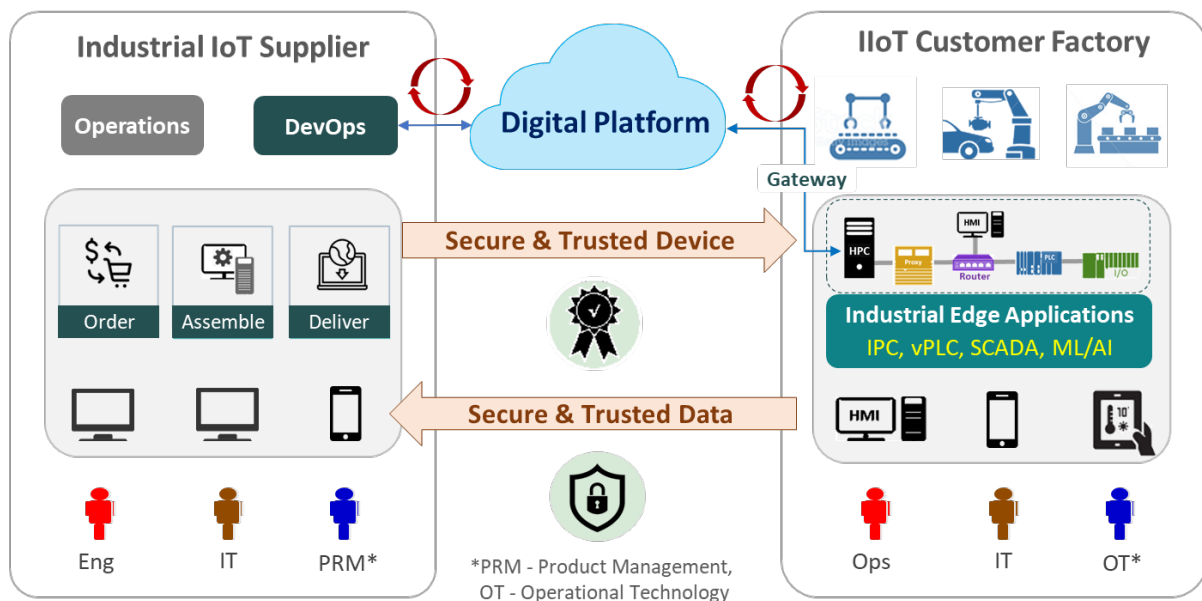
⁶⁵ https://www.nist.gov/system/files/documents/2022/04/25/04-25-2022-GSA_TIES.pdf

results in increased efficiency, reduced operating costs and higher value XaaS (Anything as a Service) business models.

Finding: Digital transformation combining digitalization and organizational changes enables IoT product suppliers to become smart-connected suppliers offering new IoT applications and solutions that drive XaaS revenue streams.

Digital Transformation involves a business process change through Digitalization and organizational changes to enhance IoT operations, customer experiences, competitiveness, process optimization and innovation. Suppliers of Industrial IoT products can become smart-connected suppliers by digitalizing their operations and updating functions and processes. For example, IT organizations will transform from a support function to a value-add function.

Digital transformation for Industrial IoT extends the business process change for suppliers to become high value smart-connected suppliers to their customers via their products. This may require an upgrade of the enterprise ordering and procurement infrastructure to enable data traceability and confidentiality for the enterprises of both suppliers and customers.



Evolving legacy IoT suppliers into smart-connected IoT suppliers drives economic value. In industrial IoT an order of an IPC, PLC or SCADA device starts a process for Just-in-Time (JIT) assembly followed by procurement. Remote updates are not typical.

With digitalization secure IoT devices can be onboarded to the customer's environment and connect via gateway to the supplier. Onboarded devices produce trusted data that can be shared between supplier and customers through a digital platform. This closed loop of trusted and secure data exchange enables several benefits that accelerate adoption:

- **Improved visibility and transparency** through integrated data sharing, facilitating better inventory management and demand forecasting.
- **Real-time monitoring and analytics** of production processes, for identification of inefficiencies and the optimization of workflows that lead to enhanced productivity.
- **Use of trusted data for AI-enabled digital twins** to ensure accurate simulations, timely predictive maintenance and better process optimization boosting operational efficiency.
- **Growth of XaaS⁶⁶ revenue streams** through value-added services and solutions, leading to stronger customer relationships and scalable economic value with partners.

Digital transformation is complex and requires leadership to drive economic growth. Many industrial companies have been slow to embrace digitization, but digital leaders who invested in automation and e-commerce have outperformed their peers in terms of revenues and total returns to shareholders. Digital transformation⁶⁷ provides a first-mover advantage in the industrial sector and has been proven to facilitate a successful end-to-end solutions that encompass culture, organization, and technology systems, ultimately improving services for a diverse customer base.

Industrial digital transformation is a shifting market landscape with constant disruption, affecting several functions, digital technologies and business models for large organizations that strive to drive growth and efficiency. Deloitte has published as collection of topics on Digital Industrial Transformation⁶⁸ that executives can use to accelerate adoption and growth.

⁶⁶ <https://www2.deloitte.com/us/en/pages/consulting/solutions/xaas-everything-as-a-service-model.html>

⁶⁷ <https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/implementing-a-digital-transformation-at-industrial-companies>

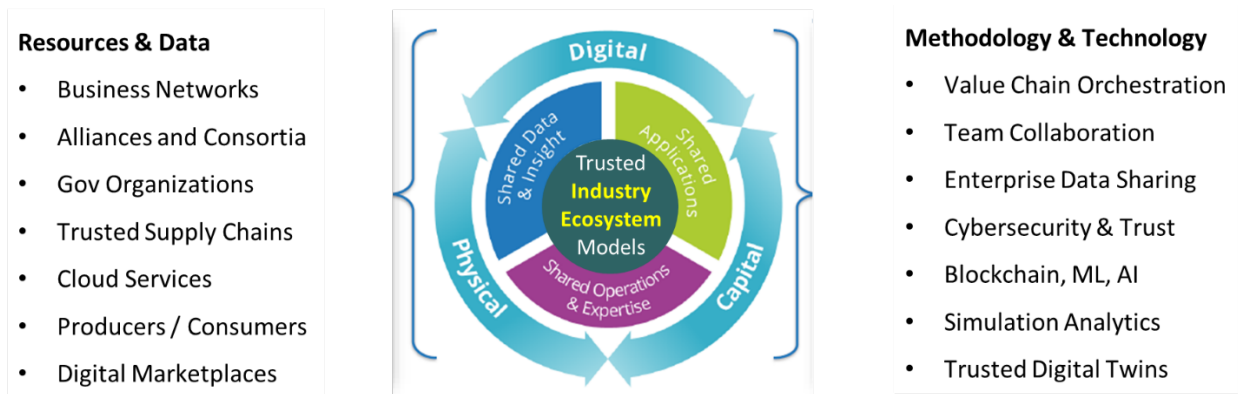
⁶⁸ <https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-transformation-in-the-age-of-industry-4-0.html>

Finding: Slow adoption of enterprise digital transformation is the main barrier to IoT adoption. Phased approaches toward creating a *Digital First Business* are emerging that leverage industry ecosystem partners to drive economic growth.

As stated before, in 2021, McKinsey & Co. revised downward the 2014 projection about IoT growth stating to The IoT has faced headwinds related to change management, cost, talent, and cybersecurity, and slow market adoption of digitalization and cyber-resilience in enterprises.



Enterprises are starting to implement Digital transformation in phases. Market research firm IDC suggests that digitalization has started. In phase 1.0 enterprise test various use cases experimenting with digital technologies. In phase 2.0, they develop new XaaS business models focusing on driving repeatable ROI. Finally, they extend the traditional value chain by working with ecosystem partners to become a **digital first business** to boost growth and profitability.



To accelerate revenue growth, enterprises develop industry ecosystem partnerships in line with their business needs by solving key problems in their industry. Industry ecosystems must have a core mission, and business incentives for companies to work together. The fundamental pillars of ecosystems include shared data insights, shared applications and shared operations and expertise⁶⁹.

⁶⁹ <https://www.idc.com/promo/future-of-x/industry-ecosystems?tab=one>

Trusted industry ecosystems evolve from two key core competencies *Resources & Data* to maximize collective IQ output and *Methodology & Technology* to maximize operating efficiency.

Resources & Data bring several parties collaborating in Private-public partnerships (PPPs) including, trusted networks, consortia, supply chains, government organizations, cloud services and digital marketplaces providing shared operational intelligence. PPPs accelerate the creation of data ecosystems⁷⁰, which are vital for growth of digital businesses generating high margin recurring revenue streams. Many ecosystems focus on the provision of data: exchange, availability, and analysis. Incumbents seeking to excel in these areas must develop the proper data strategy, business model, and architecture⁷¹ to create services that improve customer relationships, lift adoption barriers, and secure strong positions through economies of scale.

Methodology & Technology help harmonize stakeholder orchestration, collaboration, data sharing and governance across supply chains or value chains by using adjacent technologies like blockchain, cybersecurity, ML/AI and digital twins enabled by trusted digital threads to maximize the value for all. Harmonization takes ecosystems to the next level⁷² in creating value by consolidating supply chains horizontally across sectors and strengthening touchpoints along value chains vertically. Participants collaborate and incentivize each other, fostering innovation and efficiency improvements across business ecosystems. Traditional companies need to expand beyond their historical industry boundaries to serve customers comprehensively. Multiple sectors, including B2B services, mobility, travel, health, and housing, are transitioning into vast ecosystems, potentially forming a \$60 trillion integrated network economy by 2025.

Multi-stakeholder orchestration and business platforms should consider how ecosystems can integrate capabilities or IoT and AI, for circular economies, and cope with challenges related to value creation, regulation, and misinformation. To speed adoption the US government should consider the creation of an office for emerging technologies, IoT, 5G+, AI, Blockchain, and Quantum Computing, as stated in an earlier finding and commentary.

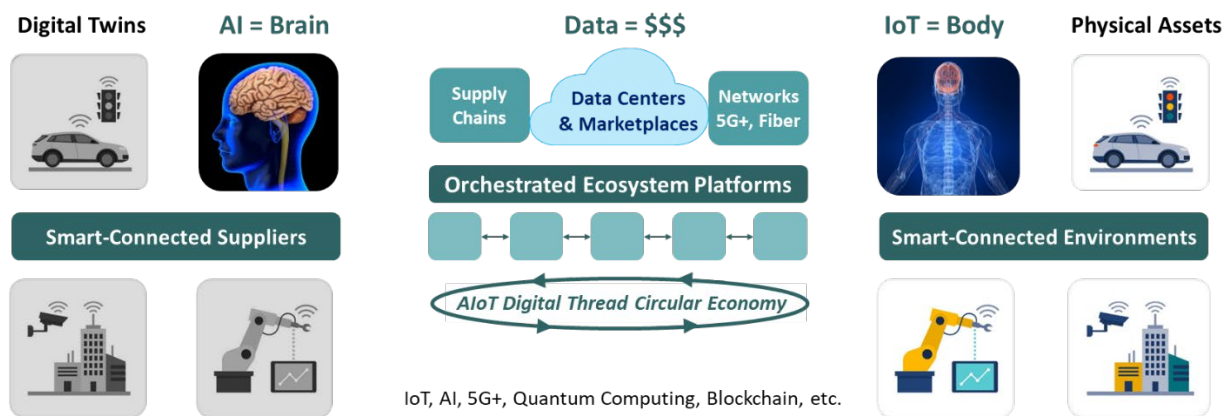
⁷⁰ <https://www.bcg.com/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition>

⁷¹ <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/data-ecosystems-made-simple>

⁷² <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/ecosystem-2-point-0-climbing-to-the-next-level>

Finding: Convergence of AI and IoT plus adjacent technologies and platforms serving circular supply chain ecosystems will accelerate sustainability and drive disruptive growth fueled by massive data centers in a hyperconnected planet.

The global economy operates linearly, extracting, producing, consuming, and disposing of materials, posing challenges due to finite resources. Transitioning to a circular economy, where resources are recovered and recycled, has been elusive but offers trillions in value. Barriers include low residual product value, material collection challenges, high processing costs, and supply chain traceability and monetization issues. AI and IoT platforms collapse these barriers⁷³.



IoT is the body and AI is the brain, supply chains & networks are the arteries where data flows. Orchestrated AI + IoT (AIoT) platforms linking smart-connected suppliers with smart-connected environments powered by massive data centers will create digital marketplaces and sustainable ecosystems, which will surpass human intelligence in a few decades. AIoT and data are intricately interconnected in a circular, rapidly evolving technological landscape⁷⁴:

1. **Data and IoT:** IoT devices generate vast amounts of data through sensors and connected devices, including temperature readings, location information, and user interactions. This data can be stored and analyzed to gain insights and make informed decisions, such as optimizing energy usage or monitoring machinery health.
2. **Data and AI:** AI relies heavily on data with machine learning algorithms requiring extensive datasets for training. Once trained, AI models can analyze and interpret data for tasks like natural language processing and predictive

⁷³ <https://hbr.org/2023/06/how-ai-will-accelerate-the-circular-economy>

⁷⁴ <https://www.linkedin.com/pulse/transformational-power-data-ai-iot-shaping-worlds-future-jha/>

analytics, extracting valuable insights and patterns that may be too complex for manual analysis.

3. **AI and IoT:** AI enhances IoT systems by processing and analyzing real-time data from IoT devices. For instance, AI algorithms can detect anomalies, predict equipment failures, or optimize resource allocation in smart cities. AI empowers IoT systems to make autonomous and intelligent decisions based on the data they collect.

The convergence of IoT and AI will drive high value solutions across industries.

Data is the new raw material or the “new oil” for AI, which, in turn, can be applied to analyze and extract valuable insights from the data generated by IoT devices. This synergy between data, AI, and IoT coupled with quantum computing powered by massive data centers will drive advancements across various industries, including healthcare, manufacturing, transportation, and smart cities.

- **Smart Cities:** Implement AI-powered analytics on IoT sensor data to optimize traffic flow, waste management, energy usage, and public safety in urban environments.
- **Predictive Maintenance:** Use AI algorithms to analyze IoT data from industrial machinery and equipment to predict maintenance needs, reducing downtime and improving operational efficiency.
- **Healthcare Monitoring:** Combine IoT wearables with AI-powered analytics to monitor patients' health data in real-time, enabling early detection of health issues and timely medical interventions.
- **Supply Chain Optimization:** Employ IoT sensors to track goods in transit and use AI to predict potential disruptions, enhancing supply chain visibility and reducing inefficiencies.
- **Precision Agriculture:** Utilize IoT devices to gather data on soil moisture, weather conditions, and crop health, then apply AI algorithms to optimize irrigation, planting, and harvesting. Utilize sensors and analytics to measure spoilage in storage and distribution.
- **Energy Management:** Integrate AI algorithms with IoT-connected devices to optimize energy consumption in buildings, adjusting lighting, heating, and cooling based on occupancy patterns.

- **Connected Vehicles:** Use IoT sensors in vehicles to collect data on driving behavior and road conditions, then apply AI to improve road safety, traffic management, and vehicle diagnostics.
- **Environmental Monitoring:** Deploy IoT devices to collect environmental data (air quality, water levels, etc.), and employ AI to identify trends and potential hazards.
- **Smart Homes:** Integrate IoT devices like smart thermostats, cameras, and appliances with AI to create intelligent and automated home management systems.
- **Wearable Health Tech:** Combine IoT wearables with AI-driven analytics to provide personalized health recommendations based on continuous monitoring of vital signs.
- **Industrial Automation:** Use AI to analyze data from IoT sensors in manufacturing processes, optimizing production, quality control, and resource utilization.
- **Natural Disaster Management:** Combine IoT sensor networks with AI algorithms to predict and manage natural disasters, such as flood monitoring and early warnings.
- **Agricultural Automation:** Use AI and IoT to automate tasks like planting, watering, and harvesting in agriculture, leading to increased crop yield and reduced labor costs.
- **Energy Grid Optimization:** Utilize IoT-enabled smart meters and AI algorithms to balance energy demand and supply, improving efficiency and reducing costs.
- **Waste Management:** Combine IoT sensors on waste bins with AI analytics to optimize waste collection routes and schedules, reducing fuel consumption and operational costs.
- **Consumer Electronics:** Infuse AI capabilities into IoT-connected consumer electronics to create intelligent devices that can learn user preferences and adapt their behavior.

- **Smart Appliances:** Integrate AI and IoT to create appliances that can interact with users, optimize energy usage, and provide real-time feedback on performance.

Orchestrated platform ecosystems combining AI and IoT accelerate adoption and growth of digital economies. IoT produces data, AI consumes data, supply chains and networks transport data and data centers process applications to monetize data for a wide variety of use cases. Emerging trends in digital platforms include sustainability, connected manufacturing, creator economies, and new regulations⁷⁵:

1. **Integration of Artificial Intelligence (AI):** AI is becoming integral to digital platforms, offering scalability, flexibility, better decision-making, and personalized processes. Some platforms will offer AI as a service, while others will adopt AI for their own operations. Challenges include addressing biases, labor issues, and equitable share of AI benefits.
2. **Growth of Circular Platforms:** Digital platforms will support circular economies by enabling product and material exchanges, promoting reuse, repair, redesign, and recycling. Opportunities include material exchanges, reuse/resale marketplaces, sharing assets (e.g., cars, real estate), circular supplier networks, and sustainable logistics.
3. **Varied Platform Regulations:** Platforms face new regulatory oversight, with variations between geographic regions. For example, the US Section 230 offers legal immunity for content posted by third parties, while the EU Digital Services Act requires transparency and holds platforms liable for violating terms of service.
4. **Connected Manufacturing:** Manufacturing is adopting digital technologies with platform-based solutions leveraging data for smarter factory operations, optimized supply and demand forecasting, and predictive analytics. This enhances supply chain visibility and competitive advantage.
5. **Increasing Power of Influencers and the Creator Economy:** The creator economy, estimated at \$100 billion, is driven by independent creators monetizing their activities. Influencers and creators face challenges like burnout and time management, with AI tools like ChatGPT offering assistance in saving time and managing workloads.

⁷⁵ <https://mitsloan.mit.edu/ideas-made-to-matter/5-trends-mit-platform-report>

The circular nature supply chains require trusted digital threads combining AI and IoT. Trusted digital twins and AI require trusted data produced by trusted devices. Trusted devices require trusted hardware and software bills of materials (HBOM and SBOM). Trusted HBOM require trusted design and manufacturing of physical assets that may be disposed on recycled. The convergence of IoT and AI has a potential to drive high-value sustainability platforms across circular supply chains for tracking and monitoring product utilization, analyzing materials to minimize waste, and increasing the use of recycled materials to reduce carbon emissions.

The explosive growth of AI and IoT platforms require monitoring and regulatory actions: The above use cases are a fraction the vast potential combining AI and IoT platforms fed by data transported through supply chains or networks which may or may not be trusted. ChatGPT platform reached 100M users in a fraction of time compared to Twitter and Facebook and 2M developers creating a plethora of APIs and apps. Many of these developers rogue actors from adversary nations connecting remotely to AI platforms, so monitoring and regulating these platform ecosystems are key to mitigate risks and drive growth.

Industry findings

Finding: Precision Agriculture. IoT brings significant value to agriculture, but adoption is slow.

Agriculture is undergoing a transformation driven by the integration of information and digital communications technologies, the Internet of Things (IoT), data analytics, automation and robotics and other emerging technologies.⁷⁶ This transformation offers the potential to increase agricultural productivity, operational efficiency, facilitate adaptation to climate changes and enhance overall competitiveness.

Some examples of top IoT applications in agriculture include:

- **Precision Farming.** IoT sensors on tractors, drones and in the soil collect data on soil moisture, nutrient levels, and crop health. This information enables precision farming by optimizing the use of water, fertilizers, and pesticides to increase crop yields and reduce waste.

⁷⁶ "Agriculture 4.0: Broadening Responsible Innovation in an Era of Smart Farming", D. Rose and J. Chilvers, Frontiers in Sustainable Food Systems, Dec 21, 2018. Link

- **Smart Irrigation.** IoT-based irrigation systems monitor weather conditions and soil moisture levels, enabling automated and efficient watering. This reduces water wastage and ensures crops receive the right amount of water.
- **Livestock Monitoring.** Wearable IoT devices on livestock provide real-time data on animal health, behavior, and location. Farmers can quickly identify signs of illness, track grazing patterns, and enhance overall livestock management.
- **Crop Monitoring and Predictive Analytics.** IoT sensors in fields continuously monitor environmental conditions and provide data for predictive analytics. Farmers can anticipate disease outbreaks, pest infestations, and make informed decisions to protect their crops.

The application of IoT to agricultural production and operations produces a variety of benefits, including increased efficiency, minimize and optimize the use of inputs (water, fertilizer, pesticides, and herbicides), improve crop and livestock production yields, reduce waste, and decrease costs and increase profitability.

- **Increased Efficiency.** IoT helps farmers and ranchers become more efficient and productive. For example, the use of IoT to monitor animal health minimizes the need for workers to physically inspect the livestock on a regular basis. Sensors mounted on drones flying over large fields check plant health and quickly identify areas needing attention. Autonomous tractors and combines facilitate row crop operations with minimal human involvement.
- **Input Optimization.** IoT devices help optimize the amounts of inputs (water, fertilizer, pesticides, and herbicides) to be used based on real-time knowledge of growing conditions and providing insights into the exact needs and application of inputs to maximize crop growth and health.
- **Enhanced Yield and Quality.** Agriculture is a data-driven business. The ability to monitor growing conditions, animal and crop health in real-time, along analyzing the data collected, helps farmers identify and respond to issues earlier and more proactively. This facilitates crop and livestock production, leading to improved yields and less waste.
- **Cost Savings.** IoT yields cost savings by reducing and optimizing the use of inputs, minimizing livestock health issues, support automation, and reducing the number of workers needed to support operations. These cost savings increase productivity and improve profitability and cash flow.
- Story 1: IoT can help small family farms be productive and profitable

- 2 million farms in US. 98% are family farms. Small family farms (gross income < 350K) are 90% of all farms, 48.8% of all farmland, and 21.1% of production
- 62 - 81% of these small family farms are operating on < 10% margins
- Production expenses have increased by 18% in 2022
- Story 2: IoT can help agricultural producers navigate around the impacts of the changing climate.
 - Changing temps and precipitation patterns affect plant lifecycles, decrease crop yields, increase livestock stress and health, reproduction and milk and egg production
 - Corn yields have declined 3.8% and wheat yields have declined 5.5% (compared to no climate trends)
- Story 3: IoT can help increase agricultural production yields to support the upcoming food shortage
 - By 2050, UN estimates there will be a global food shortage
 - Increase in half percent in yield was enough to end starvation and famine in India (Green Revolution)

IoT in agriculture suffers from a variety of challenges. The top barriers include:⁷⁷

- **Connectivity.** Agricultural producers face three connectivity challenges. First, there is very limited broadband infrastructure and Internet service in rural areas, and many agricultural producers lack “broadband to the farmhouse”. Second, while the FCC considers 25/3 Mbps (download/upload) service to be the broadband benchmark, this asymmetric level of performance is insufficient for precision agriculture needs which send large amounts of data, such as drone imagery and mapping data, to cloud data centers for processing and analyses to support critical decision-making in a timely manner. Finally, wireless connectivity service must be made available to the “last acre” to support agricultural activities. This is complicated by the size of farms and ranches, some of which span thousands of acres over diverse terrains.

⁷⁷ Chan, B., Feller, G., Paramel, R., Reberger, C., 2022, September. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things Sponsored by the National Institute of Standards and Technology

- **Digital skills.** As digital and emerging technologies are increasingly integrated into agricultural equipment and operations, the skills that agriculture workers need to be successful will change. For example, as smart machines increasingly automate previously manual activities, agriculture jobs will evolve from being low skill repetitive physical work to medium to high skill non-repetitive digital work. New skills include data analytics, precision agriculture, robotics and automation, networking, and systems integration.
- **Interoperability.** Farms have a variety of equipment, from the “latest and greatest” equipment with current technology to 30- to 40-year-old legacy equipment with limited technology and no connectivity. Interoperability challenges are a major barrier to IoT adoption and value realization in agriculture where old and new equipment coexist and work together. Many of the machines employ a variety of proprietary and incompatible protocols that make sharing information with each other, as well as farm operations software difficult or impossible. For example, some equipment may incorporate incompatible physical connections and require the use of adapters to communicate with other equipment. Others may have different formats (or syntaxes) for the same data, while others have different meanings for the data. Old equipment may not work with newer equipment, despite coming from the same manufacturer.
- **Adoption resistance.** Despite the benefits of IoT and precision agriculture technologies and solutions, uptake of these solutions have been uneven and may take as long as 15 years for the technology to reach a critical mass.⁷⁸ Large producers are more likely to adopt these technologies compared to smaller farms because they have more education, are less wary of technology and can support larger economies of scale.⁷⁹ Some of these reasons, include the limited availability of broadband and connectivity in rural areas, “right to repair” concerns, trust in personal expertise over technology, and poor previous experiences with technology.

Need Ranveer and Nick content/stories here. Maybe use the story ideas I had supplied previously.

⁷⁸ “Adoption of Farming Technology, Or Precision Ag, Varies Across Generations”, KTTN News, December 20, 2020. [Link](#)

⁷⁹ “Adoption of Precision Agriculture”, USDA NIFA. [Link](#)

Finding: Smart cities and infrastructure. The development of smart cities in the United States is limited, uneven and slow to develop.

IoT and its adjacent technologies offer the potential to transform cities and communities to become more responsive, resilient and sustainable. For residents of these communities, smart cities offer opportunities to improve quality of life, drive economic vibrancy, and increase public safety. Despite the potential for beneficial outcomes, current smart city efforts in the United States are small in scale, limited in scope and fragmented in nature.

While the vision of a fully connected and integrated city or community is still decades away, there are examples of IoT-enabled smart city applications in use today. These include:

- Smart streetlights employ LED bulbs, connected sensors and a controller to dim and brighten the streetlamps as needed. Streetlights may be dimmed late at night to reduce energy usage, and brightened during the evenings when people are returning home to increase safety. Smart streetlights also determine if the lamp has malfunctioned, and notifies city staff immediately so that it can be replaced.
- Smart parking employs either in-ground sensors or cameras to monitor parking space availability. Open spaces are communicated to drivers through a mobile app or digital signage on the street or garage. This helps drivers navigate to the space directly, instead of driving around looking. In addition, it also helps identify parking space violations and direct parking enforcement officers to the spot directly without having to drive around.
- Community air quality networks are deployed in select areas of the community to monitor environmental conditions and inform residents and policymakers. Air quality networks may be deployed in areas with poor air quality, or where poor air quality would harm vulnerable populations. For example, the communities directly adjacent to freeways or industrial plants are subjected to poor air quality.
- Intelligent traffic management systems help manage the flow of traffic, minimize congestion and decrease accidents and injuries. These systems monitor traffic flow, adjust streetlight signal timing based on real time conditions, and monitor traffic and pedestrian behaviors. For example, LIDAR or camera-based traffic analytics systems monitor “near misses” at intersections and inform traffic engineers of dangerous conditions to be addressed.

- Camera systems employing AI and facial recognition algorithms help reduce crime and aid in the identification and capture of criminals. Images are captured and analyzed in real time by facial recognition software.

[Describe some benefits of Smart Cities]

Despite the tremendous potential offered, smart cities have been slow to develop. This is attributed to a variety of reasons. These include:

- Awareness and Vision. Many community and political leaders lack awareness of IoT and smart city technologies. Others lack the vision and the innovation culture to incorporate these technologies and capabilities into a city's infrastructure and operations.
- Lack of funding. Funding is one of the top issues holding back smart cities. These projects, at scale, is very expensive. While larger cities may have the capabilities and some funding vehicles to support these projects, America's small and medium size cities do have very limited capabilities. In some cases, federal, state and regional grants may be available, but securing these grants can be difficult.
- Lack of skills and resources. Many cities and communities lack the new innovation and digital skills and resources to plan, deploy, operate and support IoT applications. These resources are scarce in the market, and cities often cannot compete with the private sector for the same talent.
- Privacy Concerns. The extensive collection of data from IoT devices raises concerns about data security and privacy. Ensuring robust cybersecurity measures and transparent data handling practices is crucial to building and maintaining public trust.
- Community and political resistance: Candidates are not elected for building a smart city. Political leaders are re-elected if they are responsive to the needs of their constituents. Smart city initiatives that don't align with the city's strategic and near-term priorities are likely to face resistance from both citizens and policymakers.

Smart Infrastructure

Infrastructure is essential to the functioning and resilience of the United States. For example, a nationwide network of roads, waterways, rail and airports transports freight and goods to market, and connects people with places. A regional system of natural and man-made reservoirs, aqueducts, pipes, pumping stations, and treatment

plants brings fresh water to cities and farms. Electricity generated from renewable and non-renewable energy power plants travels over through a network of transmission lines and substations to power cities and communities across the country. Sewage is routed from homes and buildings through a regional network of underground pipes to wastewater treatment plants for reclamation for reuse and release.

Smart infrastructure integrates IoT and other digital technologies into physical infrastructure. This convergence enables new innovative capabilities for physical infrastructure and allows it to be managed, operated, and maintained more efficiently and effectively. Sensors embedded into infrastructure, such as roads, building structures and machinery, monitor its condition in real time, notifying operators of abnormal conditions immediately so that it can be addressed before it becomes a hazard or lead to service interruptions. Data collected from the sensors are analyzed by algorithms to optimize performance and usage, predict maintenance needs, and extend infrastructure life. In addition, IoT data helps validate and improve engineering models, build high fidelity digital simulations, and facilitate managerial and operational decision-making.

The benefits enabled by smart infrastructure include increased reliability, service availability and improved delivery of services. For example, streetlights provide illumination to increase road and pedestrian safety, reduce crime and facilitate economic vibrancy. However, broken streetlights take months to be replaced because the city or utility company is unaware of the problem. IoT-enabled streetlight sensors notify the city or utility company immediately of broken lights, leading to replacements in days, not months. In another example, fatal and non-fatal traffic accidents commonly occur in street intersections. “Smart intersections”, equipped with cameras employing artificial intelligence algorithms mounted on traffic signal poles, capture vehicle and pedestrian behaviors that allow traffic engineers to study and apply corrective actions before serious accidents occur.

Other benefits of smart infrastructure included optimized operations and decreased costs. For example, mechanical water pumps equipped with sensors monitor equipment conditions during operation. The sensor data is analyzed by algorithms to determine when maintenance is actually needed so that the pumps can be proactively serviced, thereby ensuring continuous system operation and preventing cost escalation. Similarly, smart electrical grids employ sensors and two-way communications between utilities and consumers to monitor and manage power flows, and respond to changes in electricity demand. This ensures that the most appropriate energy sources, including renewable energy, batteries, and upstream generation plants, are utilized to meet demand while increasing grid resilience,

reducing operational costs, and minimizing carbon emissions from upstream fossil fuel power sources.

A third benefit of smart infrastructure is its facilitation and acceleration of a future autonomy-driven economy, supporting autonomous vehicles and machinery, autonomous robotic operations, and other AI-driven applications. Despite the advances in autonomous vehicle technology, they are still many years away from truly safe and reliable operation. The sensors and processors in smart infrastructure provide additional data that autonomous equipment, machines and vehicles need in order to operate safely and reliably. For example, today's autonomous vehicles operate based on the limited information collected through its on-board sensor array. Sensors embedded on roads and buildings provide an extended set of "eyes and ears" to complement the limited range of the vehicle's on-board sensors. This additional "beyond line of sight" information is shared and processed by the vehicle's algorithms and enables better decisions and safer, more reliable, and predictable operations.

Despite the many capabilities and benefits offered by smart infrastructure, American infrastructure is old and failing. It must be repaired, replaced, and upgraded before it can be digitized and made "smart". The American Society of Civil Engineers (ASCE) have given American infrastructure an overall C- grade in its 2021 report card,¹ a slight improvement from the previous report card (2017), which rated the state of American infrastructure as D+.² For example, the United States has over 2.2 million miles of underground pipes that deliver drinking water. There is a water main break every two minutes and an estimated 6 billion gallons of treated water are lost each day.³ Many of America's wastewater treatment plants were built in the 1970's and have an average life span of 40-50 years.⁴ This aging infrastructure and inadequate capacity leads to the discharge of 900 billion gallons of untreated sewage into U.S. waterways each year.⁵ Of the four million miles of public roadways in the United States, 43% are in poor or mediocre condition.⁶ The poor road infrastructure resulted in motorists paying an additional \$1,000 annually in time and fuel, 36,000 road deaths annually and rising pedestrian fatalities.⁷

Another concern is the vulnerability of smart infrastructure to cybersecurity threats, cybercriminals, and malicious state actors. IoT and other smart technologies create new attack surfaces and vulnerabilities to assets and infrastructure that had traditionally not been digitized or had been protected through "air-gaps". These cyberattacks may lead to disruption of operations and services, compromise of control and operational capabilities, and harm to millions of Americans who rely on this infrastructure. For example, the energy sector was the third and fourth most targeted sectors in 2020 and 2021 respectively.⁸ The utility industry averaged 736 cyberattacks per week and experienced a 46 per cent year-over-year increase in cyber-attacks in 2021.⁹ In 2019, a renewable energy generator company, the largest private owner of

operating solar assets in the United States, was subjected to a denial-of-service attack. While no loss of energy generation was reported in the attack, the company lost visibility into about 500 MW of wind and PV generation in California, Utah and Wyoming.¹⁰ Similarly, U.S. water utilities are prime targets for cyberattacks. The March 2020 Cyberspace Solarium Commission report stated that the nation's 70,000 water utilities "remain largely ill-prepared to defend their networks from cyber-enabled disruption."¹¹ In 2021, an operator at a small water treatment plant in Oldsmar, Florida, thwarted an attempt by an intruder to boost the level of sodium hydroxide (lye) in the water supply to 100 times higher than normal.¹²

While the Bipartisan Infrastructure Law of 2021 provides funding to repair and update America's infrastructure, it also represents a "once in a lifetime" opportunity to build an initial set of smart infrastructure and realize the benefits that it brings.

- Some content on smart cities
- Some content on public safety

Finding: Transit and traffic: IoT is transforming transit systems and traffic management with real-time data analytics, intelligent traffic management, and predictive analytics to enhance efficiency, reduce congestion, increase safety, and improve overall transportation experiences.

According to data from the National Highway Traffic Safety Administration (NHTSA), in 2022 an estimated 42,795 people died in motor vehicle crashes. While this latest estimate shows that roadway fatalities have remained flat after two years of dramatic increases, Transportation Secretary Pete Buttigieg states that "We continue to face a national crisis of traffic deaths on our roadways, and everyone has a role to play in reversing the rise that we experienced in recent years." <https://www.nhtsa.gov/press-releases/traffic-crash-death-estimates-2022>. Back in January of 2022, the DOT released the comprehensive [National Roadway Safety Strategy](#), a roadmap to address the national crisis in traffic fatalities and serious injuries. One of the key actions in that roadmap includes leveraging technology to improve the safety of motor vehicles on our roadways.

Smart traffic technologies provide an organized, integrated approach to minimizing congestion and improving safety on streets through connected technology. These technologies smooth traffic flows and prioritize traffic in response to demand in real time. They enhance pedestrian, bicycle and vehicle safety and reduce accidents that cause injuries and fatalities. Connected vehicles can alert drivers of potential hazards such as pedestrians crossing the street or other cars in the vicinity. Smart traffic lights can detect when cars are approaching and adjust their timing accordingly,

minimizing the risk of accidents. Using adaptive control, detected vehicle congestion triggers changes to traffic signal timing to optimize traffic throughput in near real-time. Traffic signal timing can be adjusted to maintain schedules of bus and rapid transit lines. A path through the city is coordinated for first responder vehicles, using congestion data and vehicle location to adapt route guidance and traffic signal timing allowing these vehicles to get to their destination sooner.

These technologies can facilitate and support multimodal transit and other innovative transportation models (including ride-share, e-scooters, drones, etc.). They also facilitate the safe testing and operation of autonomous vehicles (including cars, trucks, robotic delivery services, etc.). They can also reduce energy consumption by obviating stop-start driving that typically occurs at intersections.

There is a large and growing ecosystem of public and private sector stakeholders to deploying this technology that will redefine traffic safety. Some examples showcasing their benefits are provided below.

- A project to deploy Cellular Vehicle to Everything (C-V2X) in vehicles as part of an ongoing joint project with the Virginia Department of Transportation, the Virginia Tech Transportation Institute, and others to showcase the technology's ability to improve work zone and intersection safety.⁸⁰
- A collaborative venture among an auto maker, school bus maker, and a school system that demonstrated C-V2X's ability to protect children in and around school zones and bus stops.⁸¹
- A project with an auto maker and a bicycle safety platform maker to highlight the benefits of C-V2X-powered bicycle use cases.⁸²
- A project with the Tampa Hillsborough Expressway Authority (THEA) to deploy and pilot Connected Vehicle (CV) applications to demonstrate safety and mobility benefits of the technology with respect to pedestrians in and around downtown Tampa.⁸³
- A project with the Florida Department of Transportation (FDOT) to test and implement connected vehicle and pedestrian/bicyclist safety applications

⁸⁰ Jacob Levin, "Virginia Tech Transportation Institute researchers to deploy smart work zone in Wise, Virginia," Virginia Tech Exponentially More (May 19, 2022), https://vtx.vt.edu/articles/2022/05/vtt-smart-work-zone.html?utm_source=cmpgn_news&utm_medium=email&utm_campaign=vtUnirelNewsDailyPublicCMP_052022-public; Audi, *Audi collaborates to deploy C-V2X communication technology on Virginia roadways* (Sept. 29, 2020), <https://media.audiusa.com/en-us/releases/437>.

⁸¹ Press Release, Audi, (Mar. 30, 2021), *Blue Bird, Fulton Co. Schools join Audi, Applied Information on connected vehicle deployment to boost school bus and school zone safety*, <https://media.audiusa.com/en-us/releases/465#>

⁸² Press Release, Audi, *Audi joins Spoke Safety, Qualcomm, Commsignia to help protect bicyclists through connected technology*, <https://media.audiusa.com/en-us/releases/514>.

⁸³ https://www.its.dot.gov/pilots/pilots_thea.htm

(active or passive) at 13 signalized intersections and 8 mid-block crossings within the core of the University of Florida (UF) campus.⁸⁴

- The New York City Department of Transportation Traffic Safety Network. a large-scale Intelligent Transportation System (ITS) upgrade, replacing their entire citywide traffic communications network with a cellular IoT system. DOT's traffic management system controls the traffic signals at 14,000 intersections, as well as a range of ITS devices including traffic cameras, variable message signs and vehicle detection devices. The new network is highly automated, secure, and achieves four 9's availability using dual concurrent cellular links.⁸⁵
- Tri-Met in Portland, OR. The Tri-County Metropolitan Transportation District of Oregon (TriMet) serves an area of 500 square miles, operating a fleet of over 700 buses on 85 routes with thousands of stops. Smart systems maintain bus intervals and on congested corridors, prioritize bus travel over other vehicles by sensing bus arrival time then manipulating traffic signal phases⁸⁶
- Positive Train Control- - SEPTA, LIRR, MNR, MBTA, AMTRAK. Positive Train Control (PTC) utilizes GPS, sensors and wireless communications technology to autonomously stop a train when necessary and to prevent train-to-train collisions, over-speed derailments, and unauthorized train movement. PTC helps ensures the safety of passengers by acting as a safeguard against human errors and other potential hazards.⁸⁷

Generally speaking, these technologies include hardware, software, systems, and some type of connectivity. Hardware includes traffic signals and traffic controller assemblies, dynamic message signs, connected vehicle roadside units, cameras, sensors, LIDAR, electric vehicles (EVs) and EV charging equipment, vehicles with varying levels of autonomy (drones, delivery shuttles), and electric mobility (scooters, e-bikes). Systems include those that focus on security, intelligence, monitoring, and management. Software includes route planning and travel alerts. Connectivity includes- Cellular Vehicle to Everything (C-V2X), 5G, autonomous navigation both edge and cloud techniques.

While there are several opportunities and benefits for personas that use these technologies, primarily in the realm of safety (e.g., emergency vehicle preemption, entering school or work zone, pedestrian crossing ahead), these technologies can also provide valuable support functions such as package, food, and medicine delivery. There are also environmental benefits from congestion mitigation and providing an

⁸⁴ <https://teo.fdot.gov/architecture/architectures/d2/html/projects/projarch47.html>

⁸⁵ <https://www.digi.com/resources/customer-stories/new-york-city-dot-deploys-digi-solutions>

⁸⁶ <https://www.digi.com/resources/customer-stories/trimet-bus-fleet-management-with-digi-connectivity>

⁸⁷ <https://www.digi.com/resources/customer-stories/digi-helps-septa-comply-with-federal-mandate>

orderly flow of traffic (See Carnegie Mellon Study for an example: <https://www.cmu.edu/piper/news/archives/2012/october/smart-signals.html>) as well as increased productivity (drivers spend less time stuck in traffic). Other personas may use these technologies to develop and operate innovative transportation services, such as those involving multimodal transit, ridesharing, and autonomous transportation of people and goods.

There also exist several barriers faced by personas seeking to implement these technologies. On the policy side clarity is needed with respect to data governance and privacy and what aspects of data jurisdictions can collect, retain, and subsequently use. Certain aspects of this sector still need high level policies and regulations that adequately address safety and liability concerns. The benefits of these technologies are not available in rural or underserved areas. Interoperability and fragmentation is also a challenge when dealing with different jurisdictions and it's important to address cybersecurity implications of all the connected devices that can be used as a gateways. Finally, there is a considerable amount of funding needed to drive adoption in this sector. The examples provided above reinforce that this technology is ready to go mainstream.

Finding: Healthcare. IoT is transforming healthcare and is poised to revolutionize it, but significant challenges need to be addressed.

The Internet of Things offers the potential to revolutionize healthcare by reshaping patient care, clinical workflows, and healthcare management. The integration of connected sensors, digital technologies, and data analytics creates a connected ecosystem of Internet of Medical Things (IoMT), medical devices, healthcare systems, and software applications that communicate with each other to streamline healthcare delivery, improve patient outcomes, and pave the way for a more efficient and patient-centric healthcare system.

IoMT devices range from wearable devices and remote patient monitoring solutions to smart medical implants. These IoMT devices encompass a vast network of smart, interconnected medical devices that collect, transmit, and analyze health data in real-time to enhance the quality of healthcare services and create a new era of personalized medicine.

IoMT devices fall into four categories:

1. Wearable on-body devices, including consumer health devices (fitness watches, sleep trackers, etc.), and clinical-grade devices (regulated by health agencies, and prescribed by healthcare professionals).

2. In-home devices that support telemedicine applications such as remote patient monitoring, and emergency response.
3. Community IoMT systems, such as emergency response intelligence systems that connect patients and first responders, mobility services, and devices for measurement and regulation of temperature, blood pressure, etc.
4. In-clinic IoMT systems that support administrative functions that allow medical workers to help patients remotely, track hospital assets and equipment, etc.

Some examples of top IoMT applications include:

- **Remote patient monitoring.** One of the most impactful applications of IoT in healthcare is the continuous monitoring of patients outside traditional healthcare settings. Wearable devices track vital signs, medication adherence, and other health metrics. This allows healthcare providers to monitor patients outside traditional clinical settings, providing timely interventions and reducing the need for frequent hospital visits. This is beneficial for individuals with chronic conditions, allowing healthcare providers to remotely track and manage patients' health, reducing hospital readmissions, and enhancing overall patient well-being.
- **Consumer health awareness.** Wearable devices, such as smartwatches and fitness trackers, have become ubiquitous. These devices play a pivotal role in promoting preventive care, tracking physical activity, monitoring sleep patterns, and even detecting early signs of health issues, fostering a proactive approach to well-being.
- **Enhanced patient care.** IoMT has propelled the development of smart medical devices, including insulin pumps, pacemakers, and continuous glucose monitors. These devices not only offer real-time monitoring but also enable healthcare professionals to adjust treatment plans based on individual patient data, leading to more personalized and effective care.
- **Asset and Inventory Management.** IoT plays a crucial role in optimizing hospital operations by monitoring the location and status of medical equipment and supplies. This ensures that resources are efficiently utilized, reduces waste, and enhances overall operational efficiency.

IoMT enables the following benefits, including:

- **Enhanced Patient Outcomes.** By enabling continuous monitoring and personalized care, IoMT contributes to improved patient outcomes. Timely access to health data allows for early detection of potential issues, better management of chronic conditions, and more proactive interventions.

- **Efficiency and Cost Savings.** The implementation of IoT in healthcare streamlines workflows, reduces manual tasks, and enhances the efficiency of healthcare delivery. This not only improves the quality of care but also contributes to cost savings by minimizing unnecessary hospitalizations, optimizing resource utilization and minimizing administrative costs.
- **Patient Engagement and Empowerment.** IoMT empowers patients to actively participate in their healthcare journey. Access to real-time health data through wearable devices fosters a sense of ownership and encourages individuals to make informed decisions about their lifestyles and treatment plans.

While IoMT offers the potential to revolutionize healthcare, there are some challenges, including:

- **Security and Privacy Concerns.** The vast amount of sensitive health data transmitted through IoT devices raises significant concerns about data security and patient privacy. Ensuring robust cybersecurity measures and compliance with privacy regulations is crucial.
- **Interoperability Issues.** The integration of diverse IoT devices and platforms poses challenges related to interoperability. Standardization efforts are essential to enable seamless communication between different systems, ensuring a cohesive and efficient healthcare ecosystem.
- **Regulatory Compliance.** The rapid pace of IoT development often outpaces regulatory frameworks, leading to challenges in ensuring compliance with healthcare regulations. Addressing these issues requires ongoing collaboration between technology developers, healthcare providers, and regulatory bodies.

The Internet of Medical Things holds immense promise for the healthcare industry, facilitating a future where patient care is personalized, efficient, and technologically advanced. However, to realize this promise, the healthcare industry ecosystem must evolve and adapt its practices, operations, policies and regulations.

Finding: Environmental Sustainability. IoT supports environmental sustainability through real-time monitoring, optimizing resource usage, and facilitating data-driven decision-making across infrastructure and multiple sectors of the economy.

IoT supports and facilitates environmental sustainability in a number of ways. IoT devices monitor environmental conditions, optimize usage of resources, and control operational processes. The data collected from IoT devices is analyzed and used to inform policymaking, enforce regulations and monitor progress and success of

programs and initiatives. In other cases, IoT technologies initiate actions and control operational processes that support sustainability outcomes.

IoT is used in a variety of applications to support environmental sustainability across all aspects of infrastructure and economy. Some examples of IoT applications for environmental sustainability include:

- **Monitor air quality.** Air quality sensors measure the concentration of pollutants in the air, including particulate matter (e.g., soot or black carbon), and gas pollutants (carbon monoxide, nitrogen dioxide, etc.). This information informs residents of a community whether to go outside exercise or not. The collected data may be used by city and health officials to identify areas of poor air quality, and to devise programs to mitigate its effects (such as planting trees in the area, restricting traffic at certain hours, banning idling cars at certain hours, providing residents with respiratory healthcare information, etc.).
- **Optimize water use.** Farming consumes a lot of water. Soil moisture sensors, integrated with automatic irrigation systems, measure moisture levels and activate the irrigation systems in those spots in the field where the water is needed. This helps save water (and the corresponding expenses) by precisely directing water to those spots where it is needed. This optimizes water usage by applying water it is most needed and reducing waste and conserving resources.
- **Reduce carbon emissions.** Intelligent traffic management systems, incorporating IoT sensors, detect heavy traffic conditions and automatically adjust traffic signals to reduce congestion. This increases the capacity of the street or freeway to handle more cars, while reducing the time cars are idling. The overall effect is a reduction in emissions and its impact on residents of the surrounding community.
- **Reduce energy use.** Buildings are one of the largest consumers of electricity. Room occupancy sensors turn off lights in empty rooms. Smart thermostats learn the behavior of building occupants and autonomously manage ambient temperatures based on those patterns. Automated demand response systems, connected to building automation and energy management systems, automatically reduce energy use by turning things off during peak demand periods while minimizing impact on building occupants.
- **Optimize use of renewable energy sources.** IoT optimizes and maximizes the use of renewable energy sources to power communities and cities. Smart inverters in solar power systems and sensors in batteries communicate with

the local electrical grid to continuously manage how much electricity is stored, discharged to the grid, and used to power loads in the home and business. This maximizes the ability of renewable energy systems to meet demand in the local grid, while delaying the use of upstream fossil fuel power generation plants to meet local community demand.

The use of IoT to support environmental sustainability offers the following benefits, including:

- **Improved and more effective outcomes.** The use of IoT enables the direct monitoring of the environment at the precise locations needed. The data collected can be used to improve and validate simulation models, and to predict likely trends and patterns. This foresight leads to more informed policies and strategies, which can then be implemented and monitored.
- **Increased resource use efficiency.** Analysis of the collected data provides insights that lead to optimization strategies. For example, a study of energy usage data helps identify patterns that may be adjusted. Automation systems may be programmed with these insights to optimize energy utilization, minimizing waste and enhancing efficiency.
- **Agile and proactive response.** Real-time monitoring of environmental conditions, such as water contamination and air quality levels, allow the community to plan and respond swiftly. This enhances the effectiveness of the response, the number of resources applied, and minimizes the extent of the adverse impacts.
- **Informed and data-driven decision making.** The vast amount of data collected by IoT devices enables informed decision-making for policymakers, businesses, and individuals in the pursuit of sustainability goals. This leads to more effective policies and strategies, more productive use of resources, and sustainable outcomes.

The use of IoT for environmental sustainability faces a number of challenges. These include:

- **Data accuracy.** Environmental monitoring is performed by many types of sensors. For example, air quality sensors range from low-cost sensors “consumer grade” to expensive regulatory grade units. Despite measuring the same things, these sensors have different accuracy levels due to the underlying sensing technologies used. Low-cost sensors would not be suitable for use in situations where environmental monitoring is used for verification of

compliance. In addition, sensors experience calibration issues, drift, or malfunctions, leading to inaccurate readings.

- **Lack of supporting infrastructure.** Environmental monitoring devices may be deployed in remote or rural areas with limited or unreliable network connectivity, affecting the real-time transmission of data. For example, many wildfires start in remote areas and early detection is critical to containing the impact. Many river monitoring stations are located upstream in remote areas. Ocean monitoring buoys are located in areas with no infrastructure. These remote areas have limited to no connectivity service, and hinders the ability to deploy IoT in these areas.
- **Initial Implementation Costs.** The upfront high costs of purchasing and deploying environmental monitoring sensors are a barrier for many agencies and communities. These costs are increased if a large network of sensors is needed. For example, in a city environment, air quality levels significantly. A street next to a freeway has poorer air quality than a street a mile away. In those applications where a dense network of sensors is needed, such as community air quality monitoring, the costs can be beyond the financial means of the purchasing agency. While low-cost sensors may alleviate the financial burden, they suffer from lower accuracy and will not meet regulatory standards.
- **Data management.** Environmental monitoring sensors collect a large volume of data over time. For example, some air quality sensors collect data every 15 minutes. During a storm, sensors monitoring rising river water levels during a storm collect data more frequently than when it is not raining. Managing this data is complex and challenging. This is complicated when sensor data from different brands is combined. These sensors have different accuracy levels, different measurement methods, and different methods for how the readings are calculated. Normalizing the data is laborious and time-consuming. This data must then be stored and maintained. The challenge is magnified as the volume of data collected grows.
- **Interoperability.** Environmental monitoring is a fragmented ecosystem of diverse devices and sensors, each designed with specific communication protocols and standards. This lack of standardization hinders seamless integration and data exchange between different IoT platforms and devices, limiting the holistic view required for comprehensive environmental monitoring. The lack of standardized communication protocols hinders the ability of environmental monitoring networks to expand and scale. Without standardized interfaces, scaling up becomes a cumbersome task, leading to increased complexity in managing and maintaining diverse systems. The

challenge is further exacerbated pronounced when attempting to create a unified system that aggregates data from various sources, such as air quality sensors, water quality monitors, and weather stations. Overcoming interoperability challenges is crucial for establishing a cohesive and interconnected network of environmental monitoring devices, enabling more accurate and comprehensive assessments of environmental conditions.

Finding: Public Safety. IoT can enhance and improve public safety outcomes, but must overcome a wide variety of technical, community and policy challenges, before it can be deployed and used at scale.

The Internet of Things offers the potential to increase public safety by enhancing the capabilities of public health systems, emergency response systems, law enforcement, and disaster management. The incorporation and integration of connected sensors, digital technologies and data analytics creates applications that improves monitoring and detection, response effectiveness, and recovery and resilience actions. Some examples of IoT applications for public safety include:

- **Smart Surveillance.** IoT-enabled surveillance cameras and sensors are deployed in public spaces to monitor and detect unusual activities or potential threats in real-time. For example, connected audio sensors detect the sound of gunshots or breaking glass, identify the location and notify police so they can respond faster. Smart cameras detect and report suspicious and unpermitted behaviors, such as unattended luggage or packages, trespassing into secure areas, lack of social distancing, or fighting, display of a gun and other illegal activities. These smart applications enable accurate monitoring and review of thousands of camera and sensor feeds autonomously with limited human involvement. In addition, when integrated with next-gen 911 systems, IoT systems provide dispatchers and first responders with relevant information and situational awareness for more effective deployment of resources and personnel.
- **Situational Awareness.** The use of IoT provides communities and responders with detailed information about existing and future events. For example, drones fly over active disaster areas to provide responders with a fast assessment of the scene to inform on deployment of resources and activities. Water level sensors monitor upstream river and stream levels to provide communities with knowledge of real-time conditions and enhance flood response, evacuation, and mitigation activities. Sensors that detect Wi-Fi signals from mobile phones allow first responders to know how many people are inside a building and where they are at. Air quality sensors monitor the pollution levels of communities, and inform public health officials of

intervention programs to mitigate respiratory illnesses. The use of IoT for situation awareness facilitates where to focus initial resources to save human lives.

- **Responder Monitoring.** Wearable IoT devices, such as body cameras, biometric monitors, and communication devices, enhance the capabilities and safety of first responders during operations. These IoT devices inform operations managers of responder stress levels, conditions of the surrounding environment and state of responder equipment. For example, sensors on oxygen tanks provide responders with a real-time estimate of the remaining time left, and takes into account responder exertion and stress levels. Body cameras on police provide a record of how officers respond to activities, document actions, hold officers accountable and provide a record of activities that is reviewed to improve future operations.
- **Connected patient monitoring.** Emergency response vehicles equipped with IoT devices monitor the health of the people being treated at accident or disaster scenes, as well as those critically injured transported by ambulances. This monitored patient information can be viewed in real time by Emergency Room doctors, who may instruct paramedics to apply additional measures to stabilize and treat patients before they reach the hospital. For the most critically injured, the additional information could mean the difference between life and death.

The use of IoT to support public safety activities offers the following benefits, including:

- **Improved Situational Awareness.** IoT devices provide real-time data, supplementing existing information. and enabling public safety agencies, first responders, disaster and resilience managers, and health officials to have a comprehensive and real time view of ongoing and developing situations. This improves decision-making and facilitates resource allocation during emergencies.
- **Increased Response Effectiveness.** Connected devices enable faster communication and response coordination. Emergency services can be dispatched more efficiently, reducing the time it takes to address critical situations.
- **Preventive and Predictive Capabilities.** IoT sensors enable the collection of data for predictive analytics. For example, information collected from gunshot detection sensors can be analyzed to predict when and where potential future incidents may occur. The police can anticipate potential risks and take

preventive measures like stationing more officers at the predicted times and locations, to reduce the likelihood of incidents.

- **Data-Driven Decision-Making.** The data collected from IoT complements existing and historical information and knowledge to inform and enhance decision-making. For example, air quality monitors identify areas of a city where poor air quality consistently exists. Using this knowledge, along with the correlation between increased death rates and air pollution,⁸⁸ public health officials can decide to target this area for information campaigns to prevent COVID-19 exposure, as well as to station medical resources for early intervention and treatment of COVID related illnesses.

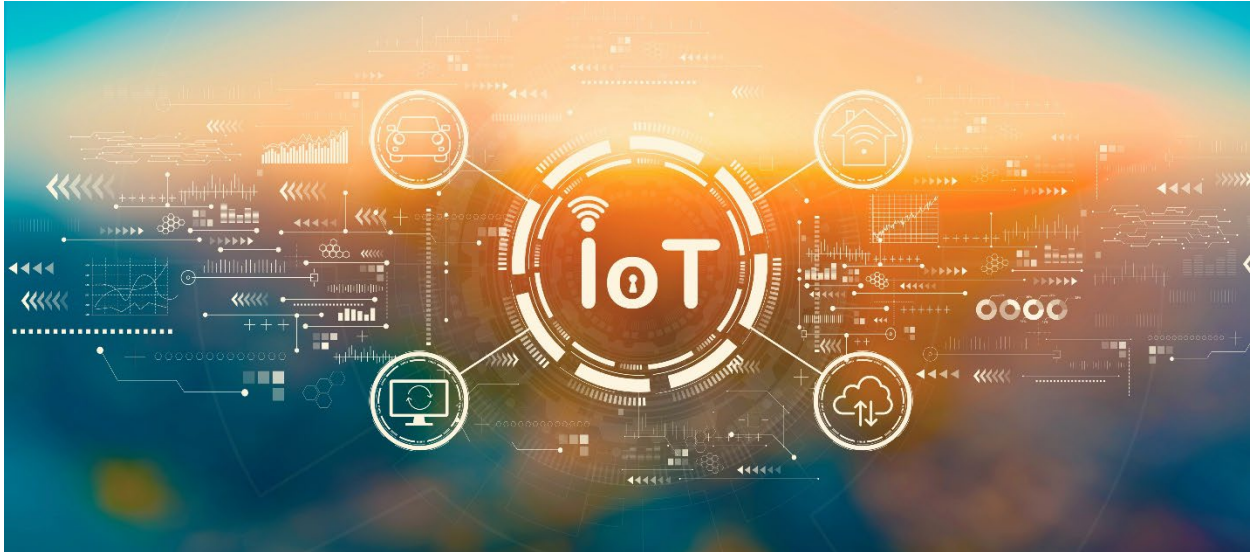
The use of IoT to support public safety actions faces a number of challenges, including:

- **Cybersecurity Concerns.** The use of connected devices leads to increased cybersecurity vulnerabilities and risks. Cybercriminals may use vulnerable devices to gain unauthorized entry into the systems used by law enforcement and other public agencies. This may result in access of sensitive information, and the operational compromise of public safety devices and systems.
- **Privacy Issues.** The extensive data collection capabilities of IoT devices raise privacy concerns. For example, traffic cameras may be used outside of its original and authorized scope to surveil private citizens. Cameras in public spaces may be equipped with facial recognition capabilities to identify people for detention. These concerns may lead to a lack of community support and ban of these technologies in the communities they serve. The use of IoT requires the development of policies and legislation that balance the benefits of data-driven public safety with individual privacy considerations.
- **Interoperability Challenges.** The IoT devices used to support public safety may face interoperability challenges in integrating and communicating with the various systems used by public safety agencies. This lack of interoperability makes it difficult for the various systems to share and process information in real time for operations, decision-making and situational awareness.
- **Scalability and Infrastructure.** Scaling IoT deployments to cover large geographic areas requires robust and modern infrastructure. This infrastructure must be scalable and interoperable to accommodate a growing number of future devices, and be reliable and critical for use under harsh

⁸⁸ Air pollution linked with higher COVID-19 death rates, <https://www.hsph.harvard.edu/news/hsph-in-the-news/air-pollution-linked-with-higher-covid-19-death-rates/>

conditions. It must cover remote areas, such as for wildfire detection or flood monitoring, where limited connectivity infrastructure currently exists.

- **Funding.** A lack of funding prevents public safety and public health agencies from procuring, deploying and operating IoT-enabled applications and systems. These systems may be costly, and limit agencies to what they can purchase. Traditional funding sources have been through a variety of agency funding vehicles, including grants, internal capital budgets, and capital improvement budgets. Other than grants, funding is based on agency priorities and availability, and can be subject to long procurement cycles.



Recommendations of the IoT Advisory Board

As the IoT Advisory Board (IoTAB) met repeatedly throughout the year, several topics and eventually themes surfaced repeatedly across the IoT landscape. The board's recommendations are organized around five major themes. These themes represent elements that are fundamental to facilitate, accelerate and sustain the adoption and integration of IoT into the American economy and society. These themes are:

1. Modernize IoT infrastructure
2. Establish and sustain trust in IoT
3. Secure the IoT supply chain
4. Government facilitates industry adoption
5. Foster a IoT ready workforce

The IoTAB recommends that the IoTFWG consider (and where appropriate, act to implement or document the existing implementation of) 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.

[Ed. Note: When the recommendations are mostly stable, we will place a table here as a quick reference, with hyperlinks to each recommendation.]

[Note to Reviewers: There has been debate about how to frame whom the recommendations are directed to. In the previous edition, with a few exceptions, we were general, as in "The government should ...". Dan and some others have pointed out that this report is to Congress and that recommendations should be more specifically addressed. Your input on that is needed since it will affect each item.]

Establishing a National IoT Strategy

Objective 1: Congress and the White House must work together to create and implement a coherent comprehensive coordinated national IoT strategy, as numerous federal experts have suggested over the years.

Key Recommendation 1.1: The IoTAB recommends a strategic national approach for taking full advantage of the opportunity presented by the IoT.

In 2010, the President’s Council of Advisors on Science and Technology (PCAST) recommended the Federal Government invest in a national, long-term, multi-agency, multi-faceted research initiative in these areas.⁸⁹ They said, “those agencies tackling problems whose solutions entail instrumenting the physical world ... should conduct research to design, fabricate, and test sensors that are problem-domain specific and that are cheaper, smaller, better packaged, lower powered, and more autonomous than those available today.”

In 2011, an OSTP/NSTC White Paper outlined many reasons why we needed a more comprehensive and strategic approach for taking advantage of the Cyber Physical System (IoT) opportunities over the horizon to grow our economy and help solve our national challenges.⁹⁰ They found that “Isolated efforts by mission agencies are simply not sufficient to address the underlying issues in a holistic manner.” Trying to address ~~them~~ such issues agency-by-agency or sector-by-sector would result in inefficiencies and insufficient progress relative to system development timetables, and we might never get to where we need to be, and the recommended the creation of a long-range action plan.

They went on to say, “Without a strong, central focus on innovation and the common issues in translational research for innovation in cyber-physical systems, including standardization, manufacture, and deployment, each of the jump start activities above runs the risk of devolving into an isolated, marginally-effective effort.”

Likewise, a NITRD Report from 2012 that looked at opportunity in Agriculture, smart building, defense, emergency response, energy healthcare, manufacturing and transportation, advocated for a multi-agency, multi-sector comprehensive focus on the difficult crosscutting R&D challenges in CPS.⁹¹

⁸⁹ The 2010 PCAST report is available from: <https://www.nitrd.gov/pubs/PCAST-NITRD-report-2010.pdf>

⁹⁰ The OSTP/NSTC white paper is available from: <https://www.nitrd.gov/pubs/CPS-OSTP-Response-Winning-The-Future.pdf>

⁹¹ The 2012 NITRD report is available from: https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

As shown in the earlier section [The Current State of IoT](#), these predictions from 2011 and 2012 were accurate, and the lack of a national strategy has impacted growth. And ~~now yet~~ today, the IoT opportunities are even more pervasive, the economic stakes even more enormous, and the impacts are even more profound. In other words, it is not too late.

We need a comprehensive national IoT strategy that:

- describes a comprehensive vision for the federal government's role in IoT;
- articulates the role that IOT can play across sectors and agencies, and within sectors, in advancing national priorities and solving social challenges – across health, transportation, manufacturing, energy etc.;
- ensures continued U.S. leadership in connected device technologies, a vibrant and innovative commercial sector, and U.S. leadership in the way the technologies are harnessed to address national challenges;
- comprehensively catalogues the game changing work the administration is already doing across many agencies in fundamental research, development, demonstration and deployments – and the important role agencies are playing in meeting our critical needs;
- identifies potential opportunities, and synergies across agencies, and identifies remaining gaps; and,
- outlines an R&D roadmap around the often multi-disciplinary R&D needs to push new frontiers and achieve major grand challenges.

For example, there is a high risk-to-reward ratio for research into new and advanced sensors for viewing and detecting environmental conditions. Such devices could unlock new IoT potential across many domains. The research could help ensure the continued responsible development and use of new technologies and enable those interested (i.e., agencies, innovators, scientists, stakeholders, and commercial partners) to see and engage with the effort. Like nano.gov, quantum.gov, and ai.gov, stakeholders could also benefit from a one stop shop on the internet (e.g., **iot.gov**) that would share the strategy and vision, demonstrate the many ways the government is tackling these issues, and that allows stakeholders to engage in meaningful ways.

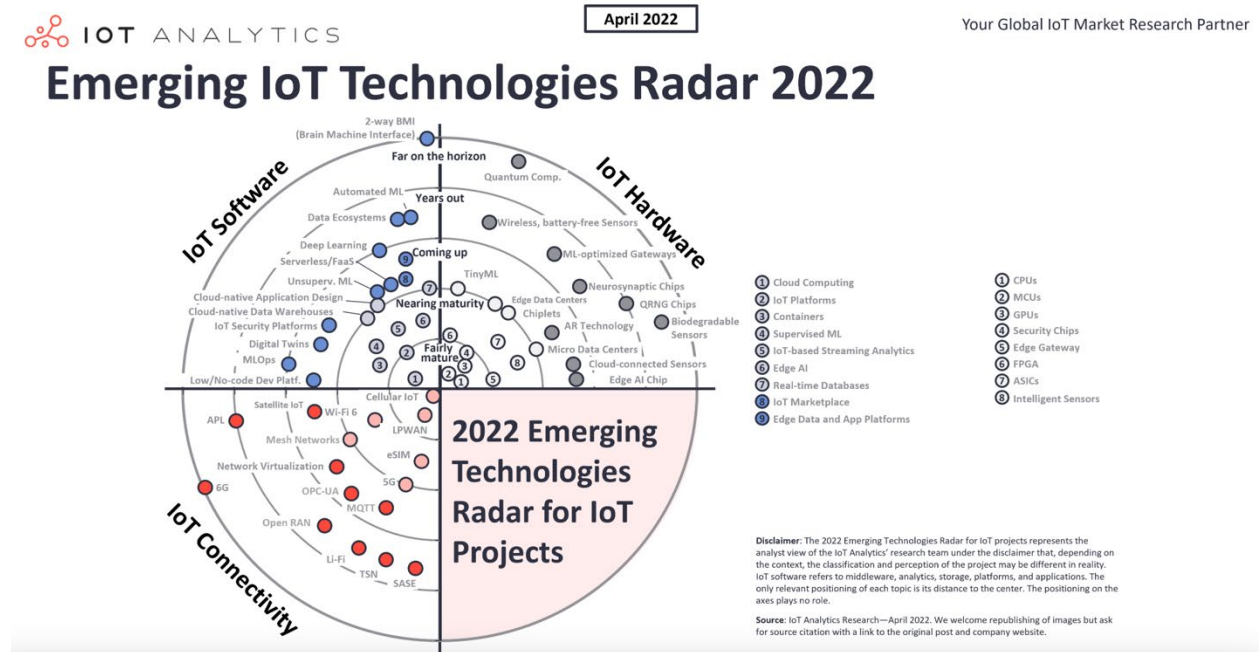
[Editors Note: Add items from Smart City strategy recommendation from Benson]

Enabling Recommendation 1.1.1: IoT must be added back to the critical and emerging technology list.

The U.S. National Standards Strategy focuses on emerging technologies, yet the IOT is no longer included in the list of critical emerging technologies <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and->

[Emerging-Technologies-List-Update.pdf](#). This as a problem since the IoT is critical to U.S. prosperity and socioeconomic success and still faces many barriers to adoption. The IoT must be added back to the CET to ensure that the government remains aware of new opportunities to apply IoT and ensure adequate oversight.

In addition, IoT is an evolving set of disparate technologies at various levels of maturity. While some are mainstream and mature, others are emerging and immature.



Source: <https://iot-analytics.com/iot-technologies/>

Technologies such as cloud computing, IoT platforms, containers, supervised machine learning, IoT streaming analytics, cellular IoT and Low Power Wide Area Networks (LPWAN) have reached maturity.⁹² Others are “coming up”, including edge data and app platforms, serverless/Function-as-a-Service, cloud-connected sensors, edge AI chips, and low code/no code development platforms and satellite IoT connectivity.⁹³ Still others like data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, QRNG chips, biodegradable sensors, 6G and quantum computing are still “years out” and require continued research investments.⁹⁴

⁹² “55+ emerging IoT technologies you should have on your radar (2022 update),” S. Sinha, IoT Analytics, April 6, 2022.

⁹³ [Link](#)

⁹³ *ibid.*

⁹⁴ *ibid.*

Enabling Recommendation 1.1.2: Congress should further improve and elevate inter-agency coordination.

Within the White House, the National Science and Technology Committee (NSTC) conducts research coordination across the federal government. For more than a decade, there was a Cyber-Physical System (CPS) Inter-Agency Working Group, which has made some important contributions and recommendations to advance IoT fields. But in 2019, its focus was diluted. It is important to ensure there is an NSTC IoT committee that is properly named, elevated, and empowered, just like other NSTC committees focused on AI, Quantum and Nanotechnology. This is particularly important as formerly separate disciplines of AI, Quantum and IoT begin to converge. It's also critical that an approach must be inclusive of IoT and the many different names and enablers.

The U.S. should lead in the adoption and integration of emerging technologies like the IoT into the U.S. economy and infrastructure. Currently a lack of coordination from the Executive Office of the President leads to siloed planning, policies, execution, suboptimal utilization of resources, duplicate programs, monitoring, thus limiting realization of economic, social, security and other values and benefits.

Congress should expand the mission of OSTP for additional focus on the IoT as identified by the National Standards Strategy of May 2023 or similar curated list, with additional staffing support as required for the expanded mission. OSTP has historically played a critical role in coordinating such inter-agency endeavors.

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

The list of Critical and Emerging Technologies (CET) is broad (AI, IoT, quantum, etc.) and some agencies may have some existing CET interagency roles. Having OSTP in a leadership role, potentially convening interagency efforts, FACAs or other whole-of-government or public-private activities, will help steer government and private sector activities.

Congress should create and fund a new National Coordination Office for IOT/CPS for advancing this strategy, like it has in the areas of Nanotechnology, Quantum, and AI, then in doing so it should also ensure that OSTP is fully resourced and funded to be able to take on these task – or risk losing focus on other critical needs.

Enabling Recommendation 1.1.3: Congress should monitor and track the progress toward the implementation of the IoT national strategy.

This is placeholder for the pending recommendations to be provided for a series of related sub-recommendations:

- Define key outcomes of the IoT national strategy and initiatives to accomplish those outcomes
- Track and report on the key metrics, and the progress of implementation of key recommendations and initiatives
- Report on initiatives and progress on iot.gov

Modernizing IoT Infrastructure

Objective 2: The U.S. should call upon and collaborate with industry to enhance and modernize the infrastructure that enables and supports IoT. Such collaboration should include the provision of clear direction and support for data sharing methods and repositories, consistent and resilient ways for interoperable communications among devices, update of legacy computing and networking systems, and improved means to connect among devices and interconnect with existing technologies.

There are four critical aspects to modernizing and expanding this infrastructure:

- Data Sharing,
- Consistent and Resilient Interoperability and,
- Updating of legacy computing and networking systems
- Enhanced Connectivity.

The U.S. Government should call for immediate attention to these needs, as it has done for other topics through strategic objectives and planning. In particular, NIST may be able to support the development of outcome-based objectives that inform industry consensus standards and may be able to offer assistance as industry collaborates and develops those standards. That partnership may also help support international success in expanding and improving IoT infrastructure and reliability.

Equitable and Responsible Data Sharing

Key Recommendation 2.1: The government should foster policies that encourage responsible and equitable sharing of IoT data and thereby drive economic growth, societal benefits, and sustainability.

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

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

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

Implementation considerations: Implementation of this recommendation would include programs to promote the necessary infrastructure for data security and

privacy, including aspects of data sharing, licensing, ownership, analytics, control, and monetization. Agencies would need to establish and maintain data policies that ensure compliance with regulatory requirements, in consultation with industry, academia, and government agencies.

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

Enabling Recommendation 2.1.1: The government should establish templates or best practices for clear and robust corporate policies regarding data sharing, usage, and licensing among parties in the IoT ecosystem.

Where practical, agencies can help foster voluntary, industry-led adoption of such policies to enhance transparency, reliability, and consistency in applying IoT. These types of ~~templates and policies~~ best practices are vital due to the significant data protection risks presented by IoT's increased interconnectivity and data-sharing capabilities. The government should establish templates for non-sensitive data collected by federal IoT systems (air quality, water monitoring, etc). Since these risks may discourage IoT adoption, clear corporate policies safeguarding users' personal data and ensuring transparency would foster trust and expanded IoT use.

Implementation considerations: The government should create guidelines on effectively communicating data sharing and data use in relevant corporate policies, in alignment with other recommendations from this report. Those guidelines and policies would be supported by public awareness campaigns to educate users about their expectations for the use of data ~~data rights~~ and to share information about how to properly share and protect IoT data.

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

Enabling Recommendation 2.1.2: The government should partner with industry and collaborate with international allies to develop and support comprehensive data sharing policies that stimulate economic growth, societal benefits, and sustainability.

As digital threads drive growth of data among marketplaces, the growth of IoT continues to drive the growth of data availability, policies will be needed regarding data confidentiality, ownership, control, management, access, licensing, and trust for data use in applications, to minimize security risks and maximize economic value.

Monetization of data will require infrastructure for security, privacy, data sharing, ownership plus control frameworks for identity and access management (IAM), data protection, sharing and exchange, data analytics and AI, to minimize supply chain risk and maximize economic value. Policies related to data can have a major impact as they can fuel synergistic ecosystems and the future digital economies.

A lack of clear and consistent data policies can create uncertainty and hinder the growth of digital economies. The right data strategy can drive business growth and fuel synergistic ecosystems. Policy guidance from the government will support the infrastructure required for data sharing (i.e., for security, control, trust, licensing, identity & access management (IAM), and analytics), and will also help support consistent protections, such as anonymization of collected data (an essential element of privacy, safety initiatives, and other risk management considerations).

Implementation Considerations: The government should work with industry to help establish model policies related to trusted data, including identification of areas that are critical or sensitive enough that regulatory oversight might be necessary. That process can include methods for promoting essential requirements and guidelines (such as for data privacy, confidentiality, and anonymization) and define methods for how stakeholders (e.g., industry, academia, civil society, and government agencies) might evolve the policies to keep them up to date with changing technologies and business models.

As the government works with partners to create policies that promote interoperability and data sharing across different systems and corporations, the resulting efficiency may be particularly helpful for SMBs.

Potential Implementation Barriers: As these new policies are drafted and released, the lack of familiarity with them, and any lack of clarity about how the data policies will impact stakeholders, might cause some uncertainty and, thereby, hinder the adoption by businesses and workers as well as the growth of digital economies.

The cost of establishing infrastructure for data security, privacy, sharing, and exchange, as well as data analytics with AI, may be significant, though the benefits may prove the investment worthwhile.

Enabling Recommendation 2.1.3: The government should establish data repositories for privately collected data.

The growth of the Internet is directly traceable to the fact that large amounts of data can be efficiently and responsibly stored, enabling significant exploration to gain insights into a myriad of information types. For more than a decade, the U.S. Government has recognized that data is a key asset that can provide valuable benefits to its citizens and other stakeholders. As with many existing datasets, there is an opportunity for the Government to help create and maintain repositories for IoT data, ensuring transparency and availability.

The growth in IoT devices portends a rapid deployment of devices. IoT devices generate large amounts of data, some of which is likely to include information that may be openly shared with a broad constituency, as many thousands of existing open datasets do. There is value in helping to establish private data stores that can be licensed for particular consumer segments, bringing value to those who operate some types of IoT devices (accelerating adoption) and supporting availability of important information to those who would consume the information produced.

Federal data repositories provide transparency and the opportunity to empower community research to conduct analysis on the data far beyond the capabilities of a single federal agency. The government should support and facilitate industry efforts to create these data repositories for the purpose of collecting public data such as a common societal good like weather or environmental data (e.g., air quality, water level, etc.). In this way, the government can use non-sensitive federal open data as a basis for the community research and analysis to determine the right level of deployment for IoT devices. These devices have the potential to provide a strong public good, however without transparency, privacy and data ownership issues may arise. Additionally, the use of different technologies and methodologies across different platforms may result in conflicting measurements, fostering misinterpretation and reducing public confidence in the monitoring process.

Implementation Considerations: There are existing examples where the federal government has provided a clearinghouse for raw data and other information. For example, the Department of Energy's EIA sharing of power plant data may provide a template and lessons learned for similar sharing.

Consistent and Resilient Interoperability

Key Recommendation 2.3: The government should establish methods to foster interoperability for IoT technology, including through the use of consistent models, protocols, application interfaces, and schemas.

While the Internet of Things and related technologies have made significant advancements in recent years, much of that work has been focused on the devices themselves with less focus on the interoperability, compatibility, and connectivity that converts these discrete “things” into an “Internet of Things”. In some cases, while manufacturers have provided reliable interoperability within their own product line, improved interaction among a broad range of devices from disparate producers will encourage competition and technology availability, thereby increasing adoption by enterprises and consumers.

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

A model of industry-led interoperability in another space—not IoT, but streaming media—is the WAVE Project hosted by the Consumer Technology Association. This program has participation from major streaming media services, major smart TV and device hardware manufacturers, and other necessary ecosystem entities. The goal is to foster interoperability between the streaming media and the hardware playback—that is, from one’s favorite video streamer to one’s smart TV, media stick or set-top box. The WAVE Project convenes most of the major players in these categories. The subject matter experts from each company work not to make new standards, but to ensure consistent application of existing accepted industry standards. By constraining the many options in the standards to a few and creating test suites to test for conformance to those constraints, the WAVE Project helps all of these organizations’ products to “speak the same language”. [ref. <https://CTA.tech/WAVE>]

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

Before the government can foster specific standards, it may be helpful for one or more agencies to perform a survey of available and relevant standards, protocols, and models. Due to the differences in sub-sectors, each such effort must be constrained to a specific application space, such as smart home or IoMT. 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 taxonomy or set of applicable models will promote industry adoption and foster standardization.

Enabling Recommendation 2.3.1: The government should work with various organizations to facilitate interoperability through the development of a consistent data taxonomy for the sharing and exchange of traffic and other data collected from IoT and non-IoT sources.

Transportation and traffic agencies have a limited ability to share and exchange data. Transportation data includes things like geographic information, asset and infrastructure information, traffic mobility history, public transportation performance, and traffic anomalies. At best, these exchanges may happen on a limited basis within each agency, but not across other agencies in other jurisdictions. This makes collaboration requiring multiple agencies difficult.

Once a taxonomy is established, government and industry can partner to develop conformance review criteria and methodology, further facilitating the reliable and consistent exchange of information.

Implementation considerations: Projects involving multiple jurisdictions and requiring federal funding should specify the development of a data taxonomy that can be further used and developed by other jurisdictions. It’s also important to engage with AASHTO as they are a standards setting body which publishes specifications, test protocols, and guidelines, that are used in highway design and construction.

Enabling Recommendation 2.3.2: The government should support research and industry-led standards in areas such as telematics and sensor technologies for autonomous vehicles.

These standards should be based on high-level safety guidelines (perhaps as determined by the National Highway Traffic Safety Administration or another federal organization).

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

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

High-level safety guidelines will need to be finalized by the National Highway Traffic Safety Administration as there are still open liability questions particularly regarding a determination of fault in the event of an accident. Spurred by these guidelines, industry can develop appropriate performance and safety standards in a market that is still emerging while avoiding the possibility of market fragmentation. It's important that all key stakeholders in the autonomous vehicle ecosystem participate in these safety discussions and standards development activities.

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

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

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

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

The existing UNECE regulatory framework for automotive security⁹⁵ is not a U.S. regulatory requirement, but it is in force in over 50 countries, making the cybersecurity requirements of WP.29 a de facto global standard. Since automakers already conform to these regulatory requirements in other areas, significant consideration should be given to avoid unnecessary overlap or redundancy.

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

For industry members to develop and implement protocols it is resource-intensive, requiring significant investments in time, money, and expertise. High-level guidance is needed from applicable government agencies to set the safety requirements for autonomous vehicles. The board notes there is still an open issue of liability concerns that needs resolution. There are also public concerns that warrant the need for consumer education on autonomous vehicle technology.

⁹⁵ <https://unece.org/wp29-introduction>

Enabling Recommendation 2.3.3: The government should promote and adopt industry led standards, guidelines, and protocols for minimum baseline interoperability for smart transportation technologies and corresponding transportation infrastructure (i.e., sensors in roads, cameras at intersections).

Industry standards and protocols ensure that devices from different manufacturers can communicate and work together seamlessly. In particular, smart transportation systems focus on safety, so standardization (especially for security and interoperability needs) is vital to ensuring that devices can communicate basic safety information to other vehicles and to/from infrastructure.

There are also cases where baseline standards, guidelines and protocols can address existing market fragmentation scenarios particularly in the global market. Some examples are provided below.

- ITxPT (Information Technology for Public Transport) is an international association with the mission to enable interoperability between IT systems in Public Transport by offering public specification of an IT architecture based on standards with open interfaces for on-board, over-the-air and back-office IT systems. By sharing standardized communication technology solutions, public transportation systems in different cities and regions can achieve interoperability, provide better passenger experience, and manage the transportation system more efficiently. Industry benefits as well, as vehicle manufacturers and integrators gain efficiencies with interoperability to reduce cost and accelerate innovation and enable better access to the global transit market. ITxPT has a growing international base of support, driven by its international members and by transit agencies around the world eager to deploy smart systems based on open standards and not proprietary solutions. If its adoption is delayed in the USA, the transit industry could lose competitive advantage in an increasingly global market.
- Positive Train Control (PTC). There are numerous PTC systems deployed in North America, with varying features and capabilities though all designed and proven to prevent train accidents. Where train operators share tracks, especially when a mix of passenger and freight rail, multiple PTC systems are installed on rail vehicles. The 3GPP consortium has targeted certain use cases for core support within 5G, including public safety, connected vehicle and train control. In collaboration with International Union of Railways (UIC), 5G is supporting the requirements of the Future Railway Mobile Communication System (FRMCS), of which the main goal is to fully digitalize railway operations, support an increasing level of automatic train operations, and take advantage of the broader capabilities of 5G for passenger travel as well. Train control based on FRMCS has a growing international base of

support. If adoption is delayed in the USA, the rail industry could lose competitive advantage in an increasingly global market.

There must be a way to address cybersecurity risks such that industry standards that describe minimum cybersecurity requirements of relevant technologies (will help to provide implementing agencies some level of assurance that these risks are mitigated. An example for this is having a unique set of keys for traffic controller cabinets (See the NEMA Standard: Cyber and Physical Security for Intelligent Transportation Systems: <https://www.nema.org/standards/view/Cyber-and-Physical-Security-for-Intelligent-Transportation-Systems-ITS>)

Standards and protocols can set a path forward for subsequent government regulations or policies and are particularly relevant if industry led standards are attempting to address known gaps and market fragmentation issues. This is particularly important when dealing with multiple states and local jurisdictions.

Standards can stimulate innovation and competition by providing a level playing field for businesses and developers as well, regardless of their size or market share. With a level baseline achieved via a multi-stakeholder process, companies can now build upon it and tailor their own solutions. Standardization can lead to cost savings for businesses by reducing the need for customized solutions and simplifying the procurement process.

Potential barriers: Cybersecurity threats are constantly evolving, so standards and guidelines could be outdated rather quickly. There is concern about protecting an organization's intellectual property (IP) whereas some organizations may have their own IP different from what's described in a baseline standard and not want to participate in activities that would deviate or reveal their IP. Therefore, it may be beneficial for the standard to propose a reference implementation baseline. Companies are then free to build upon it with their own IP, which can then help to differentiate the organization in the market. There are also cost and resource constraints to developing and implementing industry standards.

Enabling Recommendation 2.3.4: The government should facilitate and support the adoption of smart city and sustainable infrastructure standards.

Smart city infrastructure relies upon IoT technology to consistently operate. The IoT Advisory Board recommends that the Working Group address funding and implementation considerations for smart cities. For example, municipalities may not have the budget to modernize IoT solutions that better integrate with those in other

cities. Therefore, the government may need to develop creative solutions to help local, regional, and state entities to future proof their infrastructure.

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

Enabling recommendation 2.3.5: The government should promote development and adoption procedures that accelerate and streamline planning, permitting, and interconnection aspects related to energy efficient technologies within the broader electric grid.

The U.S. could benefit from improvements in decarbonization and reduction of greenhouse gas emissions. Many of the energy efficient technologies today incorporate the use of IoT (smart inverters, energy storage systems, etc.). There are improvements to be made in the deployment, permitting, and interconnection processes. Improvements to deployment of critical electric transmission to move electric power from location constrained renewables. Improvements to the installation and operation of rooftop solar panels for the permitting and interconnection process.

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

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

Promoting Existing Methods

Key Recommendation 2.4: The government should promote collaborative development across industries to adopt existing industry standards and protocols.

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

adopted. The Board did not identify any single protocol that will solve the interoperability issues, since these models tend to application or domain specific. Therefore, the Board highly recommends not to mandate any formal or informal standard or protocol, but rather to encourage voluntary conformance in the interest of improved interoperability.

Enabling Recommendation 2.4.1: The government should promote the collaborative development and adoption of existing industry standards activities with respect to energy efficient, clean, and renewable energy technologies that are used in sustainable infrastructure.

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

Implementation considerations: Implementation efforts will benefit from encouraging inclusiveness, prioritizing identified gaps, and building on existing standards. Proponents must encourage flexibility and adaptability in order to promote global adoption and collaboration.

Potential barriers: Achieving consensus among stakeholders may be time consuming and resource-intensive. As technology advances, international harmonization may create more complexity and time, fragmentation may exist, and some entities may not all agree on standards adoption.

Enabling Recommendation 2.4.2: The government should advocate for the implementation and adoption of interoperable data standards for public safety IoT.

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

Implementation considerations: Compiling guidelines and best practices for entities from what currently exists as a starting point (e.g., NISTIR 8255: Interoperability Real-

Time Public Safety Data, CISA SAFECOM Interoperability Continuum, etc.), prioritizing solutions which adhere to interoperability guidelines in government contracts for public safety IoT (e.g., bulk purchase pricing a la General Services Administration (GSA) catalog). From a high level, the consideration of tax incentives that would encourage companies to implement public safety IoT with interoperable data standards and the education and promotion of interoperable data guidelines for public safety IoT across different jurisdictions (e.g., local and regional).

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

Enabling Recommendation 2.4.3: The government should 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.

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

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

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

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

Enabling Recommendation 2.4.4: The government should promote the development and use of standards for supply chain logistics, traceability, and assurance.

The federal government should foster the development, adoption, and use of standards and protocols for supply chain logistics, traceability, and assurance. It should collaborate with Standards Development Organizations (SDOs) and international allies to promote assured & traceable products by manufacturers for efficient, reliable, and secure supply of goods. It should incentivize suppliers to establish unique corporate IDs, product IDs, asset IDs, and part IDs linked to a digital thread of information and data, that are used to track and trace goods while improving supply chain efficiency, transparency, resilience, and security. There is value in encouraging the use of Global Identifier Standards (such as GLS or GSI) in procurement contracts and regulatory frameworks and track goods and info related to assets and data, to optimize risk, cost, benefits, and value.

The federal government should offer financial and technical support to businesses, particularly small and medium-sized enterprises, to help them adopt and comply with the established standards and protocols. There should be mechanisms to monitor and evaluate the effectiveness of the standards and protocols over time and adjust as needed to address emerging challenges and opportunities. Additionally, the federal government should also support industry-led initiatives and education campaigns to foster the development and adoption of IoT standards and protocols for supply chain management, traceability, and enablement of economic value. These standards should best enable interoperability, reliability, and security across IoT-enhanced supply chains, facilitating data exchange, decision-making and services. By creating and promoting such standards, the government can drive widespread adoption of IoT technology, minimize supply chain risk, and maximize economic value to businesses and users.

Implementation Considerations: Encourage inclusiveness from a diverse range of stakeholders. Prioritize critical areas of supply chain management where standardization can yield significant benefits (i.e., data exchange, device interoperability, security, and privacy). Build on existing standards as a starting point and adapt/expand as necessary and identify where gaps exist to create new standards. Design standards and protocols that can accommodate new technologies, emerging threats, and evolving industry needs. Promote adoption to incentivize businesses. Develop mechanisms to monitor and enforce compliance to standards. Foster global collaboration to incentivize suppliers. Promote use of unique identifiers across the supply chain. Facilitate the adoption of identifiers through incentives, education, and outreach programs and promote linking Identifiers to IoT cybersecurity labeling programs for different markets. Create incentives to upgrade

existing supply chain management systems to include global identifier standards that ensure seamless tracking and tracing.

Potential Barriers: Resistance to standardization due to potential loss of competitive advantage, customization capabilities, or intellectual property rights. Fragmentation challenges across supply chains with different ecosystem stakeholders. Cost and resource constraints. Rapid technological advancements make it difficult to keep standards and protocols up-to-date and relevant (and growth of AI will potentially make it even more complex). Technical implementation challenges by stakeholders who may view implementation of identifier infrastructure as resource intensive (e.g., time, money, and expertise). International harmonization challenges and creating a secure and reliable database to manage the identifiers and share across borders.

Enabling Recommendation 2.4.5: The government should promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across various IoT systems and devices.

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

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

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

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

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

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

Connectivity

Key Recommendation 2.5: The federal government should expand and improve programs that ensure availability, reliable and sufficient connectivity among and between IoT devices in all areas of the country.

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

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

Additionally, enabling recommendations found elsewhere in this report that support sector specific examples of connectivity include:

- Under Agriculture –

- 5.4.5: The government should facilitate development of connectivity policies and programs.
- Under Environmental Monitoring –
 - 5.11.3: The government should facilitate the expansion of wireless connectivity to support remote monitoring and sensing in areas not serviced by traditional connectivity.

Enabling Recommendation 2.5.1: To promote continued U.S. leadership on spectrum policy, the government should continue to make licensed and unlicensed spectrum available, such as through spectrum sharing and repurposing underutilized federal spectrum.

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

As has been noted, IoT applications are expanding and continued growth is expected.⁹⁶ The technology industry uses both licensed and unlicensed spectrum to enable this growth. Spectrum availability should not become a choke point in this growth.

- Licensed spectrum usage through 5G (discussion of 5G)
- Whereas unlicensed spectrum typically (discussion of unlicensed) ...
- A comprehensive report on U.S. unlicensed spectrum usage is available from <https://shop.cta.tech/collections/research/products/unlicensed-spectrum-and-the-us-economy-quantifying-the-market-size-and-diversity-of-unlicensed-devices>

Enabling Recommendation 2.5.2: The government should consider increasing funding and accelerating implementation of broadband deployment across rural America.

A recent U.S. Department of Agriculture (USDA) report identified that 60% of U.S. farmland doesn't have good internet connectivity. While innovative solutions have expanded in recent years, point to point solutions and satellite-based connectivity

⁹⁶ *Op cit* the prior background discussion on billions of IoT devices in coming years.

quickly become expensive and do not resolve all issues. For example, it can be difficult to maintain connectivity to all areas of a farm.

One way to address this might be for the federal government to consider using its property to place broadband communications networks or towers. For example, there is a US Postal facility in almost every community. Its facilities can be used to house wireless broadband antennas (it could also be subleased to private operators). Similarly, the Bureau of Land Management and the National Park Service own federal land with access that could be granted for equipment placement.

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

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

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

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

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

Enabling Recommendation 2.5.3: The government should actively promote and support the adoption of satellite narrowband IoT systems, with the aim of improving connectivity, data collection, and decision-making in rural and remote areas, resulting in economic growth.

Satellite IoT systems provide a reliable and efficient means of connectivity and data transfer in remote agricultural areas where traditional terrestrial connectivity options may be limited or unavailable. Encouraging the adoption of satellite IoT systems will

enable farmers to optimize their operations through real-time data management, resulting in benefits for various stakeholders, including farmers, policymakers, agricultural companies, and consumers.

Encouraging the adoption of satellite IoT systems will enable adopters such as farmers, those monitoring infrastructure (e.g., powerlines, river levels), or rural remote patient monitoring to optimize their operations through real-time data management, resulting in benefits for various stakeholders, including farmers, policymakers, agricultural companies, utility companies, medical personnel, and consumers.

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

Implementation Considerations:

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

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

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

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

The role of states should be clearly defined, and funding for satellite IoT infrastructure and adoption may be allocated to states to manage and distribute. Incentives or subsidies for satellite IoT adoption and integration could be considered as part of the upcoming Farm Bill or other relevant legislation. There might be international

coordination, along with spectrum considerations with the International Telecommunications Union (ITU).

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

Establish Trust in IoT

Objective 3: The U.S. has an opportunity to build more trust and confidence in IoT. IoT provides powerful benefits but reaping those benefits, at times, requires placing sensors and devices in physical locations that can be highly sensitive and intrusive. While IoT promises exciting innovation and advancement opportunities, trust in the technology (and in the protection of associated data) by industrial adopters and other stakeholders is a key prerequisite. Trust considerations directly influence IoT adoption, including IoT safety, reliability, and ability to protect sensitive information stored and processed.

Cybersecurity Improvement

Key Recommendation 3.1: The Federal Government should provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach.

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.

Enabling Recommendation 3.1.1: The government should strengthen cybersecurity measures focused on IoT across supply chain networks to address concerns around data privacy, security, confidentiality, trust, and potential risks associated with increased connectivity and interdependence of IoT systems.

The recommendation to strengthen cybersecurity measures focused on IoT across supply chain networks aims to address the growing concerns around data privacy, security, and the potential risks associated with the increased connectivity and interdependence of IoT systems. While many manufacturers have adopted best practices, many more have not. By implementing robust cybersecurity measures, the government can help ensure that businesses can confidently adopt IoT technologies

in their supply chain operations without compromising the security and integrity of their networks and data.

Strengthening cybersecurity measures involves promoting the development and adoption of security best practices, guidelines, and standards specifically tailored to IoT systems in supply chain management. This includes securing data transmission, storage, and access, as well as protecting IoT devices and networks from unauthorized access, manipulation, and cyberattacks.

To implement this recommendation, the government should collaborate with industry stakeholders, cybersecurity experts, and technology providers to identify potential vulnerabilities and develop appropriate solutions that address the unique security challenges associated with IoT systems in supply chain operations. For example, the emerging U.S. Cyber Trust Mark program is proving to be a model of public-private cooperation, Administration leadership and agency execution. Additionally, the government should support research and development efforts aimed at advancing cybersecurity technologies and solutions tailored for IoT environments.

Training and awareness programs should also be promoted to ensure that businesses and professionals understand the importance of IoT security and are equipped with the knowledge and skills required to protect their systems and data. By strengthening cybersecurity measures focused on IoT across supply chain networks, the government can foster trust in IoT technologies and enable businesses to fully leverage their potential benefits while minimizing risks.

Implementation Considerations:

Implementation considerations for strengthening cybersecurity measures include:

1. Promote the adoption of best practices and standards: The government can encourage organizations to adopt industry best practices and internationally recognized standards such as the NIST Cybersecurity Framework and the ISO/IEC 27000 series. The Department of Commerce's National Institute of Standards and Technology (NIST) could play a pivotal role in this process, offering guidance and resources to streamline adoption.
2. Encourage information sharing: Facilitating the sharing of threat intelligence, vulnerabilities, and best practices among industry stakeholders can significantly improve collective defense against cyber threats. The Cybersecurity and Infrastructure Security Agency's (CISA) Automated Indicator Sharing (AIS) program could be an effective platform to foster such exchange.
3. Invest in security technologies: The government can promote the adoption of advanced security technologies, such as encryption, intrusion detection systems, and AI-based solutions, to protect IoT devices and systems. The

National Science Foundation (NSF) and Department of Defense (DoD) have research and development programs that could be expanded to support these technologies.

4. Implement security-by-design principles: The government should encourage organizations to adopt a security-by-design approach, integrating cybersecurity considerations into the design and development of IoT devices and systems. Existing programs, like NIST's Secure Software Development Framework (SSDF), can provide guidelines for this approach.
5. Develop a comprehensive supply chain cybersecurity framework: The federal government can leverage programs like the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to create a comprehensive framework that addresses various aspects of supply chain cybersecurity. This includes risk assessment, threat monitoring, incident response, and recovery plans specifically tailored for IoT in supply chain logistics.
6. Raise awareness and provide training: The federal government could develop programs to raise awareness of supply chain cybersecurity risks and provide training for organizations and their workforce. Programs such as the Federal Virtual Training Environment (FedVTE) can be leveraged to provide free cybersecurity training for personnel involved in managing IoT technologies within supply chains.

Potential implementation barriers:

Possible barriers to implementing this recommendation include:

1. Limited resources: Organizations may face resource constraints, including financial, technical, and human resources, which may limit their ability to strengthen cybersecurity measures.
2. Complexity of supply chains: The complexity of global supply chains, with numerous interconnected partners and systems, may make it challenging to implement comprehensive cybersecurity measures.
3. Resistance to information sharing: Organizations may be hesitant to share information about vulnerabilities or incidents due to concerns about revealing competitive information or damaging their reputation.

Evolving threats: Cyber threats are continuously evolving, which may make it difficult for organizations to stay ahead of potential attackers.

Enabling Recommendation 3.1.2: The government should consider additional ways to highlight those vulnerabilities most likely to be applicable to IoT product developers.

Provide guidance to IoT developers to help them efficiently meet requirements in standards or best practices for addressing “critical vulnerabilities” (or similar

requirements for making sure known or identified vulnerabilities are addressed). This may be accomplished, for example, by providing a list of known IoT operating system vulnerabilities that developers should be aware of and address, or a means to filter an existing list for such vulnerabilities.

The government provides key guidance to the private sector in many categories. For IoT, CISA has guidance for IoT acquisition (<https://www.cisa.gov/resources-tools/resources/internet-things-iot-acquisition-guidance-document>), use (<https://www.cisa.gov/news-events/news/securing-internet-things-iot>), and for specific sectors (<https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper%203.6.19%20-%20FINAL.pdf>).

The government also maintains vulnerability lists, including the National Vulnerability Database (NVD) maintained by NIST (<https://nvd.nist.gov/vuln/Vulnerability-Detail-Pages>) and the Known Exploited Vulnerabilities Catalog (KEV Catalog) maintained by CISA (<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>).

An IoT developer is encouraged or required to make sure they address any “known vulnerabilities” or “critical vulnerabilities” as part of best practices. The FCC NPRM on the U.S. Cyber Trust Mark program (FCC 23-65 in PS docket no. 23-239) mentions “identified security vulnerabilities” @58 and “critical patches” @40.

One can already filter by “IoT” as a keyword in the National Vulnerability Database, which pulls up 1100+ hits. Those results include many product-specific hits. For example, CVE-2023-23575 is, “*Improper access control vulnerability in CONPROSYS IoT Gateway products allows a remote authenticated attacker to bypass...*” That information is useful to users of the CONPROSYS product, but not to IoT developers.

But buried in that the same set of results are items relevant to IoT developers. For example, CVE-2023-23609 is, “*Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. Versions prior to and including 4.8 are vulnerable to an out-of-bounds write...*” As Contiki is an IoT operating system, this result would potentially be useful in this context.

While there is a national interest in IoT developers addressing critical vulnerabilities, there appears to be no resource in the public or private sector that can be mapped to IoT vulnerabilities.

Implementation Considerations:

- Vulnerabilities under consideration may be in developer-generated code, or in an IoT operating system or open-source library. The open-source or operating system vulnerabilities would be subject to this list.

- Vulnerabilities under consideration may be known pre-market (at the time of development), or discovered post-market. Developers should monitor the list for both pre-market and post-market vulnerabilities.
- Criteria must be established for “critical IoT source vulnerabilities”. These criteria should be based on whether the IoT vulnerability in question is applicable to a developer of a product, rather than to a specific model from a specific brand.

Potential implementation barriers:

If the NVD is used, existing data would need to be reviewed to see if it meets the criteria and should be flagged as a critical IoT source vulnerability.

Enabling Recommendation 3.1.3: The government should accelerate the promotion and adoption of procedures and methods to make the electric grid enabled by IoT more reliable and resilient.

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

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

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

Enabling Recommendation 3.1.4: Congress and regulatory agencies should support domestic IoT cybersecurity labeling initiatives by establishing incentives for manufacturers to participate.

Participation in the U.S. cybersecurity label program has begun strong, but with the expectation that certain issues would be addressed over time. Manufacturers cite concerns over perceived new liabilities incurred by adding the label to the product, as well as concerns over the existing possibility of enforcement action by relevant agencies in the event of a device hack. Relief from this concern could be via an earned

safe harbor provision and agencies' affirmation that participants in the program have met a criterion of "reasonable security".

Other incentives include preemption of mismatched state regulations for program participants, global recognition of the U.S. mark, and well-funded government campaigns to educate consumers about the mark.

Implementation considerations:

- Congress should enact an "earned safe harbor" that includes protection for program participants from civil actions.
- Regulatory agencies should act within the scope of their authority to clarify that earning the U.S. Cyber Trust Mark meets their expectations of reasonable security or the equivalent.
- Congress should establish preemption of mismatched state laws for program participants.
- The Department of State, the FCC and NIST should negotiate mutual recognition or "equivalence" across borders.
- Congress should ensure adequate funding for a robust consumer education campaign.

Enabling Recommendation 3.1.4A (to be renumbered): Congress must ensure adequate and continuing funding for the Cyber Trust Mark consumer education campaign.

[Added Thursday]

The U.S. Cyber Trust Mark program can empower consumers to make informed decisions about the cybersecurity of the connected products they purchase. This in turn can move the market, providing manufacturers with an incentive to improve the security of the product they make and maintain. The result can be reduced systemic risk for U.S. networks.

The success of the program is vitally dependent upon the awareness of the individuals and businesses that take advantage of it. Consumer education enables stakeholders to make informed decisions about product selection and helps to differentiate trustworthy products in the marketplace. Of course, industry participants recognize that they have a role to play in educating the public. Manufacturers will likely include information about the Mark with products; retailers will likely train sales associates to help customers.

But a public service advertising campaign is required as well. This PSA campaign must be broad and effective enough to create high Mark recognition among the U.S.

population. Such results are beyond the reach of manufacturers and retailers. The U.S. government must take a leading role.

A multi-year campaign and funding on par with that of EchoStar is required. For this, Congress must step in to ensure adequate and continuing funding for a consumer education campaign.

Enabling Recommendation 3.1.5: The government should establish appropriate U.S. representation regarding international harmonization of IoT cybersecurity programs and requirements as such programs are established for domestic market sectors.

The IoTAB strongly supports the voluntary public/private partnership that created the U.S. Cyber Trust Mark.

The U.S. Department of State must prioritize supporting the Mark program owner, NIST and stakeholders in the relevant private sector for each of the various U.S. cybersecurity trust certification programs, in conjunction with relevant agencies, to engage allies and partners toward harmonizing standards and pursuing mutual recognition of the U.S. Cyber Trust Mark and similar labeling efforts.

In Consumer IoT, the FCC's U.S. Cyber Trust Mark is the subject of a joint agreement between the U.S. and the EU. In October 2023, the two governments released a Joint Statement covering many areas of agreement. For consumer cyber protection, the Statement says,

"[We] commit to work together on achieving mutual recognition for our government-backed cybersecurity labeling programs and regulations for Internet-of-things devices aiming at a Joint CyberSafe Products Action Plan."[ref. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/20/u-s-eu-summit-joint-statement/> @ 28]

Subsequently, the Biden Administration announced a roadmap to that end [<https://broadbandbreakfast.com/2024/01/ces-2024-biden-administration-announces-deal-with-eu-on-cyber-trust-mark/>]. It is expected that the consumer-oriented U.S. Cyber Trust Mark at the FCC is the first of multiple sector-specific IoT cybersecurity programs. Other examples may be smart energy or industrial IoT. Harmonization of U.S. programs with those of other nations is key to global relevance and success.

Going forward, NIST, as the central agency of IoT cybersecurity expertise, should be part of such harmonization discussions. As program ownership is determined, as is

the case of FCC with the U.S. Cyber Trust Mark, that program owner should also be deeply involved in harmonization discussions. State, with international relationship responsibility, can assist in convening or coordinating.

Enabling Recommendation 3.1.6: The government should recognize and promote existing standards, and conformity assessment schemes that facilitate cybersecurity in industrial IoT applications.

Cybersecurity postures vary depending on the type of product produced and its intended market audience and use, thereby complicating the creation of a comprehensive or one-size-fits-all solution in relaying the security level of a product. The industrial IoT sector primarily utilizes operational technology (“OT”) systems and products. OT is comprised of hardware and software that detects or causes a physical change through the direct monitoring and/or control of industrial equipment. OT devices are those that are not broadly defined as ‘consumer’ due to their usage in commercial operations and are not available or readily available for sale to the public.

There exist numerous standards and conformity assessment schemes related to industrial OT systems and smart manufacturing, such as the IEC 62443 series of standards and conformity assessment programs. The IEC 62443 program is mature, well-respected, and already has multiple certifying programs such as ISASecure.org. The UL 2900 series of standards is another suitable program. These standards and certification programs provide a systematic, practical, and holistic approach to addressing cybersecurity.

Implementation Considerations:

- These existing standards and conformity assessment schemes can demonstrate cybersecurity compliance by a number of methods based on a risk assessment. They can include a manufacturer self-attestation that the product or device complies to a certain cybersecurity standard, documentation that the product or device uses a Secure Development Life Cycle that places security front and center during the product development, or third-party testing compliance via a Nationally Recognized Testing Laboratory.
- NCCoE or similar public-private agency groups should be considered for programs to highlight usage of selected standards.
- International harmonization and alignment should be pursued to the greatest extent possible

Data Privacy Regulation

Key Recommendation 3.2: Congress should pass comprehensive federal privacy legislation.

To address the growing complexities and uncertainties surrounding data privacy in the United States, a key recommendation has been proposed to the U.S. government: the support of a comprehensive Federal Data Privacy Regulation. This initiative seeks to support the establishment of uniform standards for data privacy across the nation, aiming to harmonize the existing patchwork of State privacy regulations. The primary motivation behind this recommendation is to reduce the complexity and legal uncertainty currently faced by businesses, which often have to navigate a labyrinth of varied State laws regarding data collection, storage, use, and sharing.

To effectively implement this regulation, several challenges need to be considered. These include addressing four key aspects of data privacy - collection, storage, use, and sharing - and carefully considering the costs associated with implementing and enforcing the new regulation. Additionally, there needs to be a well-thought-out transition period and set compliance deadlines for businesses presently operating under various State laws.

However, implementing a comprehensive Federal Data Privacy Regulation is not without challenges. The U.S. government is likely to face legislative gridlock and potential opposition from various interest groups. Managing preemption and the private right of action will be crucial, along with the need for inter-agency cooperation. Several agencies could be pivotal in championing this recommendation, including the Federal Trade Commission (FTC), the Department of Commerce, and the House Committee on Energy and Commerce.

In pursuing this course of action, it is recommended that the U.S. government support efforts like those proposed by the House Committee on Energy and Commerce on National Data Privacy Regulation. Moreover, leveraging the National Cybersecurity Strategy Implementation Plan of July 2013, particularly the initiative on cyber regulatory harmonization, could provide a solid foundation for this effort.

Enabling Recommendation 3.2.1: Congress should include IoT in proposed comprehensive privacy legislation.

To enhance privacy standards and foster innovation in the rapidly evolving realm of the Internet of Things (IoT), a recommendation has been proposed to the U.S. government to include IoT considerations in any future Federal Privacy Regulation Proposal. This recommendation focuses on adding specific provisions regarding IoT

Data Retention and Transparency. It aims to establish clear guidelines for manufacturers on the duration of data retention for business, government, and consumer data. This move is intended to align with existing or future Federal privacy legislation by integrating IoT-specific language related to data retention.

This recommendation ensures that IoT device manufacturers adhere to a consistent set of privacy standards and yet benefit from a resolution of current uncertainties in the domestic marketplace. This consistency is pivotal in enhancing the trust and protection of data across business, government, and consumer sectors. Moreover, the recommendation aims to stimulate innovation by providing IoT businesses with clear guidelines and expectations, fostering a competitive and growth-oriented environment.

For successful implementation, the U.S. government must consider privacy legislation to address the unique challenges and technological advancements in the IoT sector. However, this initiative faces several potential barriers. These include achieving consensus among stakeholders and State-level regulators on incorporating effective elements and practices into the Federal privacy legislation. Additionally, there's a need to ensure that these new IoT-specific requirements are compatible with existing national and international privacy regulations. Balancing data privacy protection with promoting innovation in the IoT sector is another critical consideration. Moreover, providing adequate resources, guidance, and support to businesses for adopting and implementing these IoT-specific requirements is essential.

Several bodies within the U.S. government could play a significant role in championing this recommendation, including Congress, the Department of Commerce (DoC), the National Institute of Standards and Technology (NIST), and the Federal Trade Commission (FTC). The overarching goal is to support the inclusion of IoT in the contemplated Federal Data Privacy legislation, ensuring a comprehensive and future-proof privacy framework in the age of IoT.

Data and Privacy Policy

Key Recommendation 3.3: The White House and Congress should facilitate/support the development of a Data and Privacy Policy Framework.

The White House and Congress should facilitate/support the development of a Data and Privacy Policy Framework that clearly considers the different aspects of privacy and confidentiality including transparency and control over data collection and usage for individuals, and data confidentiality for organizations.

The resulting framework would consider the different aspects of privacy and confidentiality including transparency and control over data collection and usage for individuals, and data confidentiality for organizations. data (i.e., machine versus personal) and how they should or shouldn't be utilized in smart transportation technologies.

The justification for this recommendation stems from the need for a consistent and unified approach to data, privacy, and security within the IoT sector. This move will reduce confusion and fragmentation for businesses, government entities, and consumers. Acknowledging the advancements in privacy legislation by several U.S. States, this framework also seeks to encourage innovation by providing clear guidelines and expectations for IoT device manufacturers, thus fostering a competitive and growth-oriented environment.

However, implementing such a framework comes with its considerations and challenges. The U.S. government is advised to draw lessons from existing privacy regulations to create an effective and efficient framework. This framework must remain adaptable and scalable to keep pace with the rapidly evolving nature of IoT technology and the data privacy landscape.

One of the key challenges in implementing this framework is balancing the protection of data privacy for businesses, government, and consumers while simultaneously fostering innovation in the IoT sector. Additionally, the government needs to provide adequate resources, guidance, and support to businesses to adopt and implement this framework. Regular review and framework updates are essential to ensure its relevance and effectiveness in addressing emerging data privacy challenges and technological advancements.

Congress is identified as a possible participating body that could assist or champion this recommendation. For successful implementation, the U.S. Federal government should consider working closely with States that have already embraced privacy frameworks or are advancing regulations. This collaboration is vital for regulatory alignment. The government is also encouraged to utilize strategies from the National Cybersecurity Strategy Implementation Plan of July 2013, particularly initiatives focused on cyber regulatory harmonization and increasing agency use of frameworks and international standards for regulatory alignment.

Example use cases include:

- Data from a Traffic Camera at an intersection could be used to determine who was responsible for an accident and allow for more efficient insurance claims.

- Data generated from a connected vehicle and its corresponding roadside infrastructure can be utilized to transmit basic safety information to the vehicle's driver such as entering a school or work zone.
- Emergency Vehicles and corresponding roadside infrastructure can generate data to preempt traffic signals so the vehicles can get to their destination sooner.

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

Implementation considerations: In conjunction with supporting a National Privacy Framework, the federal government should consider setting high-level policy guidelines for data ownership, retention and usage that include specific guidance for data that has personal information. These guidelines should leverage existing legislative or regulatory language and provide incentives for state and local jurisdictions to adopt them. The creation of a model and guidelines for data ownership, retention and usage would provide states and local jurisdictions the ability to develop criteria for how long data should be retained, how personal information should be stripped from any such data, and how to effectively utilize that data in their operations.

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

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

Notably, it may be challenging to consistently identify and separate data that has personal or private information, or for commercial entities, confidential data and intellectual property.

Enabling Recommendation 3.3.1: The government should promote "Privacy by Design" in IoT device development, deployment, and implementation.

In the realm of IoT (Internet of Things), the U.S. government is recommended to adopt and promote the "Privacy by Design" (PbD) approach in the development,

deployment, and implementation of IoT devices. This recommendation is in line with the U.S. National Strategy to Advance Privacy-Preserving Data Sharing and Analytics (PPDSA) as of March 2023 and the National Cybersecurity Strategy Implementation Plan of July 2013. The latter particularly emphasizes scaling public-private partnerships to develop and adopt technologies that are secure by design and default.

The rationale behind this recommendation is multifaceted. Firstly, it aims to minimize data privacy risks and the ensuing legal complications, thereby aligning IoT privacy practices with international data protection standards. Additionally, the approach serves to educate both businesses and consumers about privacy in IoT, providing incentives to companies that comply with PbD guidelines.

Implementing this recommendation, however, comes with its own set of challenges. These include the difficulty in monitoring a diverse and constantly evolving range of IoT applications and potential resistance from the private sector, which might perceive PbD implementation as risky or costly. Another significant challenge is developing universally accepted privacy standards for IoT.

For the successful execution of this recommendation, the involvement of key U.S. government agencies is essential. The Office of Science and Technology Policy (OSTP), the National Institute of Standards and Technology (NIST), and the Federal Trade Commission (FTC) are identified as critical players in championing this recommendation.

To effectively implement PbD in IoT, the U.S. government needs to consider several factors. These include the development of clear PbD guidelines and the provision of incentives to companies that comply. It's also important to ensure the adaptability of these principles across various IoT devices and to align them with international privacy standards. Support for small and medium enterprises (SMEs) in adhering to these principles is crucial, as is the regular evaluation and refinement of guidelines and incentives. The government should also consider leveraging the National Cybersecurity Strategy Implementation Plan to drive the development of secure-by-design technology through public-private partnerships.

Enabling Recommendation 3.3.2: The government should establish clear policies for third-party data sharing and IoT device data use

In response to IoT devices' growing interconnectivity and data-sharing capabilities, which pose significant privacy risks, the U.S. government is recommended to establish clear policies for third-party data sharing and IoT device data use. This recommendation includes outlining IoT manufacturers' and service providers'

responsibilities and obligations when dealing with third-party entities, emphasizing the importance of user consent and secure data practices.

The rationale for this recommendation stems from the need to safeguard consumers' personal data and ensure transparency in how this data is shared and used. By establishing clear policies, the government can foster trust among users and encourage wider adoption of IoT technologies. These policies are expected to communicate third-party data sharing and usage in privacy policies and be supported by public awareness campaigns to educate users about their data rights.

However, implementing these policies faces potential barriers, including resistance from IoT companies who rely on third-party data sharing for their business revenue and challenges in aligning these new policies with existing privacy regulations and international data protection standards.

To overcome these barriers and effectively implement these policies, the U.S. government should consider working with industry leaders to establish data use guidelines, leveraging the National Cybersecurity Strategy Implementation Plans from July 2013. These include Initiative Number 1.1.1, focusing on cyber regulatory harmonization, and Initiative Number 1.1.3, which aims to increase agency use of frameworks and international standards for regulatory alignment.

Agencies within the U.S. government, including the National Institute of Standards and Technology (NIST), the Federal Trade Commission (FTC), the Department of Energy (DOE), the United States Department of Agriculture (USDA), and the Office of the National Cyber Director (ONCD), are identified as key players who could assist or champion the recommendation, contributing to the establishment of a more secure and transparent IoT ecosystem.

Enabling Recommendation 3.3.3: The government should encourage the use of plain language in IoT privacy policies.

In IoT and privacy, a crucial recommendation for the U.S. government is adopting plain language in privacy policies. This recommendation, stemming from the Internet of Things (IoT) Cybersecurity Improvement Act of 2020, focuses on integrating plain language into privacy policies. The goal is to simplify privacy policies, notices, and data use policies, making them more accessible and understandable to users. This initiative aligns with the "Plain Writing Act of 2010" (Public Law 111-274), which the government can use to model this recommendation on organizations providing IoT technology to the government.

The justification for this recommendation lies in its potential to improve user understanding of data privacy policies, thereby leading to more informed decisions regarding IoT device usage. Additionally, it aims to enhance public trust in IoT devices and related technologies, and simplified policies could result in increased compliance and fewer legal disputes.

Implementing this recommendation requires the U.S. government to develop guidelines and best practices for organizations on simplifying privacy policies. It involves establishing criteria for evaluating the readability of these policies and coordinating with various stakeholders, including the private sector, business, government, and consumer data advocacy groups, to ensure widespread adoption.

However, potential barriers exist. Organizations might resist simplification, fearing it could limit their legal protections. There are also challenges in defining the appropriate level of simplification while ensuring policies remain accurate and comprehensive. Moreover, monitoring and updating these guidelines in response to technological advancements and emerging privacy concerns is crucial.

Agencies within the U.S. government that could play a key role in championing this recommendation include the National Institute of Standards and Technology (NIST), the Department of Commerce (DoC), the Office of Management and Budget (OMB), which oversees the Act's implementation, and the Office of the National Cyber Director (ONCD).

For effective implementation, the U.S. Federal government should consider creating requirements for IoT providers to implement simplified privacy policies in government contracts. This can be achieved by utilizing the National Cybersecurity Strategy Implementation Plan of July 2013, particularly Initiative Number 3.2.1, related to the IoT Cybersecurity Improvement Act of 2020, and Initiative Number 1.1.1, focused on cyber regulatory harmonization. The Plain Writing Act of 2010 is also a foundation for this recommendation.

Privacy Protections and Transparency for IoT

Enabling Recommendation 3.3.4: The government should develop and implement privacy transparency mechanisms.

In the evolving landscape of IoT and privacy, the U.S. government is poised to take a significant step forward with the recommendation of establishing a comprehensive privacy transparency system for IoT devices. This initiative, drawing inspiration from other transparency frameworks, is designed to significantly empower various stakeholders – businesses, governments, and consumers – by providing them with

detailed insights into the privacy features and practices of IoT devices. This move is anticipated to enhance general awareness and stimulate IoT manufacturers to prioritize privacy, thereby fostering innovation and competition in the development of privacy-enhancing technologies.

For the successful deployment of this system, the government needs to consider the perspectives of privacy experts, industry stakeholders, and advocacy groups. It is essential to develop clear guidelines and standards for privacy transparency, including what information should be included, its format, and how it should be presented. It is also crucial to motivate IoT device manufacturers to adopt this system, supporting them in aligning with these new recommendations.

However, challenges such as ensuring widespread adoption and compliance across different industries, motivating manufacturers, and balancing comprehensive information with simplicity and understandability need to be addressed. Key agencies like the Department of Commerce, the National Institute of Standards and Technology, and the Federal Trade Commission could play instrumental roles in driving this initiative forward.

Additionally, the government's strategy should promote the benefits of IoT privacy transparency, forging partnerships with industry leaders to develop this system and leveraging existing initiatives under the National Cybersecurity Strategy Implementation Plan. These steps would establish a robust framework for IoT privacy and significantly contribute to enhancing cybersecurity and data protection in the digital era.

Enabling Recommendation 3.3.5: The government should endorse universal opt-out signals for IoT devices and companion apps.

In an initiative to bolster privacy and data protection in the Internet of Things (IoT) realm, the U.S. government is recommended to endorse Universal Opt-Out Signals for IoT devices and their companion apps. This proposal is driven by the growing need to safeguard user privacy in an increasingly interconnected digital world. Adopting Universal Opt-Out Signals would simplify the process for consumers, enabling them to easily manage their privacy settings across various IoT devices and applications.

However, implementing this recommendation is not without its challenges. The government must consider the technical feasibility of applying these universal opt-out signals across various devices and apps and the associated costs of establishing and enforcing such a system. Standardized guidelines or legislation may be necessary to ensure uniform adoption of the Universal Opt-Out Signals.

Resistance from IoT manufacturers and app developers is anticipated, primarily due to the potential costs and complexities of implementing these signals. Additionally, the technological constraints of harmonizing these signals across different platforms and devices pose a significant challenge. Another crucial aspect is effectively communicating to consumers how Universal Opt-Out Signals can facilitate easier management of their privacy rights.

Several agencies within the U.S. government could play pivotal roles in championing this initiative, including the Federal Trade Commission (FTC), the National Institute of Standards and Technology (NIST), the Federal Communications Commission (FCC), and the Department of Commerce.

In formulating the implementation strategy, the government should consider leveraging existing frameworks and regulations. This includes the National Cybersecurity Strategy Implementation Plan of July 2013, which suggests initiating a U.S. Government IoT security labeling program. Furthermore, existing privacy laws like the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), along with the Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act (CTDPA), provide valuable precedents for enforcing privacy provisions starting from 2024. These laws and initiatives could serve as models for developing a comprehensive and effective system of Universal Opt-Out Signals in the IoT space.

Enabling Recommendation 3.3.6: The government should include IoT Privacy information on new car automobile “Monroney Stickers”.

In the landscape of connected automobiles, where privacy concerns are mounting, a crucial recommendation has been presented to the U.S. government: including IoT Privacy Information on "Monroney Stickers" for new and used cars. This recommendation aims to leverage the traditional role of Monroney Stickers – known for detailing fuel efficiency and safety ratings – to now also disclose vital information about IoT privacy. This encompasses data collection, retention, sale, and the availability of a universal opt-out feature.

This initiative is primarily driven by the need to enhance consumer protection and address growing concerns over personal data use and sharing by IoT devices in automobiles. The urgency of this issue is highlighted by findings from the Mozilla Foundation's Automobile Privacy Report in 2023, which reveals that all 25 car brands reviewed in this report collect personal data, with most sharing or selling this information. The report further indicates that most brands offer limited control over drivers' data, and many have concerning records regarding privacy breaches. Notably, the report notes that none of the car brands reviewed that participate under the

Alliance for Automotive Innovation adhere to voluntary consumer protection principles focusing on data privacy.

However, the path to implementing this recommendation involves overcoming several hurdles. It requires a standardized, straightforward, and concise method to present IoT privacy information, ensuring compliance with existing privacy laws and adaptability to future technological developments. The U.S. government must also prepare for possible resistance from automakers concerned about cost implications, the task of educating consumers about the importance of this information, and the complexity of the regulatory landscape governing IoT and privacy.

A united effort from various U.S. government agencies is imperative to successfully implement this recommendation. Agencies such as the Federal Trade Commission (FTC), National Highway Traffic Safety Administration (NHTSA), Federal Communications Commission (FCC), Department of Transportation (DOT), and the Cybersecurity and Infrastructure Security Agency (CISA) could play critical roles. Their involvement would uphold the principles of the Automobile Information Disclosure Act of 1958 and significantly bolster consumer rights in an era increasingly defined by connected technology.

Enabling Recommendation 3.3.7: The government should add "Location Tracking Enabled" notice to U.S. E-labeled IoT devices.

In a move to enhance consumer awareness and data privacy in the IoT sphere, a pivotal recommendation has been proposed to the U.S. government. It focuses on incorporating a clear and upfront notification within the U.S. e-labeling program for IoT devices, specifically stating, "Notice: Precise location tracking is enabled by default on this device." This recommendation emerged from a deep-seated belief in transparency and informed consent. Consumers, often unknowingly, have their location data collected and shared by various IoT devices. This straightforward Statement aims to inform consumers about this data collection practice immediately.

The justification for this recommendation is threefold. Firstly, it upholds the consumer's right to know if and how their location data is tracked. Secondly, it emphasizes the ethical imperative of informed consent in data collection, ensuring that consumers know these practices without navigating complex privacy policies. Lastly, this recommendation aligns with various data protection regulations advocating transparency and informed consent.

However, implementing this recommendation poses several challenges and considerations. The U.S. government needs to standardize the Statement's wording and visibility to consumers as part of the U.S. e-labeling program. It is crucial to assess

the technical feasibility of how and where this notice will be displayed—be it on the physical device, a website, or an associated app—for effective consumer awareness. Moreover, robust systems for audits and compliance must be established to ensure adherence to this notification requirement.

Potential barriers to this implementation include resistance from the industry, which might perceive this as a negative impact on sales or an added complexity in providing product information. Consumer education also presents a hurdle, as there is a risk that all users might not fully understand the importance of this notice. Legal challenges are another concern, as companies might view this requirement as an unfair labeling burden.

To champion this recommendation, collaboration among various U.S. government agencies, including the Federal Trade Commission (FTC), the National Institute of Standards and Technology (NIST), and the Federal Communications Commission (FCC), is essential. Furthermore, the U.S. government should consider leveraging strategies from the National Cybersecurity Strategy Implementation Plan of July 2013, specifically, Initiative Number 4.6.1, titled "Publish a National Cyber Workforce and Education Strategy", to foster a comprehensive approach to this privacy-enhancing initiative.

Enabling Recommendation 3.3.8: The government should promote the use, development, and implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.

In the realm of IoT, the U.S. government is recommended to champion the implementation of Privacy-Enhancing Technologies (PETs). These technologies are vital in safeguarding privacy while still harnessing valuable insights from the expansive IoT data. PETs align with responsible data use principles and bolster trust and acceptance of IoT solutions across society. Their adoption is crucial for preventing data breaches and the ensuing legal complications.

However, the path to implementing PETs is not without challenges. The government needs to ensure robust security measures are in place to avert unauthorized data access and conduct thorough technical and ethical evaluations before adopting these technologies. It's also essential to enhance public understanding and trust in PETs and encourage interoperability among different PET systems is also essential. Developing a framework to monitor PETs' effectiveness and impacts in the IoT environment.

The implementation journey may encounter hurdles such as limited technical expertise for understanding, implementing, and managing PETs. Resistance from the

private sector, often due to perceived risks or costs, and the complexity of developing universally accepted privacy standards for IoT are other potential barriers.

One of the primary hurdles in this endeavor is the resistance from the private sector, often stemming from perceived risks or costs associated with PET integration. A U.S. government initiative that not only promotes PETs but also offers guidelines and support could be instrumental in helping manufacturers. Such an initiative would facilitate the production of more privacy-conscious IoT devices, thereby reinforcing the security and trustworthiness of IoT systems in the eyes of users and manufacturers alike.

To effectively implement this recommendation, several agencies within the U.S. government could play pivotal roles, including the Office of Science and Technology Policy (OSTP) and the National Institute of Standards and Technology (NIST). The government should consider leveraging existing frameworks and initiatives, such as the IoT Cybersecurity Improvement Act of 2020, The White House's proposal for Advancing a Vision for Privacy-Enhancing Technologies (June 2022), and the National Cybersecurity Strategy Implementation Plan (July 2013), particularly the initiative focused on scaling public-private partnerships for secure technology development and adoption. This approach ensures a comprehensive and collaborative effort towards integrating PETs into IoT systems, aligning with the broader goal of leveraging technology for societal benefits while maintaining user privacy.

Enabling Recommendation 3.3.9: The government should follow NIST sanitization standards for government automobiles before resale, and should encourage NIST sanitization standards for automobiles before resale.

Follow NIST sanitization standards for government automobiles before resale:

In enhancing privacy and security in the used automobile sector, the U.S. government faces a crucial recommendation: to mandate that car seller organizations adhere to the National Institute of Standards and Technology's (NIST) media sanitization guidelines before reselling vehicles. This recommendation aligns with the e-Stewards Standard, supported by the Environmental Protection Agency (EPA) Recycling Program. The core objective is to protect consumer privacy and prevent unauthorized access to sensitive data that modern vehicle systems often store.

The implementation of this recommendation, however, is not without its challenges and considerations. The U.S. government must account for the financial implications for car sellers, who would bear the cost of implementing these sanitization standards. Additionally, there's a need for comprehensive training and awareness programs to

familiarize car sellers with the NIST guidelines. The technological infrastructure to support these sanitization processes is another vital consideration, along with robust mechanisms for monitoring and ensuring compliance.

Yet, the path to implementation is beset with potential barriers. Car-selling organizations might resist these changes due to the perceived increase in operational costs. Older vehicle models might present technological limitations that complicate compliance with the guidelines. Furthermore, potential legal challenges related to data privacy and compliance need to be navigated.

To champion this initiative, several U.S. government agencies could play pivotal roles. The National Institute of Standards and Technology (NIST) and the Department of Transportation (DOT) are key players, along with the Federal Trade Commission (FTC) and the Environmental Protection Agency (EPA).

For the successful execution of this recommendation leverage existing frameworks and standards for a successful implementation. This includes utilizing the National Cybersecurity Strategy Implementation Plan, specifically Initiative Number: 1.1.3, which focuses on increasing agency use of frameworks and international standards for regulatory alignment. The NIST Cybersecurity Framework provides a solid foundation, particularly the 'PROTECT - Secure Data - 800-88 Rev. 1 - Guidelines for Media Sanitization', provides a solid foundation. Additionally, aligning with the EPA's implementation of Electronics Recycling Standards, particularly R2, and e-Stewards, will ensure a comprehensive approach to sanitizing and reselling used automobiles.

Encourage NIST sanitization standards for automobiles before resale:

In response to the emerging privacy and security challenges associated with the resale of government automobiles equipped with IoT technologies, a significant recommendation has been proposed: Mandating NIST Sanitization Standards for Government Automobiles Before Resell. This narrative encapsulates the key aspects of this recommendation.

The U.S. government is advised to ensure that before reselling, all agencies adhere strictly to the media sanitization guidelines set forth by the National Institute of Standards and Technology (NIST) before reselling. This requirement is not just a procedural formality but a critical step to safeguard consumer privacy and prevent unauthorized access to sensitive information that might be stored in modern vehicle systems. Such an approach aligns with the e-Stewards Standard, supported by the Environmental Protection Agency (EPA) as part of its Recycling Program.

However, implementing these standards is not without its challenges. The government must consider the financial implications, including the costs associated

with procuring and deploying data sanitization tools across its entire fleet of vehicles. Additionally, ensuring that these sanitization solutions are compatible with a diverse range of vehicle models and embedded systems is crucial.

Another significant aspect of this recommendation involves the human element – training and awareness. Government staff and contractors need comprehensive training in new data sanitization procedures, which could be resource-intensive. To facilitate this, developing awareness programs about these guidelines is essential.

The government should leverage existing frameworks and international standards to align regulations for effective implementation and monitoring. This includes utilizing resources such as the National Cybersecurity Strategy Implementation Plan and the NIST Cybersecurity Framework, specifically focusing on securing data and adhering to guidelines for media sanitization.

Collaboration across various agencies will be pivotal in successfully implementing this recommendation. Agencies like the NIST, Department of Transportation (DOT), and EPA are poised to play crucial roles, each bringing their unique expertise and resources.

The proposal to mandate NIST sanitization standards for government automobiles before reselling represents a comprehensive approach that combines regulatory alignment, technological solutions, and human resource training. It is a concerted effort to enhance data security, align with environmental standards, and ultimately protect consumer privacy in the age of IoT.

.

Connected IoT-based Supply Chain Logistics

Objective 4: The U.S. has an opportunity to improve supply chain visibility and collaboration by increasing the use of IoT sensors and other connected devices. Evaluating the effectiveness of this IoT adoption and monitoring progress will demonstrate the value provided, support collaborative public-private partnerships, and ensure trusted architectures. A limited pilot to demonstrate the benefits of trusted “digital threads” across the value chain will help the U.S. maintain security and efficiency.

Key Recommendation 4.1: The government should monitor and evaluate progress of IoT adoption for supply chain logistics.

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. The need to monitor and evaluate progress in IoT adoption for supply chain management stems from the need to ensure the effectiveness of implemented strategies, measure their impact, and identify areas for improvement.

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

Regular assessments should be conducted to track the progress of IoT adoption against the established targets, identify any gaps or challenges, and evaluate the effectiveness of the implemented policies and initiatives. Based on the findings of these assessments, the government should adapt its strategies and actions to address the identified issues, optimize resource allocation, and maximize the impact of its efforts. By monitoring and evaluating progress, the government can ensure that its approach to driving IoT adoption in supply chain management remains agile, responsive, and results-oriented, ultimately contributing to the long-term success and competitiveness of the industry.

Implementation Considerations:

- Establish clear goals and objectives: Define specific, measurable, and time-bound goals and objectives for IoT adoption in supply chain management to enable effective monitoring and evaluation.
- Develop relevant performance indicators: Identify key performance indicators (KPIs) that reflect the desired outcomes of IoT adoption and can be used to measure progress and impact.
- Implement data collection and reporting mechanisms: Set up systems and processes for collecting, storing, and analyzing data related to IoT adoption and supply chain performance.
- Conduct periodic assessments: Schedule regular evaluations of progress and impact, using the collected data and KPIs to assess the effectiveness of IoT initiatives in supply chain management.
- Foster a culture of continuous improvement: Encourage feedback and learning from monitoring and evaluation results, using the insights to improve and refine policies and initiatives.
- Collaborate with stakeholders: Engage with industry, academia, and other relevant stakeholders to gather their insights and perspectives, ensuring a comprehensive understanding of progress and challenges.
- Assign responsibility: Designate a lead federal agency or interagency group responsible for overseeing the monitoring and evaluation process for IoT adoption in supply chain management.
- Develop a monitoring and evaluation plan: Create a detailed plan outlining the goals, objectives, KPIs, data collection methods, and evaluation schedule.
- Allocate resources: Ensure adequate financial, human, and technical resources are allocated to support monitoring and evaluation activities.
- Potential Barriers: Lack of clear goals and objectives: Ambiguous or poorly defined goals can make it difficult to assess progress and impact.
- Inadequate data collection and reporting mechanisms: Ineffective systems for collecting, storing, and analyzing data can hinder accurate and reliable monitoring and evaluation.
- Resource constraints: Limited resources can impede the government's ability to conduct thorough and consistent monitoring and evaluation.
- Resistance to change: Stakeholders may resist sharing information or adopting new practices based on evaluation results, limiting the impact of monitoring and evaluation efforts.

Public and Private Partnership

Key Recommendation 4.2: The government should 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.

The federal government should lead the formation of collaborative public-private partnerships (PPPs) to accelerate the adoption of Internet of Things (IoT) technologies within supply chain logistics operations. These partnerships bring together a diverse array of stakeholders, including government agencies such as the Department of Commerce, logistics providers, IoT technology companies, and academic institutions such as MIT's Center for Transportation & Logistics. The resultant platform would foster collaboration and knowledge exchange, stimulating the development, deployment, and wider adoption of IoT technologies in supply chain management.

PPPs can address common barriers to IoT adoption, including infrastructure gaps, limited technical knowledge, and financial constraints. By aligning efforts and pooling resources, these partnerships can drive the innovation of IoT solutions, initiate pilot projects, and roll out proof-of-concept initiatives that demonstrate the value and benefits of IoT in supply chain operations. Additionally, they can contribute to workforce development by creating and supporting training programs, potentially in collaboration with technical colleges and universities.

They also play a role in establishing industry standards and regulatory frameworks conducive to IoT adoption across the supply chain industry. This would involve close collaboration with regulatory bodies like the Federal Communications Commission (FCC) and standard-setting institutions like the National Institute of Standards and Technology (NIST). By fostering such partnerships, the government can nurture a thriving ecosystem that drives innovation and competitiveness in the supply chain sector, maximizing the potential of IoT technologies.

Implementation Considerations:

- Identifying key stakeholders: The federal government should identify relevant private sector stakeholders, including businesses, industry associations, research institutions, and technology providers, who can contribute to the development and implementation of IoT solutions in supply chain management.
- Establishing a collaborative framework: A formal framework should be established to facilitate collaboration between the public and private sectors. This may include creating joint working groups, industry forums, or innovation hubs, where stakeholders can share ideas, knowledge, and resources.

- Defining clear goals and objectives: Public-private partnerships should have well-defined goals and objectives that align with the overall strategy for promoting IoT adoption in supply chain management. This will help ensure that all stakeholders are working towards a common vision and can measure their progress.
- Developing joint projects and initiatives: The federal government and private sector stakeholders should collaborate on joint projects and initiatives that address specific challenges or opportunities in supply chain management. These could include pilot projects, research and development programs, or the development of new IoT standards and protocols.
- Ensuring effective communication and coordination: Open and transparent communication between the public and private sectors is critical for successful collaboration. Regular meetings, progress reports, and information sharing mechanisms should be established to facilitate coordination and maintain momentum.
- Monitoring and evaluation: The federal government should establish a system for monitoring and evaluating the effectiveness of public-private partnerships in promoting IoT adoption in supply chain management. This may involve tracking key performance indicators, such as the number of joint projects implemented, the amount of private investment leveraged, and the impact on supply chain efficiency and resilience.

Potential barriers:

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

Enabling Recommendation 4.2.1 The government should foster orchestrated Public-Private Partnerships (PPPs) promoting network effects among connected enterprises and across supply chains.

To speed up the creation of connected supply chains the government should promote PPPs that promote network effects to speed the adoption of end-to-end digital

threads using consistent digitalization methods capturing receivables, processes, and certified deliverables.

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

Examples:

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

Implementation Considerations

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

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

Potential Barriers

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

Enabling Recommendation 4.2.2: The government should subsidize initiatives for digital infrastructure supporting the digital transformation of enterprise business processes including design, production, procurement, distribution.

The digitalization of all business functions (design, production, marketing, procurement, distribution, etc.) enables more efficient IoT product management, greater visibility, and transparency over supply chains to track products, monitor quality, and fix issues or defects. By using cryptographic methods, digitalization can have a major impact in improving the security, reliability, integrity, and trust of data for the digital economy. By providing incentives for businesses to adopt digital tools, the federal government can help promote ecosystems that create opportunities for businesses and workers in any value chains which will drive economic growth. Furthermore, digitalization enables digital transformation whereby IoT device suppliers become connected to their customers which enables sustainability and circular economy.

Implementation Considerations:

- Develop and communicate clear guidelines and criteria for eligibility for the subsidies.
- Incentivize Orchestrated PPPs to work on Proof of Concept (PoC) ~~pilot~~ projects to assess the economic value before investing ~~to~~ **in solutions** to deploy at scale.

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

Potential Implementation Barriers:

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

Enabling Recommendation 4.2.3: The government should promote the enablement and use of trusted digital threads, trusted digital marketplaces and platform-based business ecosystems.

As digital threads and digital platforms emerge, the government should promote the enablement and use of these tools to drive economic growth with trusted data exchange and licensing while protecting the proprietary IP of enterprises in the value chain.

In the most general case, digital threads are the flow of data that connects business processes, products, and assets across supply chains, networks, or applications. In a narrower sense within the supply chain, each component (chip, software, module, device) has associated information regarding provenance, integrity, version and more. As components are associated with modules and the modules with assembled devices running software, this flow of data through the supply chain has the potential to inform security, product integrity and availability. Ideally, all of this information—this “digital thread”—is and remains available throughout stages of the supply chain, from original materials through installed systems.

A trusted digital thread benefits from cryptographic protection in each stage and throughout the flow. This information is valuable and can be exchanged in digital

marketplaces. The government should incentivize the enablement and use of trusted digital marketplaces where producers and consumers query and share information about assets and related data, enabling better visibility, traceability, and monetization while protecting proprietary IP and PII.

Trusted digital marketplaces can be promoted through pilot programs, best practices and guidelines. Platforms that facilitate adoption of digital marketplaces can enable producers and consumers to reduce costs and improve efficiency. Efficiencies come from streamlining processes and eliminating redundancies, especially in complex supply chains where information flows are often fragmented or disconnected. Furthermore, trusted digital marketplaces driven by digital threads enable participating stakeholders to evolve new business models and revenue streams. When these are combined with business platforms that maximize network effects, it will fuel the growth of ecosystems and future digital economies.

Implementation Considerations:

- Identify standards, taxonomies, and best practices to define supply chain trusted digital threads and marketplaces.
- Identify suitable marketplaces to incentivize and support (e.g., EV charging and monetization). Develop guidelines and incentives for access and use of data.
- Promote the benefits of data marketplaces to potential participants and provide tax credits and subsidies to encourage participation.
- Ensure data security and confidentiality measures are in place. Monitor and evaluate the effectiveness of the data marketplaces. Use analytics to improve visibility, traceability, efficiency, and cost.

Potential Barriers:

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

Enabling Recommendation 4.2.4: The government should promote trusted AI-IoT platforms across circular supply chains and ecosystems to improve transparency and sustainability and drive economic growth.

The government should promote trusted AI-IoT (“AIoT”) platforms within circular value chain ecosystems. Circular supply chain ecosystems are those sustainable cycles

where resources remain as much as possible in the loop of collection and processing, production and purchasing, consumption and use. Key is that resources can be cycled back again in these stages by use of sustainable processes of, e.g., remanufacture or recycling. Use of AIoT can enhance transparency, sustainability, and economic growth by fostering innovation and efficiency which will benefit businesses, the environment and digital economy.

Promoting trusted AIoT platforms within circular supply chain ecosystems is imperative for ensuring transparency, sustainability, and economic growth. This initiative not only fosters innovation but also enhances efficiency, benefiting businesses, the environment, and the future digital economy. By strategically integrating AIoT into circular supply chains, the government can create a foundation for responsible and sustainable technological advancement, positioning the nation as a leader for the global digital economies.

Examples:

- Innovation Hubs: Promoting AIoT platforms will drive innovation, enabling the development of cutting-edge technologies and solutions.
- Efficiency Boost: AIoT can optimize resource utilization, reducing waste and energy consumption within circular supply chains.
- Environmental Benefits: Sustainable practices fostered by this initiative can help combat climate change and promote eco-friendliness.
- Economic Growth: The growth of AIoT-driven industries will create jobs and stimulate economic development.
- Competitive Advantage: By embracing AIoT, the nation can establish itself as a pioneer in the digital economy, attracting global investments.

Implementation Considerations:

- Public-Private Partnerships: Encourage collaboration between government, businesses, and research institutions to drive innovation.
- Sustainability Standards: Establish clear sustainability guidelines for AIoT projects within circular supply chains.
- Data Governance: Develop robust data governance policies to protect privacy and promote transparency.
- Education and Training: Invest in workforce development and educational programs to prepare individuals for AIoT-related jobs.

Barriers:

- Privacy Concerns: Balancing data sharing with privacy protection can be challenging.
- Resource Allocation: Ensuring sufficient funding and resources for AIoT development.
- Security Risks: Rapid AIoT growth increases the risk of cybersecurity threats.
- Resistance to Change: Some stakeholders may be resistant to adopting AIoT due to fear or uncertainty.

Key Recommendation 4.3: The government should support trusted architectures and conduct a limited pilot to assess the value of trusted digital threads for provenance and traceability across the supply chain.

The government should support creation of cryptographically strong architectures and infrastructure that enable supply chain provenance, traceability, and lifecycle management by linking hardware and software bill of materials to the design and manufacturing processes delivering trusted assets and data.

This should incentivize suppliers to develop trusted architectures for supply chain provenance, traceability, assurance of supply and IoT product lifecycle management. By cryptographically linking trusted SBOM⁹⁷ to trusted HBOM⁹⁸ in any IoT device or system, industries can help mitigate the risks associated with supply chain security, compromised components, and ensure the security and reliability of critical systems.

This will strengthen national security, public safety, and economic stability, making it a valuable investment for the government and society such that:

- The use of trusted architectures for supply chain provenance and traceability can help mitigate the risks associated with vulnerabilities or compromised components.
- Trusted architectures for supply chain provenance and traceability can increase the trustworthiness of critical IoT systems, which is key for national security, public safety, and economic stability.
- Trusted architectures linked to Cyber Trust Mark⁹⁹ can increase consumer confidence in the products they purchase and prevent supply chain attacks and data breaches leading to greater economic benefits for businesses.

⁹⁷ Software Bill of Materials for Electronic parts and Software modules used in the assembly of a device or complex system.

⁹⁸ Hardware Bill of Materials must include a Root of Trust with a source of Entropy such for security and unique ID (fingerprint).

⁹⁹ The US Cyber Trust Mark all you need to know <https://www.iotforall.com/u-s-cyber-trust-mark-all-you-need-to-know>

- Cryptographic linking of SBOM to trusted HBOM enhances supply chain security, visibility, chain of custody and product lifecycle management. (and overall user confidence).
- Trusted HBOM and SBOM assets and related data can form the basis of trusted digital threads which also enable trusted IoT applications and data for AI based digital twins.

Implementation Considerations

- Educate stakeholders in the supply chain on the benefits of using trusted architectures for supply chain provenance and traceability.
- Promote industry adoption of trusted architectures through education and outreach. Incentivize hardware suppliers to develop trusted architectures that enable supply chain provenance and traceability and promote them with the Cyber Trust Mark.
- Develop guidelines for how the trusted architectures should be implemented by linking HBOM and SBOM with DBOM¹⁰⁰ to facilitate provenance and traceability and encourage the adoption of standards and best practices.
- Foster collaboration between government agencies and industry stakeholders (Private-Public Partnerships) to develop and promote trusted architectures that support secure protocols for provisioning and market access.

Potential Barriers

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

¹⁰⁰ Digital Bill of Materials consisting of HBOM, SBOM plus info on quality, reliability, and workflow process.

Enabling Recommendation 4.3.1: The government should incentivize multi-stakeholder alliances and collaboration for trusted end-to-end solutions across supply chains.

The federal government should implement incentives to promote collaboration for trusted end to end solutions, including enterprise business processes and workflows cryptographically linking tasks, personas, and handoffs of acids and data and we're participating stakeholders. Incentivizing IoT supply chains to adopt trusted digitalization solutions with cryptographic tracing capabilities is strategic to enhancing national security, stimulating economic growth, and positioning the US as a global leader in IoT technology. The term "trusted" indicates that IoT parts, systems, applications, and supply chains operate as intended and produce data that is not tampered or compromised.

This will allow industries to adopt additional capabilities for tracing design, manufacturing, and enterprise workflows that cryptographically link parts, personas, and data to deliver traceable products and IoT systems that function and perform as originally intended. The federal government's active role in promoting these capabilities can contribute to more resilient supply chains and valuable end-to-end solutions, that benefit societies and industry ecosystems. By encouraging industries to pursue trusted digitalization solutions, the government can strengthen national security and accelerate adoption and growth to:

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

Implementation Considerations

- Offer tax credits, grants, or other financial incentives to companies that market electronics products with traceable parts Country of Diffusion and Country of Origin¹⁰¹, provenance, and journey in the supply chain.

¹⁰¹ Country of Diffusion where a part is fabricated and Country of Origin where the product made of parts is assembled.

- Require contractors and suppliers to adhere to specific security and traceability standards when bidding on government contracts, particularly for critical infrastructure.
- Establish a certification process for electronics and IoT products that meet security and traceability standards to improve trust in value chains, linked to cybersecurity labels.
- Engage industry associations and other stakeholders to develop best practices and guidelines for trusted electronics and IoT systems development and supply chain.

Potential Barriers

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

Enabling Recommendation 4.3.2: Support collaborative IoT platforms that align stakeholder business incentives.

The government should support collaborative IoT platforms that align the business incentives of stakeholders to foster innovation, enable orchestration and while harnessing the power of network effects to enhance security, user experience and drive economic growth. Collaborative IoT platforms encourage industry-wide innovation, leading to the development of cutting-edge technologies and solutions. These platforms streamline device management, data exchange, and interoperability, reducing operational complexities. By aligning business incentives, stakeholders are motivated to prioritize cybersecurity resulting in safer IoT environments. IoT-driven industries will experience substantial growth, creating jobs, and contributing to economic prosperity. This approach will significantly benefit the nation by enhancing security, improving the user experience, and driving economic growth.

Implementation Considerations:

- Standardization: Define industry standards to ensure compatibility and interoperability across IoT platforms.
- Public-Private Partnerships: Foster collaboration between government agencies, businesses, and academia to drive innovation.
- Data Privacy and Confidentiality: Establish robust data protection regulations to build trust and protect user data.
- Incentive Mechanisms: Create incentives like tax benefits and grants to motivate businesses to align their incentives with IoT platform goals.
- Monitoring and Evaluation: Implement a monitoring system to track progress, security, and the impact on economic growth.

Potential Barriers:

- Privacy Concerns: Balancing data sharing with privacy protection can be challenging.
- Fragmentation: Lack of standardization and coordination among stakeholders may hinder platform adoption.
- Cybersecurity Risks: Rapid IoT growth increases the risk of cyber threats.
- Resource Allocation: Ensuring adequate funding and resources for IoT platform development and governance.

Enabling Recommendation 4.3.3: The government should encourage the use of digital threads for connected supply chains.

Promote the use of digital threads¹⁰² among enterprises in disaggregated supply chains, to enable the creation of connected IoT supply chains. Leverage digital threads of data across value chains to enable marketplaces of trusted data producers and data consumers.

The government should support the development of digital threads across supply chains by incentivizing companies to digitalize their workflows, link their internal data IDs and Bills of Materials to identifiers and data to create trusted (certified) digital threads that can enable trusted digital marketplaces of producers, consumers, and platform-based business ecosystems. Business platforms for data exchange can have a significant impact on improving supply chain visibility, efficiency, security, and growth. Digital threads may extend from supply chains to the field use of IoT devices and connected ecosystems of data marketplaces.

¹⁰² Digital flow of data connecting business processes products assets and bill of materials in a value chain. For the electronics value chain the digital thread includes of HBOM, SBOM and other Digital Bill of Materials (DBOM)

Linking digital threads for HBOM, SBOM, DBOM across supply chains can accelerate adoption in ways that protect proprietary IP while enabling new digital marketplaces. Digital threads enable marketplaces of data producers and data consumers, creating new business opportunities for revenue streams that will fuel the digital economies. This increased end-to-end visibility of a product's lifecycle and supply chain transparency can help reduce risk of cyberattacks, counterfeiting, and product recalls. Companies that adopt a digital thread can improve supply chain efficiency, reduce costs, manage vulnerabilities, increase differentiation, and promote innovation.

Implementation Considerations

- Develop educational and training programs to help businesses implement digital threads. Establish guidelines for creating a digital thread, including standards.
- Incentivize companies to digitalize their workflows through tax credits, grants, or subsidies for investing in digital technologies. Encourage PPP collaboration.
- Leverage the Cybersecurity labeling program to create a digital trail for BOM (DBOM, HBOM, SBOM, Security keys, certificates etc.) for IoT systems by vertical market.
- Provide funding for research and development of methods and standards to facilitate development of best practices and guidelines for implementing digital threads.

Potential Barriers

- Resistance from businesses to adopt new digital technologies and workflows. Upfront costs of digitalization may be prohibitive for SMBs, even if the ROI justifies them.
 - Reluctance to share data due to concerns about intellectual property and competitive advantage. The digital thread should allow sharing of metadata information and data at the producer's discretion.
 - Different industries may have varying requirements for digital threads, making it challenging to establish common standards and overcome concerns around data privacy, security, and interoperability.
1. Foster collaboration among federal agencies, industries, and value chains to accelerate adoption with a unified approach to IoT supply chain security and transparency.

Consider the potential impact on domestic and international trade policies and the importance of ensuring that any subsidies are distributed equitably across various stakeholders.

Enabling Recommendation 4.3.4: The government should facilitate the creation of business ecosystems that enable new business models and revenue streams

As data produced in connected supply chains and during field or IoT devices and becomes the “*new gold*”, the government should raise awareness about the value of digital or data business ecosystems and trusted data-driven digital threads that will enable new business models.

Digital networks of interconnected businesses, technologies, and platforms can leverage synergies to enhance existing products, enable digital twins and drive growth through XaaS⁴⁹ business models.

The federal government should raise awareness about the *New Gold*, Data Monetization Strategies, Data Analytics for Insights, Trusted Data Marketplaces, Platform-based Business Ecosystems, Network effects, Digital Thread of Data in connected supply chains, Data Regulations, and tools for Monitoring and Managing Data Marketplaces.

This includes:

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

Implementation Considerations

- Develop educational programs for businesses and individuals. Raise awareness about business ecosystems through public campaigns, conferences, and workshops.

- Provide funding and incentives for data-driven ecosystem and solutions PPPs with industry leaders, innovative startups, and academic institutions.
- Foster the development of orchestrated platform-based business ecosystems supporting networks effects by providing incentives and resources to businesses.
- Encourage collaboration and innovation by promoting the value network effects. Provide tools and resources for monitoring and managing data marketplaces.

Potential Barriers

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

Federal Considerations

- Ensure fair competition and prevent monopolies. Balance the need for data confidentiality and security with the benefits and value of data-driven business ecosystems for data management and sharing.
- Encourage the private sector to invest in data-driven economic growth. Promote collaboration between government, industry, and academia. Promote collaboration businesses while ensuring fair competition.
- Ensure transparency and visibility in data marketplaces by encouraging the use of data analytics to improve government operations and services.

Enabling Recommendation 4.3.5: The government should promote consistent levels of IoT device hardware and software identity documentation information included in trusted digital threads for Software IoT supply chains.

Establish a centralized IoT Device Registry to standardize due diligence, enhancing IoT device validation, security, and maintenance. This promotes transparency, sustainability, and economic growth by fostering accountability, efficient IoT management and new business models.

The Federal government should initiate the development of a centralized IoT Device Registry to standardize due diligence processes for IoT devices, capturing vital data

points necessary for their validation, security, and maintenance. This comprehensive approach aims to enhance transparency, sustainability, and economic growth by fostering innovation, accountability, and efficient management within the IoT ecosystem. The proposed registry would facilitate collaboration, risk mitigation, and timely vulnerability notifications, benefitting businesses, the environment, and the broader digital economy.

Implementation Considerations:

- **Regulatory Framework:** Develop regulations to mandate IoT device manufacturers to provide comprehensive Software Bills of Materials (SBOMs) during firmware and OS updates.
- **Centralized Database:** Create a centralized database to correlate vulnerable software and hardware components with IoT modules and devices, updated regularly.
- **Device Management Systems:** Implement reporting mechanisms for device management systems, over-the-air updates, and remote monitoring services.
- **Subscription Model:** Enterprises would pay a subscription fee to register their devices, ensuring continued access to registry information.

Potential Barriers:

- **Cost-Effectiveness Perception:** Some industries may question the cost-effectiveness of securing IoT devices, but the reality is that these devices are prime targets for botnets, which contribute to denial-of-service attacks and provide entry points for infiltrators into enterprise networks.
- **Regulatory Mandates:** High-risk industries, including critical infrastructure and healthcare, are already experiencing negative effects from IoT-related issues and are subject to new regulatory mandates. Encouraging these sectors to adopt comprehensive documentation can be challenging but is essential for security.
- **Standardization Challenges:** Coordinating with various stakeholders and IoT manufacturers to adhere to standardized practices and SBOM requirements may encounter resistance.

IoT Leadership / Government capabilities

Objective 5: The United States is recognized as an international leader in the innovation, deployment, and operation of IoT technology. Actions by U.S. government leaders set an example for private sector stakeholders and international partners.

Establish Government Capabilities

Key Recommendation 5.1: The federal government should consider incorporating secure and updated IoT applications and systems into its own facilities, assets, and operations.

Enabling Recommendation 5.1.1: The government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

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

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

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

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

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

such as the National Cyber Labeling Program for Consumer IoT versus Energy Star on appliances.

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

Owners of buildings used by federal organizations should, at a minimum, use basic cyber hygiene best practices (i.e., changing default passwords, segmentation of networks by using items such as firewalls, installing patches) as directed within requirements. NEMA has developed a cyber hygiene best practice document for end users that is available at the following URL (<https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2>)

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

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

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

Enabling Recommendation 5.1.2: The government should consider the development of Smart City and Sustainability Extension Partnerships (SCSEP).

IoT can bring great economic and societal benefits to our cities, but specific smart city and sustainable infrastructure expertise in industry is limited, unevenly distributed, and fragmented. Some cities and agencies also lack the tools and resources, and even smaller cities and agencies may be even more constrained. Municipalities and agencies may not have the budget, the empowerment, or the ability to engage the necessary resources.

A different way to engage these resources is needed. The public procurement processes to engage private sector resources are burdensome. A SCSEP similar to existing partnerships (e.g., MEP, USDA) would be a worthwhile investment, and would provide an improved model over the current public procurement process to engage private sector resources.

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

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

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

Enabling Recommendation 5.1.3: The government should fully fund existing IoT research, development, deployment and demonstrations.

We recommend Congress complete the funding procedure for vital IoT related R&D and deployment work already approved and taking place throughout the federal government. That means fully funding the critical investments that a bipartisan Congress has supported through the bipartisan Chips and Science Act, and through the bipartisan Infrastructure Act, and that these be fully funded at the levels Congress authorized. These research investments span multiple areas, including semiconductors and sensors, to the connectivity and interoperability

methods that connect them, to the infrastructure and systems that allows them to operate, automate and sustain itself at scale.

In addition, the U.S. Government should fully fund science agencies that are doing work in these areas through important IoT-related programs such as those at ARPA, DOE, NSF, and DOT. It may also require a more significant role for OSTP in IoT-related research. Failure to do so will slow down government efforts and cut our IoT opportunity short.

Leading by Example: Improved Use of IoT in Federally Funded Projects

Key Recommendation 5.2: The government should lead by example by promoting and enabling the use of IoT in those projects that are funded in full, or partially, by federal offices.

[Need additional text]

Enabling Recommendation 5.2.1: The 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. IoT tools and technologies play a central role in managing energy efficiency.

Specific examples include smart thermostats that can regulate room temperature data, intelligent lighting systems that are enabled to be turned on and off as needed, and smarter buildings that use IoT sensors to send data on energy consumption allowing it to be analyzed further so the building can more efficiently manage its air conditioning, water, heating, or lighting.

Implementation might include adoption of building and energy codes that include language like automated demand response technologies, EV Ready, EV Capable, etc. Also look at incorporating energy savings through energy performance contracts and examination of building energy use benchmarking. The GSA FAR specifies energy efficiency requirements for procurement in federal owned and operated buildings.

Potential barriers: Funds such as high costs to scale conversion to energy efficiency. Supply chain issues (e.g., in distribution transformers, mining limitations for batteries,

etc.) that manufacturing is trying to overcome. Legacy equipment and existing equipment (e.g., boilers, furnaces, etc.) that have a long lifetime.

Enabling Recommendation 5.2.2: The government should consider the specification and utilization of IoT and “smart” technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.

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

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

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

Implementation Considerations: While it is easy to say, “you shall incorporate IoT technologies”, it is more difficult to specify what IoT technologies should be acceptable to be used. Some concrete and specific IoT applications should be defined

for inclusion in the project and funding requirements, based on project types. Without this list, the contractors will be left on their own to interpret what is meant by IoT, and in some cases, will do the minimum possible just to comply or comply with things that meet the definition but not make any sense. Additionally, a broader vision and understanding of how IoT is to be incorporated, used and operated is needed by project owners, governments and operators in order to develop the requirements and specifications.

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

Leverage Federal Grants And Programs To Improve IoT Technology Use

Key Recommendation 5.3: The government should consider new financial models for sustaining and supporting programs when considering IoT project feasibility.

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

IoT enables new business and operating models. Economic service models to assist could include extended funding for O&M for select applicants (i.e., rural, tribal, small towns, etc.), encourage regional cost sharing for multiple cities in a region to apply as one, and encourage innovative models (i.e., corporate, sponsorships).

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

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

Enabling Recommendation 5.3.1: The government should encourage other models to help select adopting organizations sustain and support in evaluating IoT project feasibility.

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

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

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

Enabling Recommendation 5.3.2: The government should consider “student loan forgiveness” programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies.

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

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

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

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

Enabling Recommendation 5.3.3: The government should consider developing programs and grants to allow underserved and less developed communities as well as rural areas to adopt smart transportation technologies.

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

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

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

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

Leading the Way for IoT Adoption in Agriculture

Key Recommendation 5.4: The federal government should implement sector-specific actions to further promote IoT adoption in the Agriculture sector.

[text needed]

Enabling Recommendation 5.4.1: The government should develop a comprehensive strategy for agricultural IoT.

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

stakeholders, such as farmers, technology providers, industry experts, and research institutions, to ensure broad consensus and commitment to its implementation.

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

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

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

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

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

Enabling Recommendation 5.4.2: The government should consider fully funding the deployment of a “farm of the future” setup in every land grant university nationwide. This nationwide test-farm IoT network should span different forms of agriculture, including, but not limited to broadacre, horticulture, livestock, and aquaculture.

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

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

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

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

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

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

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

Enabling Recommendation 5.4.3: The government should actively promote and support the adoption of Generative AI applications for agricultural IoT, with the aim of improving decision-making, optimizing resource utilization, and enhancing productivity in the agricultural sector through innovative and data-driven solutions.

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

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

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

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

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

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

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

Enabling Recommendation 5.4.4: The 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.

[Note that the use of drones was primarily discussed for use in an agricultural context, although it could be used for many of the topics described including sustainability, transportation and environmental monitoring. We should add that to the prose herein.]

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

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

Implementation Considerations: It will be necessary to involve all stakeholders: drone equipment manufacturers, communications providers, among others need to

be involved. This should be accompanied by expanding access to education and training: particularly on safety aspects related to drones.

The adoption of drone technology can have substantial impacts on the nation's key sectors. In agriculture, for instance, drones equipped with advanced sensors can help in efficient farm scouting, pinpointing areas of pest infestations, disease, or poor irrigation. This not only enhances productivity but also promotes precision farming by reducing the excessive use of chemicals. For the energy sector, drones can monitor electric grids and detect faults or required maintenance, helping to prevent power outages and ensuring a stable power supply. Similarly, drones can be utilized for environmental monitoring of forests, aiding in early detection of wildfires and thus mitigating their devastating effects. Drones can also be actuated to perform tasks such as spraying pesticides or fertilizers in farming, reducing human exposure to harmful chemicals, and ensuring that the process is accomplished with greater precision and less waste.

The Internet of Things (IoT) is instrumental in accelerating the adoption of drone technology, including the use of drones in Non-Line-of-Sight (NLOS) operations. IoT facilitates seamless communication and data exchange over the Internet, enabling real-time data collection and analysis, remote control of drone operations, and automation of tasks. This is particularly beneficial for NLOS drone operations, which require sophisticated data communication and handling capabilities. Drones operating beyond visual line of sight can cover larger areas and perform tasks in remote or inaccessible locations, expanding their utility in sectors such as agriculture, energy, and environmental monitoring. However, leveraging the potential of NLOS drone operations hinges on the establishment of appropriate regulatory guidance for IoT in the drone industry. Such regulations can address critical aspects such as data security and privacy, airspace usage, safety, and accountability for NLOS operations. By providing clarity and assurance, these regulations can stimulate innovation and investment in drone technology, contributing significantly to the economy and society at large.

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

Enabling Recommendation 5.4.5: The government should facilitate development of connectivity policies and programs.

Needs include:

- Broadband service at the farmhouse greater than 25/3 Mbps
- Symmetric connectivity of at least 100/100 Mbps that supports high bandwidth precision agriculture use cases (video, imagery, automation and control, etc.)
- Last acre IoT connectivity service that addresses coverage, terrain diversity, evolving use cases, and foliage/canopy interference

Today's broadband and connectivity infrastructure and capabilities are insufficient to support current and future precision agriculture needs for a variety of reasons.

- While many agriculture IoT use cases are low bandwidth, intermittent communications applications (e.g., soil moisture, animal health monitoring, etc.), future farming required the processing of low latency, real time data, support automation applications, and high bandwidth applications. Examples are drone imagery and remote viewing/monitoring and remote operation of automated farm machinery.
- Some farming applications, such as imagery and video, require high upload speeds from device to the cloud data center. For example, drone imagery needs to be uploaded to the cloud for analysis and processing. These files are very large and need a high bandwidth connection.

Implementation Considerations

- Existing broadband infrastructure grant programs for rural areas (BIL, USDA) should account for more high bandwidth, symmetric connections. These types of connections support other non-agriculture applications, such as telehealth, remote education, and manufacturing (factories) in rural communities.
- There is no one-size-fits-all approach due to the large areas of coverage, terrain diversity and application types. Addressing this requires multiple technologies to be considered and used, including satellite service, terrestrial wireless (licensed and unlicensed), fiber, and other approaches like TV white space, etc.

Barriers

- Unfavorable economics and ROI may preclude terrestrial mobile operators from establishing services in rural communities
- Signal blockage due to foliage and tree/plant canopies from some plants may make some types of connectivity services less feasible
- Terrain diversity and wide areas of coverage may make last acre connectivity challenging

- FCC definition of broadband as 25/3 needs to be updated for modern and future applications and services

Enabling Recommendation 5.4.6: The government should support and promote industry and SDO efforts to address interoperability of agricultural systems and machinery.

Farms have a variety of equipment and machinery from different manufacturers that can't communicate or exchange data with each other, each with its own data formats and languages. The agriculture industry model is to develop s/w and devices in proprietary formats.¹ This lack of interoperability hinders data sharing, automation of processes, and timely diagnosis and analysis of problems to create positive outcomes. In addition, costly manual labor is required to extract the data for use.

Implementation considerations

There are a variety of SDOs and industry associations that are addressing small parts of this much broader problem. However, broader efforts involving the major equipment manufacturers are needed

Barriers

The industry model is to build their own ecosystem. Equipment manufacturers have limited incentives to fully address interoperability, or they may form their own "walled garden" ecosystem.

Enabling Recommendation 5.4.7: The government should facilitate small farm/ranch adoption of IoT technologies.

Small farms (< \$350,000 GCFI)² are 90% of all U.S. farms (~1.8 million farms), own 49% of farmland, but represent 20% of production. They operate with <10% margins. Because of their small scale and low margins, they are cash flow constrained and do not have the capability to buy IoT or smart equipment, even if they want to.

Implementation considerations:

- Offer grants and subsidies for purchase. Since these small farms operate on low margins, they have limited upfront cash available for investment is a critical barrier to adoption.
- Tax credits offer another way to incentivize purchase but may not be a viable option for those small farms that do not have the upfront cash to purchase and use.
- Use of Cooperative Extension Offices and resources for IoT data analytics and other technical support. In order to ensure that IoT is being used, additional

support (beyond what the IoT vendor provides) is necessary to help the agriculture producers get the value out of the data collected so they can optimize outcomes.

- Need to define and specify what subset of IoT devices and solutions would be addressed by this.

Barriers

- Not all of these small farms may have the proper infrastructure (connectivity, etc.) to take advantage of IoT, even if this program was to be offered
- Small farms may not have any awareness of IoT and may not take advantage of this program if offered.

Enabling Recommendation 5.4.8: The government should support enactment of federal “right to repair” legislation to address the inability of agricultural producers to service their smart equipment.

Smart equipment cannot be fixed by farmers. In many cases, it required servicing by the equipment dealer technicians. These repairs are expensive and may take a long time to get fixed. These may occur at sensitive times for farmers who can't afford the wait, such as during harvest season. Today, farmers are getting around this by purchasing “hacked” software from Eastern Europe or buying older non-smart equipment that they can maintain and repair themselves.³

Implementation considerations

- Current legislation has been introduced - the Agricultural Right to Repair Act⁴ - review to ensure that precision agriculture and IoT needs has been addressed in legislation

Barriers

- Manufacturer resistance
- Individual states are enacting state-level “right to repair” laws

Enabling Recommendation 5.4.9: The government should facilitate the development of IoT data confidentiality guidelines for agricultural IoT systems, and manufacturers of “smart” and IoT-enabled agricultural machinery and systems.

Producers are concerned with who and how their data is used. 77% of producers are concerned about who accesses data, 67% will consider how their data is used when making purchase decisions, and 61% are concerned that companies use their data to influence market decisions.⁵

Implementation Considerations: Integrate with privacy framework and regulations being considered

Barriers:

- Each IoT solution provider may have their own privacy and data usage policies and guidelines, which may be conflicting
- Manufacturer and solution provider resistance

[Editors' note: Recommendations 5.5 through 5.8 (specific actions for manufacturing, construction, insurance, and retail) have been removed and will be integrated into new items below. We will renumber after the next round of Board feedback.]

Leading the Way for IoT Adoption Through Smart Cities

Key Recommendation 5.9: Preliminary Text: The government should implement specific actions to further promote IoT adoption through smart cities.]

Enabling Recommendation 5.9.1: The government should facilitate and support the development and use of smart city and sustainable infrastructure reference models.

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

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

Implementation considerations: The NIST GCTC has already established a structure and model to create, engage and support industry/academia/government partnerships. This effort should consider inclusion of public entities such as counties, states, and other regional agencies and utilities. There is not a one size fits all “reference model and architecture”. There is one for small cities, large cities, as well as “smart regions”, utilities, buildings, etc. Key participants in developing the reference model include government (states), federal, industry (and industry and standards bodies), and academia. There are various efforts around models and standards. Consider projects that are funded using federal money to incorporate the use of these reference models. NIST has developed the Smart City Framework v1.0 (<https://pages.nist.gov/smartcitiesarchitecture/>) and that is a starting point for building on something that may be more usable to city planners.

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

Enabling Recommendation 5.9.2: The government should facilitate opportunities for adoption and equity of benefits of IoT and smart city technologies for local governments (cities, counties), regional entities (water districts, sanitation districts, air quality districts, etc.) and utility companies.

This may include:

- Funding regional or state programs that support municipalities and local governments in strategy and roadmap development and integration of smart city technologies into city vision, infrastructure and operations.
- Project grants for smart city and related innovations pilot projects and deployment projects
- Consideration and specification of IoT applications into the design, construction and operation of federally funded infrastructure projects (e.g. highway projects, street improvements, etc.)
- Facilitate smart city grants for communities that have received broadband grants to build on new connectivity infrastructure

Justification

While cities, regional entities, and utilities may want to do smart city projects, a number of factors is hindering this, including:

- the lack of funding for pilots and projects
- a lack of leadership awareness, vision and planning for these innovations
- A lack of project owner specification for IoT

Enabling Recommendation 5.9.3: The government should facilitate smart community opportunities and adoption of IoT for those rural communities that have broadband infrastructure, have received broadband infrastructure funding or have completed broadband infrastructure build-outs.

Examples of smart community IoT opportunities include home healthcare monitoring, agriculture, natural resources and environmental monitoring, home energy monitoring, etc. Examples of approaches include:

- Coordination with federal agencies to drive community awareness of IoT opportunities, and support programs that encourage industry participation
- Project grants for community related IoT projects and deployment projects (e.g. environmental monitoring, etc.)
- Consideration and specification of IoT applications into the design, construction and operation of federally funded rural infrastructure projects (e.g. highway projects, street improvements, energy transmission lines, etc.)

Rural communities lack many of the same resources, services and amenities that residents in urban areas benefit from. The lack of infrastructure, low population densities, private sector investment and other factors contribute to the urban/rural divide. For example, many rural areas are considered medical deserts with limited number of healthcare providers and facilities. As a result, healthcare access inequities exist. Telehealth and home healthcare monitoring are IoT-enabled services that can alleviate some of these inequities.

Enabling Recommendation 5.9.4: The government should facilitate federal adoption of IoT and smart city technologies within its facilities, including government buildings, military bases, campuses and other facilities. [For Board Review - Proposed by Benson] [This could also go in 5.2]

The federal government is the largest landlord and owner of properties across the United States. These facilities do not incorporate IoT technologies which could provide a variety of benefits, including energy savings, safety, resilience, etc.

Enabling Recommendation 5.9.5: The government should support and promote industry and SDO efforts to address interoperability of smart cities (including smart buildings, energy and utilities, traffic, etc.). [For Board Review - Proposed by Benson]

Interoperability challenges are a major barrier to maximizing the value of IoT and smart city technologies. Disparate IoT devices and smart city systems have limited to no ability to communicate with each other and other city systems. This limits the ability of the city to monitor conditions, automate operations, respond quickly, effectively and efficiently.

Enabling Recommendation 5.9.6: The government should facilitate small to medium city adoption of smart city technologies. [For Board Review - Proposed by Benson]

Considerations include:

- Develop smart city grants targeted for smaller communities and rural communities [linkage to existing recommendation]
- Develop smart city grants for communities that receive broadband infrastructure funding (BIL, USDA, etc.), to encourage them to build on their infrastructure investments
- Consider program grants that allow these communities to sustain the operation and maintenance of smart city technologies beyond the initial project funding (for initial acquisition, installation and operation). [linkage to existing recommendation in smart cities/sustainable infrastructure]
- Consider creating smart city innovation extension partnerships (modeled after MEP and agriculture extension offices) to provide the smaller cities with the technical and innovation expertise, resources and capabilities to design, operate and innovate with smart city technologies [linkage to existing recommendation in smart cities]
- Facilitate workforce development to support innovation, IoT and digital technologies in smaller cities (including municipalities, regional entities, and utilities)

There are 1300 cities that have less than 250,000 people. These cities lack the funding, expertise and resources to implement, operate and maintain smart city technologies. At the same time, these smaller cities have needs that are different from their larger city counterparts and may require grants that are more aligned to their needs.

Enabling Recommendation 5.9.7: The government should facilitate cybersecurity in IoT in smart cities.

Considerations include:

- Expand recognition and promotion of existing standards, programs, and conformity assessment schemes that facilitate IoT cybersecurity in smart cities. Cybersecurity postures vary depending on the type of product produced and its intended market audience and use, thereby complicating the creation of a comprehensive or one-size-fits-all solution in relaying the security level of a product and it's important to recognize what each sector within a smart city is already doing to address IoT

- Facilitate workforce development programs to increase pool of IoT cybersecurity trained resources for smart city and utility on both the solution provider side and city/utility (buyer) side

City and utility infrastructure are attractive targets for cyberattacks. The number of ransomware attacks on cities has been steadily growing. Similarly, the introduction of IoT into utility OT infrastructure creates new attack surfaces and vulnerabilities to formerly air gapped systems. Cities and utilities lack the resources and capabilities to defend and mitigate.

Enabling Recommendation 5.9.8: The government should facilitate equity in realization of smart city benefits.

This may include:

- Smart city project grants for underserved and rural communities, including those applications where underserved communities are disproportionately impacted (e.g. environmental monitoring, healthcare, public safety, etc.)
- Increase access to broadband services and affordability
- Workforce development opportunities for residents of underserved and rural communities for the new IoT and digital jobs to be created

Benefits of IoT and smart city technologies are not available to all members of a community. Socioeconomically challenged and rural communities may not have the broadband infrastructure, or have limited resources to implement and operate smart city technologies. The new jobs created by IoT, smart cities and digital transformation require skills and education that members of underserved communities may not be able to develop. Some services enabled by these technologies require smart phones and Internet service to access, which some community members may not have, while others are offered in ways that cannot be accessed by residents due to language barriers, digital literacy skills, etc.

Leading the Way for IoT Adoption for Public Safety

Key Recommendation 5.10: The government should implement specific actions to promote IoT adoption that will improve public safety.

Enabling Recommendation 5.10.1: The government should create a stockpile of public safety IoT devices that is available for immediate access.

[Note: The Board recommended this for removal. To be discussed at the January meeting.]

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

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

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

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

Leading the Way for IoT Adoption for Health Care

Key Recommendation 5.10: The government should implement specific actions to promote IoT adoption in the health care industry.]

Recommendation HC1: Support and promote industry and SDO efforts to address interoperability of medical and healthcare devices and systems.

Justification: Interoperability challenges are a major barrier to maximizing the value of IoT in healthcare. One of the primary challenges in achieving interoperability in healthcare IoT and IoMT is the inherent fragmentation of the ecosystem. Healthcare facilities often deploy a variety of devices and systems from different manufacturers, each operating on proprietary protocols and standards. In addition, consumer wearable health trackers have limited interoperability, depending on the device, standards and integration capabilities. This lack of uniformity creates silos of data, with disparate IoT devices and systems having limited to no ability to communicate with each other. Besides hindering the free flow of information between devices and systems, this lack of interoperability limits the ability of the systems with multiple devices to monitor patient conditions, inform and support diagnoses, and provide effective and accurate individualized treatment. The lack of interoperability among these devices poses a significant challenge to the seamless integration of IoT in healthcare.

The lack of interoperability is manifested in many forms, including:

- Diverse communication protocols
- Disparate data formats and structures. Diverse coding systems, data models, and terminology standards are prevalent across healthcare organizations, making it challenging to ensure consistency in data interpretation and exchange.
- Legacy systems that may not be inherently compatible with IoT and IoMT technologies.
- Inability to integrate and interoperate with electronic health record systems

Recommendation HC2: Facilitate cybersecurity in IoT in smart medical devices and equipment, including wearables, in-home devices, community IoMT systems, and in-clinic systems

- Expand cybersecurity trust mark program to include IoT devices and modules used in a variety of healthcare systems and applications
- Facilitate workforce development programs to increase pool of IoT cybersecurity trained resources for healthcare industry on both the solution provider side and care provider (buyer) side
- Consider development of programs, resources and incentives to help healthcare providers migrate away from those vulnerable legacy equipment and devices that cannot be patched, or upgradeable, or were not subject to compliance with section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act)
- Develop a plan to audit, inspect and update healthcare and medical IoT devices, and the networks they operate in used in federally owned or funded health facilities (e.g., VA medical facilities, military medical facilities, etc.). Replace those legacy devices and equipment that cannot be patched or upgradeable or not subject to compliance with section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act). Verify devices and systems, and practices meet IoT cybersecurity guidance and best practices.

Justification:

Healthcare and medical IoT devices and systems are susceptible to cyberattacks. These cyberattacks not only expose sensitive and personal health data and information, but they could lead to disruption to the operation of the devices and systems, leading to potential injury and loss of life. Areas of healthcare and medical device IoT cybersecurity concerns include:

- Vast attack surface due to the interconnected nature of IoT and IoMT devices. Each connected device represents a potential entry point for malicious actors seeking to exploit vulnerabilities.
- Protecting data in transit and at rest is of concern because the data generated by IoT and IoMT devices in healthcare include sensitive patient information. Encryption is critical to preventing unauthorized access.
- Unauthorized access to healthcare data can have severe consequences, ranging from identity theft to compromised patient care. Robust authentication and access control mechanisms is essential to restrict data access to authorized personnel only.
- Patching millions of IoT and IoMT devices is logistically and operationally challenging. These devices often have a longer life cycle than traditional IT devices, and some lack the capability for regular software updates. Not all device and system owners apply patches and firmware updates.
- Legacy systems and devices that cannot be patched or updated with the latest software to address known vulnerabilities
- Compliance with regulatory frameworks (e.g. HIPAA) can be challenging due to the dynamic and evolving nature of IoT and IoMT technologies.
- Securing endpoints (devices) and gateways against unauthorized access and breaches is critical as they act as crucial points in the data transmission process for IoT and IoMT devices.

Recommendation HC3: Facilitate U.S. government adoption and use of medical and healthcare IoT technologies.

These would include:

- By federal healthcare providers in federally owned or funded health facilities (e.g. VA medical facilities, military medical facilities, Indian Health Service, federal prisons medical centers, etc.)
- Consider programs by healthcare payers (HMOs, PPOs, etc.) that support federal employees to adopt these technologies in the treatment of their patients
- Consider programs by federal healthcare programs (Medicare, Medicaid, the Children's Health Insurance Program, Affordable Care Act) that support qualifying patients to adopt these technologies in the treatment of their patients

- Developing guidance that supports and integrates the use of IoT devices in existing medical services, procedures and supplies codes in Medicare (HCPCS, ICD-10-CM)

Justification

The federal government has a major influence in facilitating the adoption of IoT in healthcare. Directly, and indirectly, the federal government programs provide and support the health of millions of Americans. For example, a number of major healthcare insurance companies (payers) support its 2.951 million federal civilian employees (October 2023). Approximately 1.3 million active duty military in 2022 receive government sponsored healthcare insurance (Tricare). Nearly 45%, or 143.3 million persons are enrolled in, or heavily subsidized by, the big federal health programs: Medicare, Medicaid, the Children's Health Insurance Program (CHIP), and the Affordable Care Act health insurance exchange plans.

Because of the number of people it supports, the government can use its significant influence and scale to use innovation to help improve delivery of services, quality of services, and health outcomes in a way no private insurer can.

Recommendation HC4: Facilitate the resolution of privacy concerns in healthcare and medical IoT

- Support research in privacy enhancing technologies specific to the needs of the healthcare industry
- Consider the incorporation of PETs on IoT technologies used in the treatment of patients in federal government owned medical facilities, and federal supported healthcare programs (Medicare, etc.)
- Incorporate considerations for healthcare in the development of a national privacy framework and regulations

Justification

Privacy matters are a cause of concern and can potentially hinder the adoption and use of IoT technologies in healthcare. Concerns about the information collected and how it is used, as well as the accuracy of the data collected and the ability of the technology to create the correct outcomes. These concerns are wide-ranging and include:

- Securing data from unauthorized access. Personal health data can come from a variety of sources, including clinical medical devices, as well as consumer wearable devices.
- Ownership and consent to use of patient data. The interconnected nature of healthcare IoT devices raises questions about data ownership and the extent to which patients have control over their health information. Obtaining informed consent from patients for the collection, use, and sharing of their data (outside of patient treatment) is a complex process, especially when

considering the numerous devices involved in IoMT and the number of people who could have access to the data (e.g. insurance companies, researchers, etc.).

- Ethical use of data. The extensive data collected by IoT and IoMT devices provide valuable insights into patient health and behavior. However, the ethical use of this data is a concern. Ensuring that data is used responsibly, without enabling discrimination or exploitation, requires robust ethical frameworks and regulations.

Recommendation HC5: Facilitate and support the use and adoption of healthcare IoT in rural communities.

- Facilitate grants to drive healthcare IoT adoption among healthcare providers in those communities that have received broadband grants to build on new connectivity infrastructure
- Coordination with federal agencies to drive physician and patient awareness of IoT in healthcare for treatment

Justification

Rural communities lack many of the same resources, services and amenities that residents in urban areas benefit from. Many rural areas are considered medical deserts with limited number of healthcare providers and facilities. In addition, residents in rural areas tend to be sicker than their urban counterparts, as well as older and more likely to suffer from chronic conditions. In addition, many have limited transit options to go see a doctor on a regular basis.

As a result, healthcare access inequities exist. Telehealth, home healthcare monitoring and consumer health tracking are IoT-enabled services that can alleviate some of these inequities by providing access to healthcare and improving their health outcomes.

Implementation considerations

- Code IoT-enabled services in Medicare to support senior population in rural areas
- Facilitate support from private payers (insurance companies)
- Focus on chronic disease management

Barriers

- Cost of connectivity services (rural residents may have affordability issues)
- Limited connectivity (wireless and fixed broadband service)

Recommendation HC6- Facilitate adoption of IoT among small physician practices (< 50 physicians)

- Consider programs by healthcare payers (HMOs, PPOs, etc.) that support federal employees to adopt these technologies in the treatment of their non-federal employee patients
- Consider programs by federal healthcare programs (Medicare, Medicaid, the Children's Health Insurance Program, Affordable Care Act) that support qualifying patients to adopt these technologies in the treatment of their patients
- Coordination with federal agencies to drive physician and patient awareness of IoT in healthcare for treatment

Justification - Small physician practices make up the majority of physician practices in the United States. However, these practices tend to be less likely to use electronic information than those physician offices with 50 people or more.

Recommendation HC7: Facilitate policies and programs that support the key education and digital skills development for the current and future healthcare workforce.

Including:

- Data analytics and management
- Artificial intelligence
- IoT technologies
- Networking and systems integration
- Cybersecurity
- Installation, maintenance and servicing of IoT systems

Justification

The healthcare industry is undergoing a major digital and technology transformation towards revolutionizing healthcare, including the potential for data led individualized care and treatment. The integration of IoT and digital technologies in healthcare will provide more effective treatment, reduce the impact of a shortage of healthcare labor, and reduce healthcare expenditures. However, a lack of the relevant digital skills and workforce is hindering this transformation of healthcare across all levels, from device development and use, integration into hospital and healthcare systems, to analysis of patient data and development of AI algorithms for treatment and diagnosis.

Implementation Considerations

- Integrate the needs for the development of digital skills and workforce in the National Cyber Workforce and Education Strategy

Recommendation HC8: Facilitate the adoption of AI in IoT in healthcare through improved AI research, development and workforce improvement.

- Support research in the development of trustworthy AI algorithms and tools, including AI explainability
- Facilitate the development of IoT data usage and privacy policies that support the development of AI algorithms [linkage with Debbie recommendation]
- Support workforce development efforts to increase the pool of workers trained in data analytics and AI

Justification

While AI can help automate the analysis of massive amounts of IoT data, and other data collected from health records, its ability to create explainable, beneficial and personalized outcomes specific to the patient that are clinically appropriate, reliable and accurate is a major challenge.

AI algorithms review and analyze data, and make recommendations and in cases requiring autonomous operations, take action. Diagnosing people and identifying treatments for people is complex. Diseases such as cancer are complex, and there is still much to be learned. Furthermore, each person has a different reaction to treatments and what works for one person may not work for another. AI generated recommendations may yield treatment recommendations that lead to adverse outcomes, including injury and death. There are a variety of reasons AI may lead to negative or unintended outcomes, including data that may be outdated, contains bias, or incomplete. The source of the data may be unknown for privacy reasons. While the AI algorithms have been trained on this data, the reasons it led to a specific recommendation may not be explainable and transparent. This leads to a loss of confidence in the AI's ability to analyze the data accurately and reliably.

Implementation barriers

- Data privacy regulations and policies limit what data can be collected, and how it is used
- Lack of workforce trained to develop, test and refine data and AI algorithms

Enabling Recommendation 5.10.1: The government should promote IoT as an enterprise priority, including to healthcare facilities' leadership teams.

IoT should be equivalent in priority for all healthcare stakeholders as is IT infrastructure, cybersecurity posture, or applications. IOTs monitor, detect, inform, and deliver therapies to patients, therefore, they deserve just as much attention and

call out as cloud services, for example. Currently IoMTs are often ignored by healthcare IT organizations, as the responsibility to make decisions and/or purchase the devices is owned by the biomedical engineering department. IoMTs may not undergo strict infrastructure, privacy, and security guidelines as to large capital equipment investments such as MRI scanners.

Implementation Considerations: Applicable Federal agencies including the FDA may use their “bully pulpit” to carry this message to the healthcare industry.

Potential Barriers: Difficulty in changing organizations’ priorities.

Enabling Recommendation 5.10.2: The government should enact HIPAA-like protection for users’ medical data in mobile applications and IoT devices.

Many consumer-grade IoT devices and mobile apps collect users’ sensitive medical data. Consumers tend to believe that this data is protected similarly to medical data in a healthcare facility, but it is not.

Consider medical data as a category for defined data protections.

It should be noted that this Recommendation represents a major change. Many organizations have IoT products but no HIPAA experience. While the direction should be clear, the impact should be understood in advance through study, and the transition period adequate to allow manufacturers to adapt without unnecessary impact.

Implementation:

- Extend HIPAA protections to these classes of devices and mobile apps or enact a similar type of protection.

Barriers:

- Possible resistance from industry manufacturers to restricting the sharing of user data.
- Consequences of major changes in data flow and access rights must be carefully studied before implementation, to avoid industry-wide disruption.

Federal Considerations: Enact HIPAA-like regulations to protect user PHI in consumer IoT devices and mobile apps.

Sustainability / Environmental Monitoring

Key Recommendation 5.11: The government should implement specific actions to promote IoT adoption that will improve sustainability and environmental monitoring.

[text needed]

Enabling Recommendation 5.11.1: The 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.

Benson note: There is a lot of IoT environmental data, such as air quality, water levels, etc. that is collected by a variety of federal agencies. For example, EPA, BLM each collect AQ data for their own purposes. In other cases, water stream data is collected and managed by USGS for cities, counties, and states. This data would be useful to a lot of organizations, communities, universities and other researchers. For example, historical AQ data for a particular area of a city could be used by public health researchers to identify patterns among respiratory health diseases. There are a number of barriers that need to be overcome, including “standardizing” the data so that it would be usable. The different AQ sensors may have different standards, and so one reading in one brand may not correlate with the same reading on another brand, etc.

Enabling Recommendation 5.11.2: The 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) monitors that limit deployment by organizations and municipalities. Furthermore, there is a widespread interest in participatory science (aka citizen science) where communities or individuals are actively engaging in air quality monitoring. While such monitors are vital for particular purposes, large scale deployment of these types of monitoring equipment would be expensive and difficult.

Low-cost air quality sensors enable widespread monitoring for numerous applications and by multiple types of users.

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 regulated air pollutants. Additionally, research should be supported for other emerging chemical of concern. ~~such as optical particle scanning for particulate matter and MOx elements for gases and detection of other emerging chemicals of concern.~~

IoT sensing allows for the effortless collection of data from multiple devices and technical innovation in IoT has emerged in research communities worldwide, which together provide new opportunities for low-cost, high resolution, environmental monitoring. There are numerous applications where these sensors can help the public immediately take steps to protect their health (e.g., in the case of wildfire or smoke events) or provide communities with evidence that there are air quality concerns in their area which they can use to encourage action for improvements. However, wider implementation of such devices in the United States will require the approval and encouragement of the federal government if to be used for regulatory purposes.

- Regulatory grade sensors are expensive, limiting the number that can be deployed. Their purpose is specific to looking at broad air quality of an area and compare against EPA levels to protect health and welfare (epidemiological reasons). This limits the scaling of AQ monitors
- Sensor technology is advancing rapidly (e.g. optical sensors for particulate matter) but there is need for additional research and testing for many existing and emerging air quality pollutants;

- ~~Metal Oxide (MOx) devices are not as accurate as PID instruments; however, are excellent for the purpose of initial reconnaissance of VOC levels;~~
- ~~Optical particle scanning for particulate matter and MOx testing for VOCs are economical IoT technologies which could augment federal FRM FEM monitoring for NAAQS and NESHAP air pollutants;~~
- Gap in local (community) scalable air quality monitoring to support a variety of use cases, including
 - Increasing public awareness of AQ
 - Informing environment and public policy; real time testing of policy impacts
 - Environmental justice work
 - Supplementing regulatory grade sensing with commercial sensors
 - Public health research
 - Construction site emissions monitoring
 - Rapid or emergency AQ monitoring

Implementation Considerations:

The EPA should consider amendments to the Code of Federal Regulations 40 Part 50, to encourage implementation of IoT AQ sensing devices to augment regulatory FRM and FEM Methods for air quality monitoring.

- Need ~~top-down~~ demonstration by EPA and it's State, Local and Tribal partners, as well as concrete policy methods, by which to improve implementation of IoT devices and facilitate the incorporation of this incorporate this data into government data.
- Facilitate research and testing in low-cost sensing technologies for many existing and emerging air quality pollutants
- ~~for criterial pollutants, such optical particle scanning for particulate matter and MOx elements for gases, as well as detection of emerging pollutants of concern.~~
- Facilitate the use of space at federal infrastructure (e.g., post office buildings) and federal assets (e.g., post office delivery vehicles) for locating academic and private sector air quality monitors.
- Facilitate and support research and a program in correlating regulatory grade data with ~~low-cost sensor~~ AQ data
- Push state/city to facilitate the expansion of wireless connectivity to support remote monitoring and sensing in areas not serviced by traditional connectivity (TV white space, satellite, etc.)

Potential implementation barriers:

- Different federal agencies (e.g., EPA, BLM, U.S. Forestry Service) have adopted IoT monitors and different ways and can have different protocols for interpreting the same raw data. Consistent standards for interpreting IoT monitoring data will be needed
- Federal policies take time to be implemented at a state and local level. Funding must accompany IT device related policy statements.

~~The Code of Federal Regulations is changed by request of regulatory agencies. The EPA changes slowly by its nature;~~

Enabling Recommendation 5.11.3: The government should facilitate the expansion of wireless connectivity to support remote monitoring and sensing in areas not serviced by traditional connectivity.

[Note: Recommended for removal. To be discussed at the January meeting.]

The effortless collection of sensing data from IoT devices creates opportunity to provide monitoring in locations and at scale where direct data collection would be cost and labor prohibitive. However, the lack of data transmission in areas not currently serviceable to Internet or cellular limits implementation in areas where sensing could be beneficial.

The federal government oversees communication policy (e.g., the Federal Communications Commission) and influenced the expansion of communication infrastructure.

Implementation Considerations: Consider lower cost and precision opportunities, such TV white space for rural regions

Enabling Recommendation 5.11.4: The government should consider establishing stockpile reserves of IoT monitoring equipment for quick short-term deployment during emergency and catastrophic event scenarios

[Note: Recommended for removal. To be discussed at the January meeting.]

Description:

IoT devices are being develop for mid to long term monitoring of various environment conditions, but the low barriers to cost and deployment create new opportunities to use IoT monitors for assessing environmental conditions after emergency events, such as after fires, floods, industrial accidents.

IoT device deployment can help quickly assess safety concerns through quick deployment with relatively minimal time and effort

Implementation Considerations:

- Consider sharing stockpile across agencies
- IoT devices should be updatable during storage for quick deployment

Potential implementation barriers:

Purchase, storage, and use represent new agency costs

Enabling Recommendation 5.11.5: The government should implement a nationwide IoT-based Water Monitoring Infrastructure) to expand the nationwide water monitoring system, including water treatment facilities.

Develop a comprehensive, nationwide water monitoring infrastructure that leverages IoT technology for real-time, accurate, and cost-effective water quality and quantity data collection. This infrastructure should support data-driven decision-making, address the challenges of water scarcity, contamination, and climate change, and integrate with existing NOAA water models for enhanced forecasting and management capabilities.

Current water monitoring systems are often fragmented, inefficient, and insufficient to address the growing challenges of water management.

IoT technology enables real-time, remote, and continuous data collection, allowing for proactive responses to water-related issues.

Integration with NOAA water models can enhance forecasting and management capabilities, leading to more effective water resource planning and allocation.

Efficient water management is crucial for consumption, agriculture, and industry, ultimately contributing to environmental and economic sustainability.

Implementation Considerations:

Develop a standardized, nationwide framework for water monitoring, including protocols for data collection, transmission, storage, and analysis.

Encourage the adoption of open data standards and APIs to ensure interoperability among different IoT devices, platforms, and NOAA water models.

Allocate resources for research and development of advanced IoT sensors, data analytics tools, and communication networks that can seamlessly integrate with NOAA's existing water modeling systems.

Support pilot projects that demonstrate the potential of IoT in water monitoring and management, as well as the successful integration with NOAA water models, and scale up successful models through federal and state programs, grants, and incentives.

Potential Implementation Barriers:

Diverse geographical, environmental, and regulatory factors may present challenges in the implementation of a nationwide water monitoring infrastructure.

Ensuring data privacy and security in IoT-based systems may require significant investments in cybersecurity measures.

Achieving widespread adoption and integration of IoT-based water monitoring systems with NOAA water models may be met with resistance from stakeholders who are accustomed to traditional monitoring methods.

Enabling Recommendation 5.11.6: The government should utilize IoT Technologies to facilitate carbon transparency across economic sectors.

Promote the adoption of IoT-based solutions across multiple economic sectors to accurately estimate and manage indirect carbon emissions associated with goods and services. By leveraging IoT technologies, greenhouse gas emissions associated with upstream and downstream supply chains (scope 3 emissions) can be measured, collected, and compiled for the manufacturing, transportation, agriculture production, and end-of-life practices for economic activity. Great transparency of scope 3 emission with enable the implementation of effective mitigation strategies and contribute to national and global efforts to reduce carbon emissions.

These actions are particularly important because:

- Greenhouse gas reporting protocols are recently experiencing increased adoption and many of these reporting protocols include greenhouse gas emissions beyond those associated emitted at the company's site (scope 1) and emissions associated with the generation electricity that the company consumes (scope 2). These indirect, "scope 3" emissions can be challenging to monitor since they are distributed across supply chains of products and services a company uses (e.g., the transportation of the company's product)

- Accurate monitoring and estimation of scope 3 carbon emissions across economic sectors can help identify indirect but significant emission hotspots and develop targeted mitigation strategies.
- IoT technologies enable real-time, remote, and continuous data collection, allowing for systematic management of carbon emissions at reduced cost and effort.
- Combining IoT-based monitoring with other estimation methods can improve the accuracy and reliability of scope 3 emissions data.

Implementation Considerations:

- Develop a standardized framework for the integration of IoT technologies in scope 3 carbon emissions monitoring, including protocols for data collection, transmission, storage, and analysis.
- Encourage research and development of advanced IoT sensors and data analytics tools specifically designed for estimating greenhouse gas emissions across supply chains.
- Support pilot projects that demonstrate the potential of IoT in estimating and mitigating carbon emissions across sectors and scale up successful models through federal and state programs, grants, and incentives.
- Provide training and technical assistance to stakeholders in the implementation and maintenance of IoT-based carbon emissions monitoring systems.
- Facilitate collaboration and data sharing among stakeholders, researchers, and policymakers to promote informed decision-making and the development of best practices for emissions reduction.
- Include the use of IoT technologies in grants for carbon emissions monitoring

Potential Implementation Barriers:

The diverse nature of different economic practices and environmental conditions across supply chains may present challenges in the development and implementation of standardized IoT-based solutions for carbon emissions monitoring.

- Achieving widespread adoption of IoT technologies across sectors may be met with resistance from stakeholders who are accustomed to traditional monitoring methods.
- Ensuring data privacy and security in IoT-based systems may require significant investments in cybersecurity measures.

Enabling Recommendation 5.11.7: The government should facilitate and promote the use and integration of IoT technologies to complement and support wide area environmental situational awareness capabilities to monitor and inform on a variety of environmental conditions and hazards in environmentally sensitive areas.

The use of proprietary technologies and systems are common in systems used to monitor various environmental conditions for first responder, scientific research, and safety applications.

The federal government should facilitate and promote the use and integration of IoT technologies to complement and support wide area environmental situational awareness capabilities to monitor and inform on a variety of environmental conditions and hazards in environmentally sensitive areas. Examples of opportunities where IoT technologies should be incorporated include forest monitoring, wildfire monitoring, earthquake detection, flood, air quality, etc.

Many existing environmental monitoring platforms today use proprietary technologies. One example are the stream gauges used by various federal and state agencies, local governments and private water rights owners to monitor water flow conditions to determine river health and warn on flooding situations. Data collected from proprietary systems are not easily shared nor integrated with data from other sources, thus limiting timely analysis and responsive actions.

Environmental situational awareness monitoring is critical to ecological health, public safety and disaster recovery. For example, a dense network of low cost IoT-enabled gas sensors can be used in conjunction with a network of cameras to detect and pinpoint wildfires. Early detection of wildfires in remote forests allows firefighters to direct resources to the initial location, increasing the odds of combating the fire before it becomes widespread. A network of IoT-enabled air quality, earthquake, and other sensors integrated together allow state and regional agencies to build real time situational awareness capabilities to support and plan activities that preserve ecologically sensitive areas, mitigate, respond and recover from natural and man-made hazards.

Implementation considerations:

- Specification of IoT technologies into grants and federal procurements for environmental monitoring and situational awareness
- Collaboration with federal, state and regional agencies to define missions and requirements

- Monitoring of wide areas, especially in areas not monitored before or remote areas, may require new connectivity methods, such as satellite and other approaches

Potential Implementation barriers:

- Wide area monitoring may span multiple jurisdictions and owners who may have different missions, requirements and goals for monitoring that may not be easily met.
- IoT based sensors may be based on different technologies, which may not meet the users application scenarios, performance requirements, and integration needs.
- Owners/jurisdictions may lack the new skills to support, maintain and operate IoT technologies. Skills include integration, data science, cybersecurity, cloud, etc.

Smart Transportation

Key Recommendation 5.12: The government should implement specific actions to promote IoT adoption in Smart Transit and Transportation.

Smart transit and transportation technologies provide an organized, integrated approach to minimizing congestion and improving safety on streets through connected technology. These technologies smooth traffic flows and prioritize traffic in response to demand in real time. They enhance pedestrian, bicycle and vehicle safety and reduce accidents that cause injuries and fatalities.

Enabling Recommendation 5.12.1: The government should promote the development and adoption of policies, procedures and funding methods that can accelerate the adoption of smart, connected, and electrified transportation technologies.

Many of these transportation technologies incorporate the use of IoT. Federal funding can also serve to increase private sector investment.

Greater adoption of smart, connected, and electrified transportation technologies could help in the following examples:

- Incorporation of technologies enabled by IoT: Opportunities for IoT technologies in smart, connected transportation include sensors, cameras, and edge computing devices that can improve safety in things such as vulnerable road users (i.e., pedestrians at crosswalks), traffic intersections, school and work zones. Opportunities for IoT technologies in electrified transportation include

in car systems or mobile apps that can locate charging stations, as well sensors that manage charging stations to gather data about usage and performance, to anticipate maintenance needs, and troubleshoot problems.

- Improving overall traffic safety: Vehicles that have technologies such as Cellular Vehicle to Everything (C-V2X) can communicate basic safety messages and information to corresponding infrastructure and other road users thereby reducing traffic and pedestrian fatalities.
- Reduction in greenhouse gas emissions: The transportation sector generates the largest share of greenhouse gas emissions a big contributor to climate change. Electrification of transportation away from traditional fossil fuels are a viable option for transportation. Also smart, connected transportation can improve traffic flow and reduce congestion which is also better for the environment.

Implementation considerations:

- With the Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act (IRA) the Federal Government is already taking steps to electrify the transportation sector. Funds are being directed to the states to deploy electric vehicle charging stations via the NEVI Formula Program (<https://afdc.energy.gov/laws/12744>). Under the IRA tax credits are available for EVs that are primarily assembled in North America. Its important that this legislation stays in effect throughout its designated time period.
- While the BIL and the IRA are significant pieces of legislation, additional legislation is probably needed to focus on rural communities.
- The Federal Government could set aside easily and readily tappable funding pools year-round for innovation and next-generation technologies. Grants could be set aside for categories that the government deems high importance.
- The Federal Government can leverage innovative procurement technologies like outcomes-based contracting in surface transportation. (https://www.nema.org/docs/default-source/nema-documents-libraries/whitepaper-on-outcomes-based-contracting.pdf?sfvrsn=f3ad2716_2)
- Earlier this year ITS America published the National V2X Deployment Plan which includes a call to action for the federal government, as well as state and local transportation agencies, automotive OEMs, and other stakeholders to install V2X systems for public safety – beginning with signalized intersections, other road

users and selected production vehicles (<https://itsa.org/advocacy-material/its-america-national-v2x-deployment-plan/>)

Potential implementation barriers:

- Time and Cost: The time and cost for this transformation could be considerable. It's important that these initial investments are focused and targeted.
- Education: There is an overarching need to educate local governments and consumers on these new types of technologies (particularly those related to Electric Vehicles) which could be hard and time consuming.
- Supply Chain: The manufacturing industry recognizes the goal from the Administration of Buy America, Build America (BABA) however, there are current constraints meeting domestic content requirements and there needs to be an appropriate ramp-up, phase in period to get to full production. There is also a lack of consistent Buy America, Build America across federal and state government agencies.
- The Electric Grid: States with the most EVs today are already struggling to accommodate large scale charging loads on congested grids, and these constraints will only become a bigger problem as the number of EVs grow. Charging for heavy-duty EVs like trucks and busses is even more challenging to accommodate on the distribution grid since they require far more power in concentrated locations.

Enabling Recommendation 5.12.2: Road Safety and Ultra-Wideband (UWB)-the government should direct the FCC to revisit the regulation that prohibits the use of Ultra-Wideband (UWB) technology from outdoor fixed infrastructure.

The FCC should revisit the regulation, working with industry to determine an architecture that enables outdoor UWB deployment with adequate performance for envisioned use cases including Cellular Vehicle-to-Everything (C-V2X). UWB is a proven technology for highly accurate location estimation between connected vehicles and vulnerable road users (i.e., pedestrians, bicyclists).

A core tenant of Vision Zero (<https://visionzeronetwork.org/>) is that “people will sometimes make mistakes, so the road system and related policies should be designed to ensure those inevitable mistakes do not result in severe injuries or fatalities.”

Many of the smart systems developed for road safety, both for vehicles and vulnerable road users (e.g., pedestrians, bicyclists) are only as good as their location accuracy. For example, to avoid a collision between a vehicle and a pedestrian, the location, speed

and heading of both must be known with good accuracy. However surprisingly today that is not possible, especially in urban areas where the need is greatest. GPS suffers from multipath, RTK is better suited for open areas, smart cameras have limited field-of-view, and inertial sensors cannot recover from an errant starting location estimate.

A proven technology for highly accurate location estimation is available today in smartphones – ultra wideband (UWB). A popular use case today is for a digital key for a vehicle, whereby the vehicle knows the precise location of the UWB-equipped smartphone, and after authentication the car door is unlocked. There are many potential use cases, for example enabling the vision-impaired to navigate crosswalks or subway stations. The technology enables precise location measurement within around 10 centimeters in less than a second with very little power consumption.

UWB supports several modes of operation however the most efficient for smart city and especially connected vehicle is infrastructure mode, where many “anchor” nodes (on streetlights for example) transmit timing information received by mobile “tags”. The tags, installed in vehicles, bicycles and already in phones, calculate their own position, speed and heading constantly as a receiver only. Then communicate that using the method in the application, for example cellular in a C-V2X environment.

Potential Implementation Barriers:

- There are concerns with interference from UWB devices with other licensed devices in the cellular network.
- Until the regulation is revisited the only way for UWB devices to operate would be a waiver granted on a case-by-case basis, that process can be very time consuming.

International Leadership

Key Recommendation 5.14: The government should lead international efforts related to the adoption, implementation, and promotion of IoT.

Enabling Recommendation 5.14.1: The government should 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.

Promoting international collaboration in the drive to adopt IoT technologies across global supply chains presents a unique opportunity to foster the sharing of knowledge, best practices, and resources between countries and regions. The goal is

to spur innovation and accelerate the widespread adoption of IoT technologies in supply chain operations on a global scale. Stakeholders like the United States Federal Government, European Union Commission, and Asian Development Bank can form a global ecosystem that supports the development and deployment of IoT solutions, thereby tackling challenges related to interoperability, standardization, and regulatory compliance.

This international collaboration necessitates the creation of platforms and forums that allow policymakers, industry stakeholders, technology providers, and researchers from different countries to come together. Such platforms could include international bodies like the World Economic Forum, United Nations Industrial Development Organization, and International Telecommunication Union. These stakeholders can engage in a productive exchange of ideas, address common challenges, and explore opportunities for joint projects and initiatives. The outcome of these collaborations could be the development of harmonized regulations, standards, and guidelines that enable seamless integration of IoT systems across borders. This harmonization can foster efficient and resilient global supply chain networks.

International collaboration can facilitate the pooling of resources and expertise to support research and development efforts, pilot projects, and capacity-building initiatives aimed at promoting IoT adoption in supply chain management. Organizations like the World Bank and World Trade Organization can help bridge the digital divide between developed and developing countries, ensuring that businesses worldwide have access to the tools and technologies needed to harness the potential of IoT in their supply chain operations. This collective effort, led by governments actively engaging with international partners and participating in relevant forums and organizations, can contribute to the development of a connected and resilient global supply chain ecosystem that benefits businesses and consumers alike.

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

1. Global nature of supply chains: Modern supply chains often involve multiple countries, making it essential for governments and organizations to collaborate across borders to ensure seamless, efficient, and secure operations.
2. Harmonization of standards and regulations: International collaboration can help develop and promote the adoption of common standards, protocols, and regulations, which can reduce inconsistencies and friction between countries, making it easier for organizations to operate globally.

3. Addressing global cyber threats: Cyber threats are not limited by geographical boundaries; therefore, international collaboration can enable the sharing of threat intelligence, best practices, and resources, improving collective defense against cyber attacks.
4. Leveraging global expertise: Collaborating with international partners allows countries to benefit from the expertise, technologies, and best practices developed by others, leading to more effective and efficient IoT adoption in supply chain management.
5. Fostering innovation: International collaboration can stimulate innovation by enabling the exchange of ideas, knowledge, and technologies among countries, research institutions, and businesses.
6. Building trust: Working together on common challenges can help build trust between countries, which is crucial for the smooth functioning of global supply chains.
7. Addressing social and environmental challenges: International collaboration can help address global social and environmental issues related to supply chain management, such as labor rights, environmental sustainability, and resource management.

Implementation Considerations:

Implementation considerations for promoting international collaboration for supply chain include:

1. Establish bilateral and multilateral agreements: The United States should form strategic partnerships with key countries, particularly those with a strong presence in IoT and supply chain sectors. These partnerships can be facilitated through existing programs like the Technology Collaboration Programme, which supports work of international groups of experts to advance the research, development, and commercialization of energy technologies.
2. Participate in international forums and organizations: U.S. should actively participate in existing forums and organizations dedicated to supply chain management, IoT, and cybersecurity. This could include leveraging the Department of Energy (DOE) Office of International Science and Technology Collaboration's programs such as "Net Zero World" and "Mission Innovation", which allow for global collaborative efforts on clean energy research and technology innovations.
3. Share information and best practices: The U.S. should encourage the exchange of information, threat intelligence, and best practices related to IoT adoption and supply chain security among international partners. The Global Innovation through Science and Technology (GIST) Network, an initiative by the

Department of State, provides a platform for such exchange, connecting entrepreneurs globally and providing access to international angel investors and venture capitalists.

4. Collaborate on research and development: The U.S. should engage in joint research and development projects with international partners, harnessing the expertise of the Technology Collaboration Program to advance the research, development and commercialization of IoT technologies in the supply chain.
5. Promote capacity building: Federal programs like the GIST Initiative can support capacity-building initiatives and programs to help countries strengthen their IoT infrastructure, develop relevant skills, and improve supply chain management practices. These programs assist entrepreneurs in emerging economies through a combination of in-country training, online programming, and access to U.S. experts.
6. Identify key international partners: The U.S. should assess which countries are critical for collaboration based on their role in global supply chains, technological capabilities, and mutual strategic interests. The DOE International Science & Technology Collaboration office could potentially play a significant role in this assessment, given its expertise in coordinating international science and technology strategies and programs.
7. Leverage existing diplomatic channels: Existing diplomatic relationships should be utilized to initiate dialogue and cooperation on IoT adoption in supply chain management. Programs like "Mission Innovation", led by the Department of Energy, already foster international collaboration and could be leveraged to promote IoT-related discussions.

Potential implementation barriers:

Possible barriers to implementing this recommendation:

1. Differing priorities and interests: Different countries may have varying priorities and interests, which could make it challenging to align objectives and collaborate effectively.
2. Trust and data privacy concerns: Sharing sensitive information and best practices may be hindered by trust and data privacy concerns among collaborating countries.
3. Regulatory and legal barriers: Differences in regulations, standards, and legal frameworks may impede collaboration efforts and create challenges in harmonizing policies.

Enabling Recommendation 5.14.2: The government should create internationally compatible data minimization guidance related to IoT devices, aligning with the NIST Privacy Framework and NIST Cybersecurity Framework principles.

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

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

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

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

Small Business Leadership

Key Recommendation 5.15: The government should accelerate IoT technology adoption as well as manufacturing for small businesses and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them.

The federal government should accelerate IoT technology adoption and manufacturing for small business and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. Small businesses and startup organizations who are looking to adopt or manufacture IoT technologies may find it challenging to know where to start or have the resources and knowledge to do so. Federal funding mechanisms and procurements targeted to

them can aid these companies by giving them a resource to help speed and incentivize their adoption.

Enabling Recommendation 5.15.1: The government should accelerate the adoption of IoT technologies manufactured by small business and startup organizations through targeted Federal Government programs, policies, procedures, and funding methods.

The federal government should accelerate the adoption of IoT technologies manufacturers by small business and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. It is particularly challenging for small businesses and startup companies in this sector that have to provide upfront capital and full understanding in successfully navigating opportunities both within the federal government and with federal government support to market externally. The process for these projects can also take many years to bring them from proposal to commercial operation and these companies may not have patient resources.

Small businesses have the primary option of using a channel with existing relationships to cities to make sales which is also unpredictable and not very scalable. This makes it challenging for small businesses and startups. Federal funding mechanisms and procurements targeted to them can aid these companies so they can more effectively compete with larger organizations on RFPs relevant to their business. There are many existing Federal Government programs and policies that support small businesses and startup organizations. Rather than create from scratch, this recommendation advises tapping into these existing programs and have a dedicated IoT technologies track for related small businesses and startups in this space.

Implementation Considerations: The Federal Government could set aside readily tappable funding pools year-round for innovation and next-generation technologies. Grants could also be set aside for categories that the government deems high importance. The Federal Government could fast-track programs for startups and small companies to deploy this technology in pilots. There should be consideration to set up a system to make it easier for startups and small companies to find relevant funding sources like grants and SBIR awards. The Federal Government should encourage local governments to leverage its local startup accelerator network to develop technology and fast-track it to local adoption on successes.

The Federal Government can modify guidelines for grant programs and funding mechanisms already in existence for small businesses to allow for greater incorporation of IoT technologies, examples include:

- The U.S. Department of Commerce, Minority Business Development Agency (MBDA) (<https://www.mbda.gov/who-we-are/overview>)
- DOE Office of Small and Disadvantaged Business (<https://www.energy.gov/osdbu/office-small-and-disadvantaged-business-utilization>)
- National Science Foundation Program for Small Business (<https://www.nsf.gov/funding/smallbusiness.jsp>)

Potential barriers: The time and cost for this transformation could be considerable and small companies or startups may find it hard to continue the process. That is why targeted Federal Government programs and policies could provide greater incentive. There is an overarching need to educate local governments and consumers on these new types of technologies which could be hard and time consuming, especially relevant for small businesses and startups. The manufacturing industry recognizes the goal from the Administration of Buy America, Build America (BABA) however, there are current constraints meeting domestic content requirements and there needs to be an appropriate ramp-up, phase in period to get to full production. Again, this could be particularly relevant for small businesses and startups.

Enabling Recommendation 5.15.2: The government should accelerate the adoption of IoT technologies manufactured by small business and startup organizations.

This can be done via policies, procedures, and funding methods that specifically target them.

The federal government should accelerate the adoption of IoT technologies manufactured by small business and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. It is particularly challenging for these types of manufacturers in this sector that have to provide upfront capital, access, and knowhow, before hopefully being selected as a result of an RFP. The process for these projects can also take many years to bring them from proposal to commercial operation and these companies may lose both funding, ability, and interest in that time frame.

Small businesses IoT technology manufacturers have the primary option of using a channel with existing relationships to local governments to make sales which is also unpredictable and not very scalable. Federal funding mechanisms and procurements targeted to them can aid these companies so they can more effectively compete with larger organizations on RFPs relevant to their business.

Greater adoption of IoT technologies manufactured by small businesses and startups could help in the following examples:

- Incorporation of technologies enabled by IoT: Opportunities for IoT technologies are manufacturers by small business and startups across the IoT. For example, in smart, connected transportation these technologies include sensors, cameras, and edge computing devices that can improve safety in things such as vulnerable road users (i.e., pedestrians at crosswalks), traffic intersections, school, and work zones. Opportunities for IoT technologies in electrified transportation manufactured by small businesses and startups include in car systems or mobile apps that can locate charging stations, as well sensors that manage charging stations to gather data about usage and performance, to anticipate maintenance needs, and troubleshoot problems.
- Greater competition across IoT markets: Incentivizing small businesses and startups to bid on projects and deploy their technology will increase their market penetration and provide end-users more technology options. This would lead to greater competition in selected markets providing end-users the ability to select manufacturers based on several factors such as cost, quality of products manufactured, service, and innovation.

Implementation considerations:

- The Federal Government should set aside fast-track programs for startups and small companies to deploy this technology in pilots.
- The Federal Government should set up a system to make it easier for startups and small companies to find relevant funding sources like grants and SBIR awards and RFP opportunities.
- The Federal Government should encourage local governments to leverage its local startup accelerator network to develop technology and fast-track it to local adoption on successes.
- The Federal Government can work with the national chamber of commerce, rotary clubs, small business associations, start-up accelerators/incubators, state partnership programs to help identify relevant IoT manufacturers to support and get input on the programs.
- The Federal Government can modify guidelines for grant programs and funding mechanisms already in existence for small businesses to allow for greater incorporation of IoT technologies. Examples include the following:
 - The U.S. Department of Commerce, Minority Business Development Agency (MBDA) (<https://www.mbda.gov/who-we-are/overview>)
 - DOE Office of Small and Disadvantaged Business (<https://www.energy.gov/osdbu/office-small-and-disadvantaged-business-utilization>)

- o National Science Foundation Program for Small Business (<https://www.nsf.gov/funding/smallbusiness.jsp>)

Potential implementation barriers:

- Time and Cost: The time and cost for this transformation could be considerable and small companies or startups may lose funding and/or interest and cancel a project.
- Education: There is an overarching need to educate local governments and consumers on these new types of technologies which could be hard and time consuming, especially relevant for small businesses and startup manufacturers who have limited personnel.
- Supply Chain: The manufacturing industry recognizes the goal from the Administration of Buy America, Build America (BABA) however, there are current constraints meeting domestic content requirements and there needs to be an appropriate ramp-up, phase in period to get to full production. Again, this could be particularly relevant for small businesses and startup manufacturers who may have fewer sources to purchase needed components.

Research to Support the Future State of IoT

[Note: there was some discussion about the necessity for these in 5.16 and perhaps this text could move to another section (introduction or overview?). Board feedback would be helpful here since we were close on time at the December meeting.]

Key Recommendation 5.16: [Preliminary Text: The government should consider research in the following areas to support the future state of IoT. [For Board Review - Proposed by Benson]

[Text needed]

Enabling Recommendation 5.16.1: The government should research increased capabilities of IoT devices. [For Board Review - Proposed by Benson]

- Device processing capabilities
- Decreasing microprocessor power consumption
- Energy harvesting technologies
- Low cost sensors

- As more IoT applications shift to the edge, the complexity and intensity of the workloads processed is expected to increase.
- Smarter IoT devices incorporate more capable microprocessors and microcontrollers. However, more capable processors consume more power.
- Battery powered IoT devices have a limited lifetime. With billions of IoT devices to be deployed, replacing those batteries is not realistic nor practical. Disposal of billions of batteries is a looming environmental waste issue.

Enabling Recommendation 5.16.2: The government should research enabling robust infrastructure to support increasingly large number of IoT devices and systems. [For Board Review - Proposed by Benson]

- Management of distributed IoT networks (at scale)
- Optimization and maintenance of performance and Quality of Service under continuously varying conditions
- Improving system fault tolerance and resilience
- Improving middleware to support scaling
- With billions of devices, routers and servers of all types soon operating in a multi-layer architectural environment, the ability to monitor, manage, operate and support this infrastructure over its life cycle is a complex undertaking.
- The ability to detect workload demand and allocate appropriate resources to collect, process and store the data, whether on a scheduled or dynamic basis, is crucial to IoT performance. This is made more complex by the addition of new devices of varying capabilities to the environment which consumes existing resources, devices that drop in and out of the network (e.g., mobile devices, etc.), devices with varying resource demands and availability of resources.
- IoT applications and its enabling systems may sometimes fail to work properly. These failures affect the operations that the IoT application is managing and could potentially spread to other processes through a chain of cascading failures. Even if detected immediately, it is not always possible to repair the fault or to do so in a timely manner.
- As more IoT devices are added to the network in the future, the ability of these devices to be integrated into the network and interoperate with existing and older devices and systems is critical to scaling. Middleware, the software that sits between increasingly diverse and heterogeneous devices and applications and allows them to communicate with each other, is essential to integration and scaling of IoT networks. However, middleware must also evolve to support future IoT infrastructure needs.

Enabling Recommendation 5.16.3: The government should research methods to enable Usable AI for IoT. [For Board Review - Proposed by Benson]

- Ethical AI development
- Explainable AI tools and operations
- Collective intelligence IoT
- Human-AI collaboration
- the use of AI in IoT raises questions of fairness, privacy, ethics, maleficence, accountability and transparency
- For AI controlled operations to be trusted and adopted at scale, its users must be able to understand and assess the AI algorithm's decision-making processes, its alignment and precision to target outcomes under a variety of planned and unplanned conditions and its consistency in creating and acting on the outcomes.
- As IoT adoption scales and the number of devices grow, IoT will transition from devices working individually to create individual outcomes to a collection of IoT devices working together to create an overall greater outcome. Collective intelligence is relatively new and the technology is still immature.
- Human-AI collaboration requires both to "work together as partners to achieve a common goal, sharing a mutual understanding of the abilities and respective roles of each other". Successful collaboration requires the development of new techniques, methods and components to enable a tightly coupled perception-action integration.

Enabling Recommendation 5.16.4: The government should conduct research in the development of hyperconnected communications networks. [For Board Review - Proposed by Benson]

- Spectrum sharing and management
- Network infrastructure to support AI and complex IoT applications
- Fault tolerant and resilient network infrastructure
- Self-defending adaptive network security

Justification:

- There is a finite amount of wireless spectrum available for IoT applications. In dense urban environments, this can become problematic as the number of IoT devices scale up and data traffic volumes grow, leading to network congestion and radio frequency interference.

- AI and autonomous IoT applications impose high performance requirements for communications networks. Further research and innovation are necessary to develop the network to meet these needs.
- As additional IoT devices with varying levels of quality and performance levels are integrated into the network, they introduce faults that could disrupt operations. During operation, some devices may be capable of tolerating errors, while others propagate errors. Some devices are operating with the latest firmware updates, while others are running outdated versions or cannot be patched. Finally, the IoT devices may be operating in networks that may be outdated, misconfigured or incompatible.
- IoT devices introduce new attack surfaces that can be exploited to breach the network. To be successful, self-defending and adaptive networks must “be effective in an unstructured, unstable, rapidly changing, chaotic, adversarial environments; able to learn in real-time and under extreme time constraints, using only a few observations that are potentially erroneous, of uncertain accuracy and meaning, or even intentionally misleading and deceptive.”

Enabling Recommendation 5.16.5: The government should research methods to enable the development of Human centric ambient IoT. [For Board Review - Proposed by Benson]

- Design for human-AI interaction
- Trust in human-AI interactions
- Accessibility and inclusion

IoT AB Themes: U.S. Leadership

Justification

- For replicable and successful collaboration with humans and AI systems, continued research is necessary to understand how humans can most effectively augment AI systems, how AI systems can enhance what humans do best and how to redesign operations and algorithms to support the collaboration.
- Human-AI collaboration breaks down or becomes less productive if one or both sides do not execute as expected. Humans may not trust the outputs of AI or its ability to execute.
- To be inclusive and accessible to as many people as possible, a connected society must develop interaction models and user interfaces that are intuitive, easy to use and program and consistent with the way people expect to interact with human-AI and IoT systems.

Fostering an IoT-Ready Workforce

Objective 6: The U.S. should invest in and promote initiatives that will improve the knowledge, skills, and abilities of those who develop, implement, and operate IoT devices, applications and systems.

Key Recommendation 6.1: The government should invest in and promote IoT-related aspects of 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.

Benson note: When we talk about IoT workforce development, we need to think more broadly - we need to think about and discuss it this way. The IoT workforce development approach should consider and include:

1. Sourcing and recruitment of workers: creating initiatives to bring more people in the workforce. This could be new workers (out of high school, out of college, immigration, and people who have left the workforce - the unemployed, retired, women who left to raise kids and now coming back, etc.), as well as people who have traditionally been underrepresented (certain minority groups, disabled, etc.). The reason we need these groups is that there is a labor shortage, and as digital and IoT roles grow, there will be a shortage of workers to do these jobs.
2. Development: Educating that worker base. This can be done at a variety of levels and means - vocational training, community college and university training, and continuing professional education. Development should target a variety of roles, from engineers to those that manufacture the digital solutions/products, to those that install and service them, as well as those that operate them. Some of this can be done by the military, as the use of IoT technologies are incorporated in government and military applications and facilities.
3. Placement. Once the workforce is trained or retrained, they need to be placed in industries across the economy, or in areas of the country with shortages of this labor (for example, rural areas, etc.). This includes new workers, as well as those reskilled from other industries. Note we had a recommendation in smart cities that talked about tuition forgiveness for those people that serve their time in these areas or industries where there is a need for skills.
4. Workforce Retention. We should have to retain workers who have been trained from leaving the industry or their roles. Some initiatives should be designed around addressing this issue.

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.

Enabling Recommendation 6.1.1: The government promote continuing education, professional development, and vocational training for IoT integration in supply chain management.

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

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

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

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

- **Addressing Skills Gap:** The surge in IoT utilization in supply chain management will necessitate a workforce proficient in specialized areas such as data analytics, software development, and data integration. Investments in continuing education, professional development, and vocational training can bridge this gap, ensuring businesses have the skilled talent for effective IoT implementation.
- **Enhancing Competitiveness:** The competitiveness of the manufacturing sector hinges on a well-equipped workforce. Government investment in lifelong learning and skills development can bolster businesses' competitiveness, enabling them to maintain a robust global standing.
- **Fostering Innovation:** A workforce with deep-rooted IoT knowledge can spark innovation in supply chain management. Government-led educational and training programs can cultivate this innovative spirit, supporting the creation of avant-garde solutions.
- **Supporting Digital Transformation:** As the manufacturing sector undergoes digital transformation, there is a need to adapt operations to accommodate IoT and similar technologies. Education and workforce development investments can empower workers with the skills needed to support this transition, facilitating seamless integration of IoT in supply chains.
- **Encouraging Job Creation:** The integration of IoT in supply chain management can open new job avenues in areas like data analysis, software development, and cybersecurity. Government investment in education and workforce development can prepare workers for these opportunities, stimulating economic growth and job creation.
- **Promoting Social Inclusion:** Education and workforce development programs can enhance social inclusion, providing underrepresented groups with the necessary skills and training for the IoT-centric job market. This includes opportunities for professional development, vocational training, and continuous learning.
- **Ensuring Long-term Sustainability:** As the manufacturing sector evolves, businesses need to adapt to emerging technologies and industry trends. Government investment in education and workforce development can support the sector's long-term sustainability, assisting businesses in their ongoing IoT adoption and integration efforts.

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

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

Potential barriers: Impediments to implementing this recommendation include:

- **Insufficient Funding:** Limited resources may restrict the government's capacity to invest in continuing education, professional development, and vocational

training programs at the necessary scale. This could impact the availability and accessibility of these programs for the workforce.

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

Enabling Recommendation 6.1.2: The 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. 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.

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

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

- **Identifying skill requirements:** Conduct a thorough analysis of the specific skills and expertise needed.
- **Developing targeted curricula:** Collaborate with educational institutions, industry stakeholders, and training providers to develop targeted curricula and training programs unique to the transportation sector.

- Expanding access to education and training: Implement policies and programs that ensure broad access to this and training, including financial aid, scholarships, and online learning options to reach underserved communities.
- Encouraging industry-academia partnerships: Promote partnerships between industry and educational institutions to facilitate real-world learning experiences, internships, and collaborative research projects.
- Focusing on reskilling and upskilling: Implement programs to reskill and upskill the existing workforce, enabling them to adapt to the changing requirements of the transportation sector.
- Establishing performance metrics: Develop performance metrics and evaluation methods to assess the effectiveness of education and workforce development initiatives and make data-driven improvements as needed.
- Outcomes-based Contracting: Outcomes-based Contracting is a form of contracting comprised of four discrete characteristics: Identification, Alignment, Measurement, and Adjustment... NEMA has published a whitepaper on this topic (https://www.nema.org/docs/default-source/nema-documents-libraries/whitepaper-on-outcomes-based-contracting.pdf?sfvrsn=f3ad2716_2).

Potential barriers: Possible barriers to implementing this recommendation include:

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

Enabling Recommendation 6.1.3: The government should develop educational initiatives that include IoT, targeting workforce development, and enhancing business, government, and consumer data privacy and trust.

In response to the rapidly evolving landscape of the Internet of Things (IoT), the U.S. government has been recommended to develop targeted educational initiatives. These initiatives are not just focused on workforce development but also aim to enhance data privacy and trust among businesses, government entities, and consumers. The rationale behind this recommendation hinges on several key benefits: increasing the understanding and safe use of IoT technologies, cultivating a skilled workforce adept at navigating IoT privacy challenges, and bolstering trust and adoption of IoT devices and services across various sectors.

To effectively implement these educational initiatives the government needs to undertake a comprehensive approach to effectively implement these educational initiatives. This includes defining the scope and content of the initiatives, identifying and reaching key target audiences like schools, universities, businesses, and the general public, and ensuring that the workforce development encompasses a broad range of personas, including manufacturers, implementors, service providers, and workers.

Collaboration with educational institutions and industry leaders is vital, as is the need to ensure that the educational content remains relevant and practical. An essential aspect of this initiative is the regular update of these programs to align with ongoing technological advancements and evaluate their effectiveness through consistent assessments and feedback. In implementing these recommendations, the U.S. government should consider utilizing frameworks such as the National Cybersecurity Strategy Implementation Plan, specifically Initiative 4.6.1, which focuses on publishing and tracking a National Cyber Workforce and Education Strategy. This strategy could be a cornerstone in achieving the broader goals of enhancing understanding, skill development, and trust in IoT technologies.

Implementation considerations: Defining the scope and content of educational initiatives, identifying key target audiences (schools, universities, businesses, general public), collaborating with educational institutions and industry leaders, ensuring the relevancy and practicality of the educational content, regularly updating the initiatives to keep pace with technological changes, and workforce development to encompass personas, including manufacturers, implementers, service providers, and workers.

The government should facilitate policies and programs that support the key education and digital skills development across vocational schools, community colleges and four-year universities for the following sector-specific workforce areas:

- **Construction** -The construction industry is behind the curve in digitalization. 43% of U.S. civil engineers and contractors reported the use of digital tools and innovations, compared with 66% of non-U.S. counterparts. 43% of U.S. civil contractors had low digital capabilities, compared with only 23% of non-U.S. construction companies. In contrast, 45% of non-U.S. construction and engineering companies reported high digital capabilities, compared with just 20% for U.S. companies.
- **Insurance** - Digital innovation is transforming the insurance industry. A shortage of digital skills and talent, however, is hindering the ability of the insurance companies to innovate and deliver new products and experiences, execute and operate new business models and to re-engineer existing processes and digitize operations.
- **Retail** - The retail industry is undergoing a long running technology transformation towards omni-channel retail. This is necessary for retailers to be relevant, operationally efficient, profitable and resilient. A lack of the relevant digital skills and workforce is hindering this transformation.
- **Municipal and utility workforce** - Manufacturing jobs are no longer low skilled jobs but require new skills. Automation will require people to work alongside robots and machines. A labor shortage and skills shortage will leave 2.4 million unfilled jobs between 2018-2028. This leads to a loss of \$454 B of manufacturing value by 2028 and makes the U.S. less competitive in manufacturing.⁷

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.

References

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

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

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

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

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

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

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

U.S. & 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]

Acknowledgements

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

Include speakers with links to meeting materials

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?

Appendix A: IoT Stakeholders

The Internet of Things (IoT) provides the potential significant economic and societal benefits to individual personas, communities, businesses, and academic and government organizations across the United States. Some of these benefits provide incremental value, while others are more significant and transformational. The benefits offered by IoT are not uniform but vary across groups of people, organizations, and application markets. The benefits range from positive outcomes from the use of IoT to creation of new jobs related to IoT and those indirectly related to IoT. This section provides a brief description of which stakeholders and personas are impacted, and in what ways.

Manufacturers

IoT in manufacturing can best be categorized via the following types: companies that design and manufacture chips and modules (i.e., Intel, Qualcomm, Samsung), companies that assemble modules and produce branded products (i.e. Cisco), contract manufacturers that receive a chip design and deliver a packaged chip (i.e. GlobalFoundries), and manufacturers who receive a design and Bill of Materials, assemble them as part of their manufacturing operations, and deliver a finished product (i.e. Rockwell). There are two types of manufacturers involved with the production of IoT. Component manufacturers produce the basic IoT products that are used in the development of IoT-enabled “smart” products. For example, semiconductor and sensor manufacturers produce the core components used in IoT devices. Module manufacturers then purchase and assemble these semiconductors, radios, and sensors together to build modules that brand developers (see below) and device manufacturers purchase.

Manufacturers benefit from IoT in a variety of ways. The demand for IoT products creates significant direct and related revenue, jobs and business expansion opportunities in a variety of markets. IoT products generate immediate revenue for existing products, as well as pull through demand for other higher margin products,

such as faster processors, storage devices, and sensors. For example, the continuing evolution of IoT demand has created the need for higher price and margin AI capable microprocessors. In addition, the buildout of IoT systems creates demand for edge servers and storage.

Manufacturers face a variety of barriers. The fragmented nature of the IoT ecosystem adds confusion and complexity in the marketplace and hinders adoption. Slower than expected market adoption of IoT hinders manufacturer investment and continuing product evolution. Overseas competition creates margin pressure on domestic suppliers and limits business expansion. Supply chain disruptions limit the ability to produce enough products and components to meet customer orders. Manufacturers of hardware products have an opportunity to alleviate such barriers by making their products smart-connected IoT products and offer new services including remote support and new Hardware as a Service capabilities.

Developers

In the IoT ecosystem, there are various types of developers. “Brand developers” are businesses whose core product is not IoT but incorporate and integrate IoT technologies into their existing products. For example, a machine tool manufacturer incorporates IoT into their product line, to create “smart milling machines”. The brand developer buys or licenses the IoT technology from a 3rd party, or contracts with a product development firm to develop it for them.

“IoT technology developers” offer hardware, software, and cloud application development services. They contract with brand development companies to create IoT or IoT-enabled products. Technology developers may also work with implementers (see below) to create custom IoT applications to support business, government and other organizations using IoT. Examples of IoT technology developers include product development firms, software development firms, and original design manufacturers (ODM).

IoT offers brand developers a variety of benefits. The addition of IoT to an existing product line creates new value and enables the brand to charge higher prices and is often accomplished with partnerships. The IoT-enabled product line may generate new revenue streams from recurring subscription based models arising from better visibility to the end application including online support, quicker turnaround time of RMAs and bug fixes, and upgrades based on customer changing needs

In addition, the new product line may be more attractive to buyers and allows the brand to expand existing markets and enter new ones. Overall, IoT helps brand developers increase revenues, create recurring revenue opportunities and enhance profitability.

Brand developers face a number of barriers. Digital products require a business process change including infrastructure, operational capabilities, functions, skills, and resources that are different compared to non-digital products. The addition of IoT and digital technologies to traditional businesses and business models brings new complexity and requirements that they may not have the expertise, skills, resources and infrastructure to support. Adding digital capabilities to traditional product lines creates new issues and risks, such as cybersecurity, privacy and interoperability and liability that the developer is unaware of.

New business and operating models enabled by IoT require significant investments that brand developers may be unwilling to commit to or may not be able to sustain for long. Despite the brand developer's reputation, customers may not be willing to adopt the new IoT-enabled products because of the higher risks associated with cybersecurity and privacy vulnerabilities. Some brand developers pursue a path of digitalization to upgrade the existing infrastructure before embarking to digital transformation which involves A broader business prices change.

Implementers

Implementers are businesses who resell, install and set up, and maintain and service IoT and IoT-enabled equipment to corporate, government, consumers and other buyers. Some businesses, such as retailers, only resell, but not install or service these IoT products, while others offer a full range of services. Typically, the more complex the IoT product is, the more services the implementers offer. Implementers may contract with IoT technology developers to build and implement custom solutions. For example, a HVAC contractor sells a smart HVAC system to a building owner. The contractor will install it, connect it to the network and the building energy management system, configure and test it for proper operation. They sell the building owner a maintenance contract, which requires them to come back on a quarterly basis to maintain the system and optimize its performance. On the other hand, a retailer may only sell a IoT solution but require the buyer to install and set up the solution or find a 3rd party to do so.

For implementer businesses, IoT provides a wide range of benefits. For example, IoT enables to sell add-ons to existing products, or new products, services, leading to a new source of revenue. IoT enables implementers to create new businesses and services on top of existing products and services. This leads to new revenues from existing customers, or new revenues from new customers. Many of the business models enabled by IoT enable implementers to shift away from "one-time" transactional sales to create long lasting recurring revenue streams from subscription services.

Implementers face a number of barriers that hinder their ability to develop, operate and sustain their businesses. Their existing workforce may not be well suited to support and service these new technologies. There is a lack of a suitable and sufficient workforce with the digital skills and capabilities to install, integrate, configure and optimize these technologies. While IoT enables to create new business models, transitioning to those business models are operationally challenging because they may require business process changes and digital transformation, or a shift away from “one-time” large revenues, to recurring small revenues. This requires changing operational and business models. While IoT may offer new long lasting value, customer adoption of these technologies may take longer. These long sales cycles may drive implementers to abandon these products and services in favor of traditional “tried and true” offerings that drive sales for the business now.

Administrators

Administrators are the owners and buyers of IoT and IoT equipment for business, government and other organizations. They are responsible for the overall management of these technologies and systems, including procurement, integration, operation, maintenance and optimization within the organization. IoT technologies bring together traditional separate functions together, including information technology, operations, and the business units (marketing, technical support, finance and others). Administrators may perform some or all of these functions, or they may contract with 3rd parties, including implementers and developers, to conduct these activities. Administrators may reside in each of these organizations, or they may be centralized in a single organization.

Administrators are concerned with the benefits of IoT from an organizational perspective. The benefits of IoT depend on the application and usage, but include increased revenues, cost savings and profitability. IoT can create or enhance services and products, and lead to new revenue streams. The usage of IoT may lead to cost prevention, increased operational efficiencies, and staff and resource effectiveness. Other benefits include increased customer satisfaction, retention and loyalty.

Administrators face a number of barriers to IoT adoption in their organizations. These include cybersecurity and privacy concerns, and complexities in integrating IoT into existing information technology (IT) and operational technology (OT) or industrial processes and systems. The joining together of IT into OT and industrial operations creates resistance as it requires these separate functions and teams to break out of silos to work together. Job roles and responsibilities will change and the workforce may not have the modern digital skills, in integration, data science and programming, to fully utilize these systems.

Operators

Operators are users that use IoT products and IoT-enabled equipment to carry out their day to day jobs in a business, government or other organization. For example, operators in a factory use sensors to monitor and control the manufacturing process to increase finished product quality and reduce scrap. Operators in a power generation facility use sensors and analytics to monitor critical turbine performance to minimize unplanned downtime. Technical support staff remotely monitor sensor data to diagnose equipment deployed in the field. Resellers monitor how customers are using their equipment and make recommendations to optimize performance and outcomes. Facilities operators monitor a building's sensors and systems to optimize comfort, energy usage and operations.

While the benefits to operators vary by operator organization, there are some common benefits. These include higher productivity and performance, reduced quality defects and customer complaints, increased proactiveness and responsiveness to customer needs, reduced operating downtimes and inefficiencies, and lower operating costs and staffing resources, which collectively reduce OPEX.

Operators face a variety of barriers hindering adoption and the full realization of benefits. Operators may require training and reskilling in digital and data skills to properly use IoT-enabled equipment. While IoT increases operations visibility and leads to more transparency and accountability, it may also be perceived as “worker tracking” and is resisted by employees and their unions. Operators may resist adoption because they fear that IoT leads to operational efficiencies, automation and less need for staff. Some operators feel that their “tried and true” experiences and intuition is more relevant and resist the use of the IoT technologies. Finally, the use of IoT may lead to changes in roles and responsibilities, which operators may not be comfortable with or suited for.

Consumers

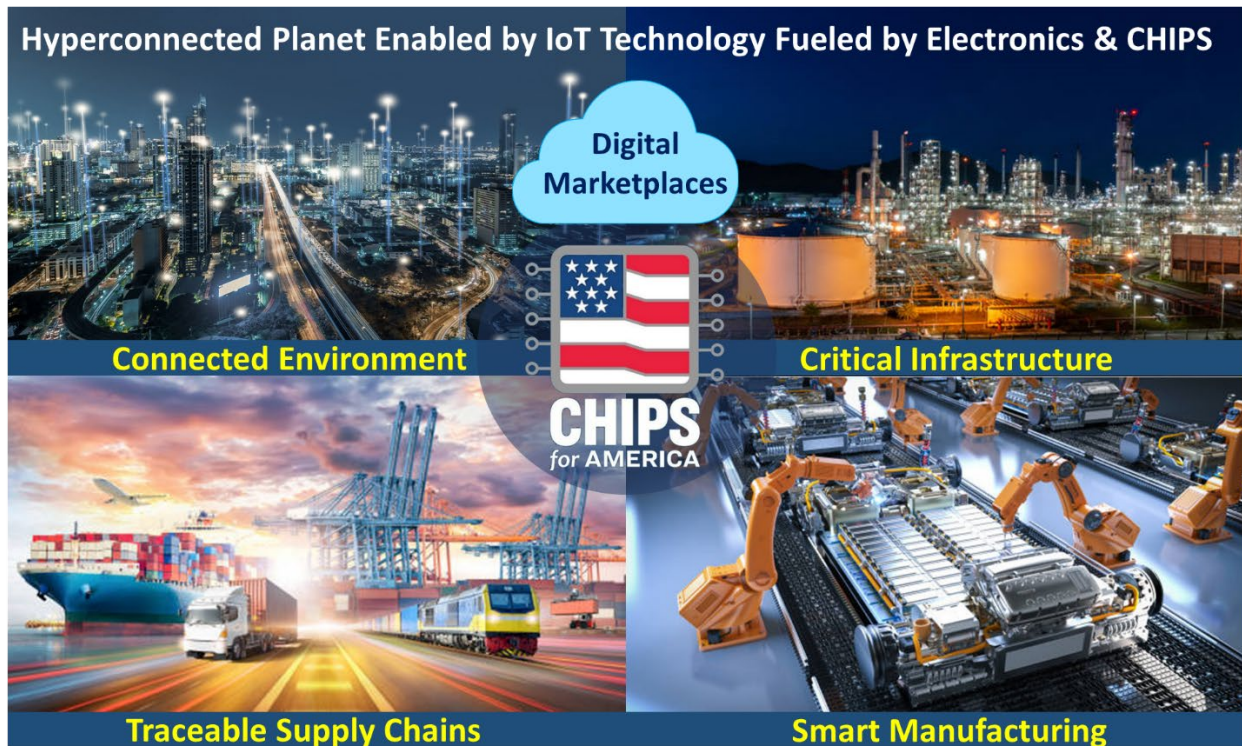
Consumers purchase and use IoT and “smart” products for their personal or family use. For example, they use “smart watches” to monitor their health and physical activities, receive and communicate messages, and run a variety of apps. They use “tracker” devices to locate their wallets, handbags, keys, luggage and other things. They use “smart assistants” to turn on and off appliances and other devices, get information, listen to music, communicate and run “voice apps”. They use “smart thermostats” to keep the home at a comfortable temperature and save on energy bills. They also use connected cars for real-time navigation, vehicle health monitoring, Bluetooth mobile phone connectivity and personalized driving experiences.

IoT provides a variety of benefits to consumers, including saving money and time, increased convenience and peace of mind, improved awareness, health, safety and performance. The actual benefits vary by IoT devices and their intended uses.

Consumers face a variety of barriers and concerns that hinder adoption, and their ability to fully realize the benefits of IoT. Consumers are concerned about privacy, how the information collected is being used, and whether that information is used intentionally or unintentionally in a manner adverse to them. Consumers with low levels of digital literacy, as well as those with limited access to broadband service, may not be able to fully realize the utility and benefits offered by IoT. Products that are poorly designed, hard to set up and operate, result in consumers limiting their use of IoT or result in poor results. High product costs and subscription fees may preclude consumers who are on fixed incomes, or those that are on the lower end of the socio-economic scale from having these devices.

Appendix B: Leveraging the CHIPS Acts and IoT for Supply Chain Traceability

[Note: Tom K has provided this significant work which provides background and rationale for numerous recommendations. We are providing it as an appendix for group discussion, recognizing that many portions would need to be revised and included in the overview and findings sections.]



Executive Summary

The U.S. must lead in coordinating subsidies between the U.S. and EU CHIPS Acts and similar programs of allied nations in pursuit of initiatives that prove the value of digital infrastructure for cross-border electronics supply chain traceability starting from chip design and manufacturing. Traceability coupled with policies that level the playing field against our adversaries' lower labor rates and higher subsidies, will ensure sourcing of trusted domestic and allied chips and exporting traceable chips that are not used by adversaries against U.S. interests.

For centuries, we have recognized the significance of tracing money to safeguard and grow our economy. Now, geopolitical realities demand similar traceability for physical goods within global supply chains, mirroring the controls, security, and benefits seen in our financial systems. With over 70 fabs being built globally backed by CHIPS-like government subsidies, the urgency for supply chain traceability is glaring. When

these fabs surge into production, vast quantities of chips used in electronic devices will flow through obscure distribution channels and unregulated supply chains, creating unprecedented risks.

Without trusted traceability of physical and digital chip assets, we face significant geopolitical, security, and economic risks. Adversaries use U.S. and allied nations' chips in their military equipment, while counterfeit or Trojan-laden chips threaten to harm our critical infrastructure. Export controls on high-end AI chips may not work as they can be remotely upgraded over-the-air. Trusted chip traceability, like money traceability, can help mitigate these risks and boost our economy. It will create new industries and workforces using digital tools for augmented supply chain logistics, tracking, auditing, and authentication. It will fuel the growth of chip enabled IoT services and business models through incentives to establish market preference, regulate market access, monitor field use, and program chip capabilities remotely.

This section outlines a strategy based on the IoT Advisory Board recommendation 4.3 and related enabling recommendations on using IoT and adjacent technologies to pursue a supply chain traceability strategy for chips and electronics devices.

1. IoT will explode in ways that are transformative for our society. It will fuel digital marketplaces and business ecosystems creating trillions in economic value.
2. IoT adoption is impacted by global supply chain imbalances and vulnerabilities impacting the security of IoT services and the trust of data used in AI apps.
3. We must act now with allied nations to build traceable supply chain networks and ecosystems aligning our incentives for security and economic growth.

The U.S. can lead a CHIPS-based traceability strategy with allied nations by using IoT technologies coupled with AI and cross-border Public Private Partnerships to track and trace chips, create digital marketplaces, and fuel the future digital economies.

Opportunity to Create Traceable IoT Supply Chains

The current geopolitical landscape presents a significant opportunity to create cross-border, traceable supply chains. The increased demand for IoT devices, accelerated digital transformation across industries, reshoring and diversification of supply chains have all created a conducive environment for supply chain innovation. Geopolitical tensions, trade restrictions, and sanctions further underscore the need for secure and

resilient supply chains. Moreover, the National Cybersecurity Strategy and NDAA¹⁰³ legislation emphasize the importance of traceability for mitigating supply chain risks.

The main drivers that create opportunities for trusted supply chain traceability are:

Increased demand for IoT devices: The Covid-19 pandemic has led to an increased demand for IoT devices, particularly in areas such as healthcare, remote monitoring, and smart homes. This has created new opportunities for chip and electronic device manufacturers to supply these devices and related components.

Accelerated digital transformation: The pandemic has accelerated the digital transformation of many industries, leading to a greater need for IoT devices to support remote work, e-commerce, and other digital applications. This has fueled demand for electronics used in IoT devices using chips from various sources of origin worldwide.

Reshoring and diversification of supply chains: Shortages have highlighted the risks associated with overreliance on a single supplier or region for critical components. This has led many companies to re-shore or diversify their supply chains, creating new opportunities for chip and electronics manufacturers to expand their customer base.

Geopolitical tensions, restrictions, sanctions: Geopolitical tensions have led to trade restrictions and tariffs, making it more difficult for companies to source chips from certain regions. This drives new opportunities for OEMs to supply trusted devices and chips that establish market preference, regulate market access, and monitor field use.

National Cybersecurity Strategy: The national cybersecurity strategy calls for global supply chain resilience and increased cooperation with international allies to combat counterfeit products¹⁰⁴ and supply chain risks. NDAA requires U.S. government agencies to purchase chips from known sources and traceable chain of custody.

Mitigating supply chain risks: Counterfeits¹⁰⁵ and chips containing Trojan Horses used in various attacks are growing. Cybercriminals often target supply chains to gain access to sensitive data or systems. By implementing supply chain traceability, governments and organizations can increase visibility and mitigate supply chain risks.

Ensuring the security and integrity of critical systems: Many critical systems, such as those used in healthcare, critical infrastructure, and transportation, rely on

¹⁰³ <https://www.securityindustry.org/2022/12/20/congress-sends-ndaa-fy23-to-bidens-desk-adds-semiconductor-procurement-restrictions/>

¹⁰⁴ <https://scm.ncsu.edu/scm-articles/article/counterfeiting-is-on-the-rise-projected-to-exceed-3-trillion-in-2022>

¹⁰⁵ <https://autosec.se/the-kojima-toyota/>

hardware and software chips from a variety of suppliers. Supply chain traceability can help governments and organizations ensure the integrity of such systems.

Strengthening international cooperation with allies: Supply chain traceability requires collaboration with international allies to combat cyber threats. By sharing information about supply chain risks and vulnerabilities, governments, organizations, and enterprises can develop effective strategies for mitigating these risks.

Addressing nation-state cyber-attacks: Nation-state cyber-attacks are growing and preferred by attackers for gaining access to systems or data, while remaining undetected and difficult to defend. By pursuing cross-border supply chain traceability programs with our allies, governments can better protect themselves against these types of attacks and improve their ability to trace cyber-attacks by rogue actors.

The urgency for secure and traceable supply chains is unprecedented. Factors like rising IoT demand, digital transformation, supply chain diversification, and geopolitical tensions highlight the importance for supply chain traceability. Allied nation cooperation, led by a US-EU coordination on CHIPS Acts subsidies, can bolster supply chain security and combat nation-state cyber threats.

Supply Chain Traceability is Critical for IoT Electronics

Growth of IoT Economies. IoT will grow in ways that are transformative for our society and our environment. The future IoT digital economies are projected to reach \$5.5 to \$12.6 trillion by 2030, will be driven by 100+ billion connected electronics devices and 500+ Zettabytes¹⁰⁶ of data which will fuel IoT services and AI applications.

IoT Barriers to Adoption. IoT adoption and growth is hindered by several barriers including supply chain disaggregation, geopolitical tensions, and cybersecurity risks. These arise from organizational silos, fragmented supply chains, and unregulated distribution channels. No one company can address these challenges in IoT adoption and monetization across value chains. It requires a collaborative business ecosystem.

Value of IoT Digital Provenance. A trusted digital thread starting from chip design and manufacturing is crucial for national security and economic growth. A digital thread facilitates the flow of data across business operations, products, and assets within value chains. It drives operational effectiveness, bolsters supply chain resilience and security, and fosters business expansion.

Digital Trust and Sustainability. Data is the “*new unprocessed oil*” that requires trusted infrastructure and standards to extract value. Chip manufacturing produces

¹⁰⁶ One zettabyte is equal to a trillion gigabytes.

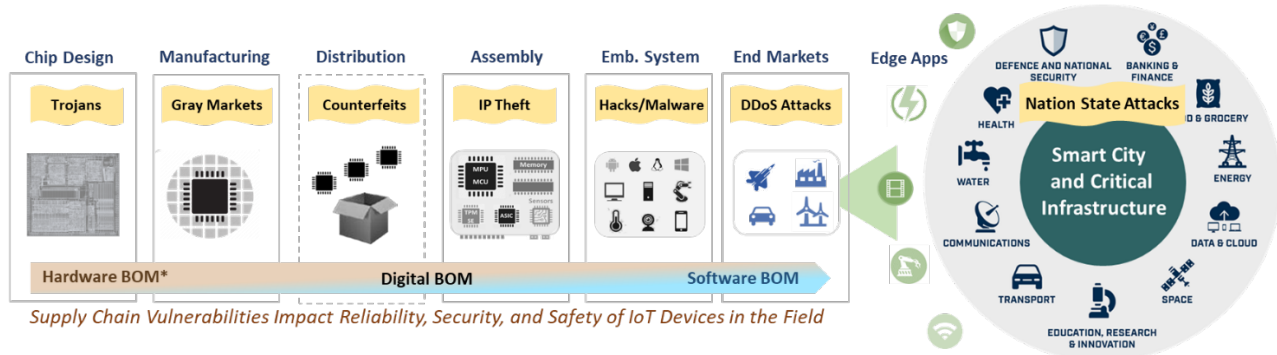
huge volumes of data for design, test, verification, and metrology, which is used to improve quality, reliability, assurance, and yield. Analytics and AI tools consume this data to create solutions and applications and that enable new revenue streams.

The U.S. and EU CHIPS Acts create opportunities for allied nation initiatives, to start a trusted digital thread for trusted supply chain provenance and traceability:

- The U.S. and EU should use the CHIPS Acts to orchestrate a trusted ecosystem of stakeholders to collaborate on trusted digitalization of the IoT supply chain.
- The U.S. can orchestrate multi-stakeholder partnerships of EDA, IP, IC, Foundry, and Cloud vendors for pilot programs on digital infrastructure for traceability.
- The U.S.-EU TTC should promote Public Private Partnerships with allied nations for cross-border trusted traceability since no one company can do this alone.

A U.S. led supply chain traceability strategy and collaboration with international allies will strengthen international security and accelerate the growth of digital economies.

Supply Chain Vulnerabilities & Risks Create Opportunities



Increasing IoT Supply Chain Security Risks. Supply chain security and trust pose major concerns due to the vast attack surface from chips to edge applications. Attacks experienced during field use of IoT devices such as DDoS attacks¹⁰⁷ are often traced back to supply chain vulnerabilities due to bugs or intrusions in the hardware .

Western chips discovered in enemy weapons. Ukraine used expensive missiles to shoot down cheap drones¹⁰⁸ shows that sanctions and customs controls on chips are ineffective¹⁰⁹. Chip suppliers complying with sanctions lack visibility into where their

¹⁰⁷<https://cybersecuritynews.com/ddos-attacks-use-iot-devices/>

¹⁰⁸<https://www.reuters.com/technology/chip-challenge-keeping-western-semiconductors-out-russian-weapons-2022-04-01/>

¹⁰⁹<https://www.bloomberg.com/news/articles/2023-12-21/chips-from-texas-instruments-txn-analog-devices-adi-flow-into-russia?srnd=undefined>

chips go and how they are being used. Tracing chips is like following the flow of drugs, with money laundering, and covert distribution networks. Our navy used \$2 million missiles in the red sea to shoot down \$2,000 Houthi drones¹¹⁰, altering modern warfare dynamics, affecting maritime routes, and raising oil prices and the cost of goods.

Actions Needed to safeguard critical infrastructure. Industrial IoT Systems and process sensors used in critical infrastructure¹¹¹ are vulnerable to attacks due to lack of security originating in hardware supply chain. Power plants lack visibility into their OT environments or exposure of IT and OT systems. Securing 10 servers (IT) connected to 1000 unsecure PLCs (OT) is a major vulnerability. Strategies to increase trust in the Information and Communications Technology and Services Ecosystem¹¹² are essential.

Limited real time visibility for IT/OT attacks. In contrast to IT cybersecurity attacks, successful OT attacks can impact human safety and damage physical equipment taking any industrial offline for extended periods of time. Attacks in Software Bill of Materials (SBOM) can be minimized¹¹³ if software is linked to trusted and traceable Hardware Bill of Materials (HBOM) with traceable provenance and chain of custody.

Growing geopolitical significance of AI chips in supply chains. With the increasing adoption of Generative AI, there is a growing need for faster, more affordable, and readily available AI chips that are critical for security and economic growth as AI applications expand across various sectors. The cost of fabricating chips at scale is substantial, and national security concerns have further intensified due to the concentration of chip production in specific regions and geopolitical conflicts¹¹⁴.

Export controls for high-end AI chips are increasingly challenging. While sanctions on exporting semiconductor manufacturing equipment in China are likely to increase¹¹⁵ the same is not true for AI chips. Secretary of Commerce stated the U.S. should sell AI chips to China, while restricting the high-end chips for security reasons¹¹⁶. However, this will be harder due to the rise of *connected chips* programmed remotely. Hardware-as-a-Service business models such as, Intel's pay-

¹¹⁰<https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480>

¹¹¹<https://www.gao.gov/products/gao-23-105327>

¹¹²[https://www.cisa.gov/sites/default/files/2023-03/Draft%20NSTAC%20Strategy%20for%20Increasing%20Trust%20Report%20\(1-31-23\)_508.pdf](https://www.cisa.gov/sites/default/files/2023-03/Draft%20NSTAC%20Strategy%20for%20Increasing%20Trust%20Report%20(1-31-23)_508.pdf)

¹¹³<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/software-bill-of-materials-managing-software-cybersecurity-risks>

¹¹⁴<https://supplychaindigital.com/supply-chain-risk-management/geopolitics-shaping-ai-chips-supply-chain-eyes-steinberg>

¹¹⁵<https://www.investors.com/news/technology/semiconductor-stocks-gear-makers-getting-china-boost/>

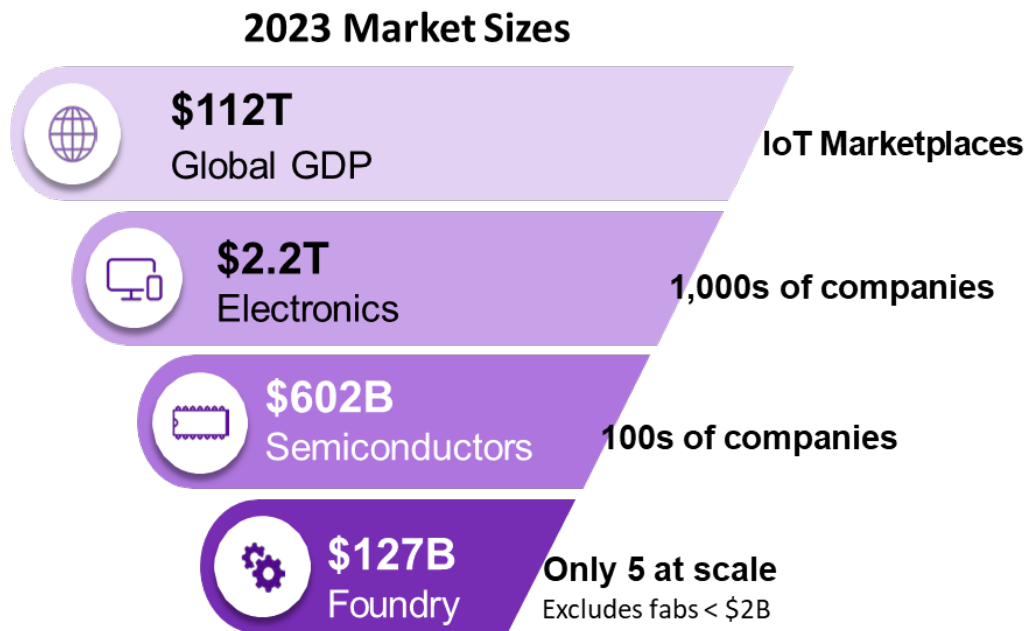
¹¹⁶<https://www.cnbc.com/2023/12/05/commerce-sec-raimondo-us-export-controls-need-to-change-constantly.html>

as-you-go chip licensing¹¹⁷ and Samsung’s chip rental service¹¹⁸ signify the start of the “Internet of Chips” era.

To mitigate supply chain disruptions, organizations are advised to establish category management for semiconductor chips, redesign products to use more readily available chips, and form partnerships with key stakeholders for better visibility into chip supply issues. Although some of these strategies may have merit, they are costly and slow to adopt. Digitalization of the electronics supply for trusted traceability can be much faster and incentivize businesses to participate in the creation of trusted digital threads which will strengthen security and fuel economic growth.

Trusted Supply Chain Traceability Starts from the CHIPS Acts

Supply chain provenance starts with trusted chip design and manufacturing. The geopolitical backdrop accelerated government initiatives worldwide to increase domestic and allied chip production capacity. This creates opportunities to drive supply chain resilience and monetization.



The multi-trillion IoT opportunity depends on a few fabs producing chips. Almost 80% of worldwide fab capacity producing chips is controlled by handful of allied nations including Taiwan. Without Taiwan’s TSMC, the allied capacity would drop down to half. Currently, the top five foundry vendors fabs, generate \$127B in revenues

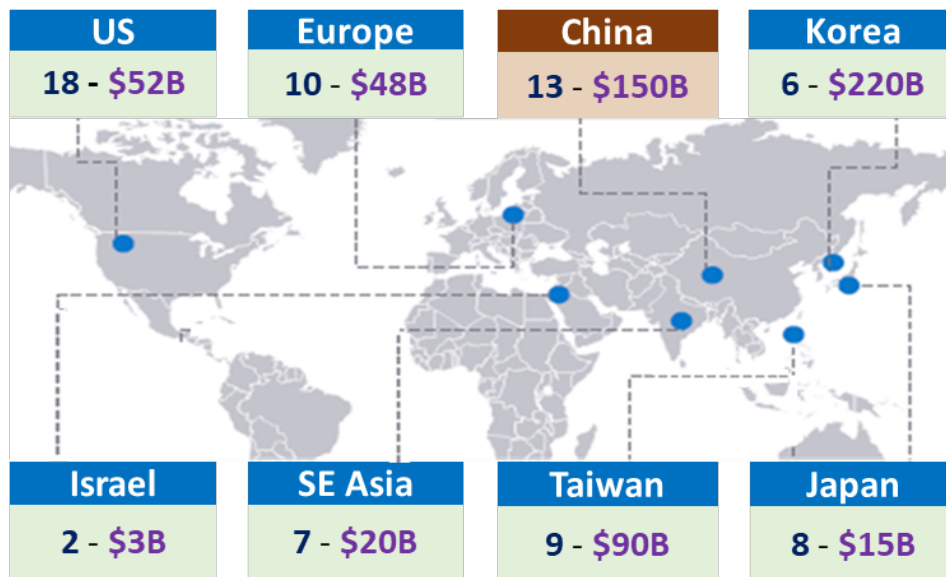
¹¹⁷<https://www.tomshardware.com/news/intel-officially-introduces-pay-as-you-go-chip-licensing>

¹¹⁸<https://min.news/en/economy/363514b98d8096e72b968a90f7a11a16.html>

which enables \$602B in chip revenues, 2.2T in electronic devices revenues, and \$112T global GDP fueled by IoT digital marketplaces.

The U.S. and EU CHIPS Acts momentum for allied collaboration: On December 5, 2022, U.S and EU top officials including Secretary of Commerce Gina Raimondo, Secretary of State Anthony Blinken, U.S. Trade Representative Katherine Tai, and European Commission Executive Vice-Presidents Margrethe Vestager and Valdis Dombrovski, agreed to coordinate semiconductor subsidy programs and work closely to strengthen semiconductor supply chains¹¹⁹. Since then, the U.S. Department of Commerce garnered allied nation support for partnerships and innovation, resulting in \$450 billion in government-funded fabs surpassing China’s \$150 billion¹²⁰.

2023-2025: Fabs Built & Government Subsidies



Since December 2022, the race to invest in chip manufacturing for allied chip sourcing and occurred in record time was extraordinary:

- In March 2023, the CHIPS Act announced funding for allied partnerships, promoting semiconductor collaboration¹²¹. Secretary Raimondo unveiled the U.S.-India Semiconductor Supply Chain and Innovation Partnership¹²².

¹¹⁹<https://www.wsj.com/articles/u-s-eu-agree-to-coordinate-semiconductor-subsidy-programs-11670284917>

¹²⁰ Source: GlobalFoundries, SEMI.org, EY.com, DARPA.mil

¹²¹<https://www.state.gov/briefings-foreign-press-centers/funding-for-international-partnerships-through-the-chips-act>

¹²²<https://www.commerce.gov/news/blog/2023/03/secretary-raimondo-announces-us-india-semiconductor-supply-chain-and-innovation>

- In April 2023, a joint statement highlighted discussions on supply chain matters with South Korea through the United States-Korea Supply Chain and Commercial Dialogue¹²³.
- In May 2023, the EU CHIPS Act launched a pilot system to monitor the semiconductor supply chain¹²⁴. Japan and the U.S. industry leaders agreed to enhance semiconductor cooperation¹²⁵, while the U.S. led a deal with 14 Indo-Pacific nations focusing on supply chain resilience and early warnings¹²⁶.
- In June 2023, a U.S.-EU Technology Trade Council (TTC) joint statement reinforced the commitment to trade cooperation¹²⁷. Another report emphasized the critical supply chain partnership on chips between the U.S. and Taiwan¹²⁸.
- In July 2023, the EU and Japan announced plans to deepen their cooperation in the chip industry¹²⁹, while Secretary Raimondo urged the Advisory Committee on Supply Chain Competitiveness (ACSCC) to act on supply chain resilience¹³⁰.
- In August 2023, India's confirmation of subsidies for tech hardware including Apple supplier Foxconn, signifies the global focus on semiconductor supply chain collaboration and innovation¹³¹.

Over \$600 Billion in government funding will be boosted to over \$1.5 trillion. The total investment for 70+ fabs including Public Private Partnerships could exceed \$1.5 trillion. That is an unprecedented boost in global manufacturing capacity and China will be a key player. Given that most of the global fab capacity is controlled by a handful of allies, the U.S. and EU are well-positioned to lead collaborative initiatives for cross-border supply chain traceability starting from chip design and manufacturing.

¹²³<https://www.commerce.gov/news/press-releases/2023/04/united-states-korea-supply-chain-and-commercial-dialogue-ministerial>

¹²⁴<https://digital-strategy.ec.europa.eu/en/news/european-chips-act-commission-launches-pilot-system-monitor-semiconductor-supply-chain>

¹²⁵<https://www.japantimes.co.jp/news/2023/05/27/business/japan-us-cooperation-semiconductors/>

¹²⁶<https://www.reuters.com/markets/asia/us-led-indo-pacific-talks-produce-deal-supply-chain-early-warnings-2023-05-27/>

¹²⁷<https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/>

¹²⁸<https://www.us-taiwan.org/resources/us-taiwan-and-semiconductors-a-critical-supply-chain-partnership/>

¹²⁹<https://news.yahoo.com/eu-japan-deepen-chip-cooperation-131405419.html>

¹³⁰<https://www.linkedin.com/feed/update/urn:li:activity:7100570220724932610/>

¹³¹<https://www.scmp.com/tech/policy/article/3242209/india-confirms-subsidies-apple-supplier-foxconn-lenovo-and-25-other-tech-hardware-firms-bolstering>

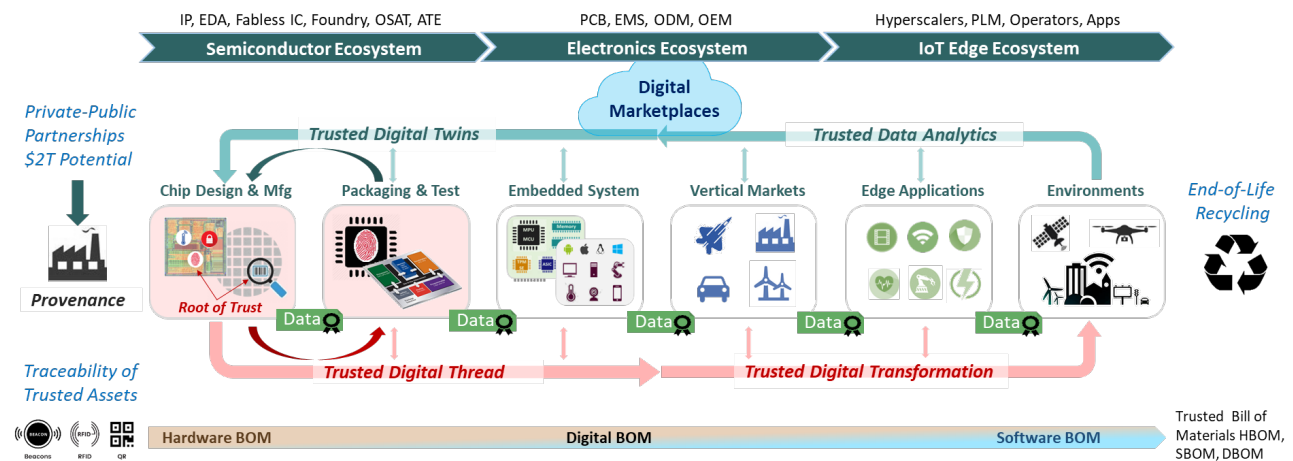
Investment in traceability infrastructure starting in chip manufacturing is small.

A digital infrastructure for supply chain traceability starting in chip manufacturing requires minimal investment compared fab construction and chipsets produced in its lifecycle. The CHIPS Act allocates little to digital traceability infrastructure, with most funds going to fab materials and equipment. Roughly 10% of fab investments support chip design and production R&D. The U.S. can lead pilot programs for the digitalization of the IoT supply chain starting from chip design and manufacturing.

Digitalization Across the IoT Supply Chain Drives Growth

Supply chain orchestration is essential for developing a trusted digital infrastructure across the IoT value chain. Participating stakeholders can be organized in three domains, semiconductors, electronic devices, and edge applications. The potential return on investment for participants can be high. Provenance for trusted supply chain traceability begins from chip design and manufacturing in existing or new fabs.

Chip Supply Chain Provenance. A trusted digital thread begins with a *Root of Trust* during chip design and manufacturing to track and trace physical and digital chip assets. One Root of Trust is placed on wafer dies or packaged chips tied to Physical IDs for traceability of physical chip assets. Another Root of Trust can be hidden inside the chip design tied to a Digital ID (fingerprint) for traceability of digital design assets. Any chip data including bill of materials (BOM) specs, etc. must be linked to these IDs.



Trusted Asset Tracking. When chips are procured in the supply chain, Physical IDs coupled with IoT technology like QR code RFID, can be used to track IoT device parts including hardware (HBOM), software (SBOM), and digital (DBOM) such as serial

numbers, product SKUs, etc. This information can be furnished as metadata into a trusted digital thread¹³² enabling a digital marketplace of producers and consumers.

Digital thread of Data and IoT Services. A digital thread provides the foundation for digital transformation for IoT with electronic devices by pointing to trusted data which can be used for analytics, AI applications, and trusted digital twins¹³³ of manufacturing that simulate how chip assets perform during field use.¹³⁴ Digitalization of supply chains requires business ecosystems driven by orchestration, governance, and network effects.¹³⁵ Orchestrated consortia¹³⁶ will give rise to digital marketplaces of data producers and consumers using data to develop and market new IoT services.

Trusted manufacturing provenance for supply chain traceability. A trusted digital thread starting from chip design to manufacturing¹³⁷ is key for establishing supply chain provenance and chain of custody for assets/data across the IoT supply chain. It uses metadata to link producers and consumers, allowing them to share information about data before a licensing transaction to utilize the data. Trusted data consumed by IoT services, analytics, AI applications¹³⁸, and digital twins enables new IoT services.



Digital thread starting in manufacturing enables business models. The rise of XaaS (Everything-as-a-Service) revenue streams seen in manufacturing for IoT end markets such as automotive, is also emerging chip design manufacturing¹³⁹. It starts with design as a service (EDA) and evolves into silicon as a service, manufacturing as a service, testbench as a service, packaging as a service, etc. These services offer many benefits such as reduced test & verification time, reduced debug, improved yield, lower capital costs, improved functional safety and security, etc.

¹³²https://www.nist.gov/system/files/documents/2022/04/25/04-25-2022-GSA_TIES.pdf

¹³³<https://www.azonano.com/article.aspx?ArticleID=6618>

¹³⁴<https://www.cNBC.com/2022/10/19/how-ai-can-help-companies-manage-the-semiconductor-supply-chain.html>

¹³⁵<https://www.wallstreetprep.com/knowledge/network-effects/>

¹³⁶<https://www.cornerstoneondemand.com/resources/article/why-network-effect-secret-formula-your-associations-success/>

¹³⁷<https://www.mckinsey.com/industries/semiconductors/our-insights/reimagining-fabs-advanced-analytics-in-semiconductor-manufacturing>

¹³⁸<https://www.mckinsey.com/industries/semiconductors/our-insights/scaling-ai-in-the-sector-that-enables-it-lessons-for-semiconductor-device-makers>

¹³⁹<https://www.linkedin.com/pulse/unlocking-new-frontiers-how-semiconductor-companies-can-rochak-sethi/>

Trusted Value Chain	Producers	Consumers	Monetization
Electronics Design Simulation	EDA tools generate data from circuit design, optimization and performance.	Hardware designers, and device makers can use this data to improve products	Offer data-driven insights and add-on solutions to design and simulation tools.
Semiconductor Manufacturing	Produce vast amounts of data on quality, reliability, performance, integrity, etc.	Chip or equipment suppliers and device makers use data to improve products	Fabs license data to chip consumers to improve time-to-market & differentiation
Supply Chain Procurement	Create data for shipping, inventory levels, demand forecasting, availability, etc.	Manufacturers, logistics companies, retailers can increase forecast accuracy	Offer data access for customers to reduce, costs, and improve customer service.
IoT Device Deployment	Generate data related to device operation, sensors, user interactions, environment.	Businesses, insurance companies, and researchers use data to offer solutions.	OEMs get insights on field use, causes for bugs, RMAs, and predictive maintenance
Electronic Part Lifecycle	Generate data on specifications, quality availability, and lifecycle management	Chip and Device makers, repair services, parts, ESG and recycling organizations	Recycling data can be licensed to designers, suppliers, and eco-friendly organizations

As chip assets/data flow in the supply chain the digital thread enables stakeholders downstream, to offer Hardware-as-a-Service¹⁴⁰ for PCB, Systems, and IoT applications driven by data producers and consumers which fuel digital marketplaces.

Electronic Design and Simulation: EDA simulation tools generate data related to circuit designs, performance, and power predictions. EDA vendors offering simulation tools can offer data-driven insights to improve design efficiency and performance and create digital twins of design for system and silicon lifecycle management.

Semiconductor Manufacturing: Fabs produce vast amounts of data during production related to equipment and silicon performance, yield, quality, etc. Fabs can sell data access to chip designers used to optimize their processes, to equipment manufacturers used to improve their equipment.

Supply Chain Procurement and Logistics: Companies along supply chains produce data for shipping, inventory management, demand forecasting, supply chain optimization, etc. Some sell data to manufacturers, logistics companies, and supply chain partners seeking to optimize operations, and reduce costs.

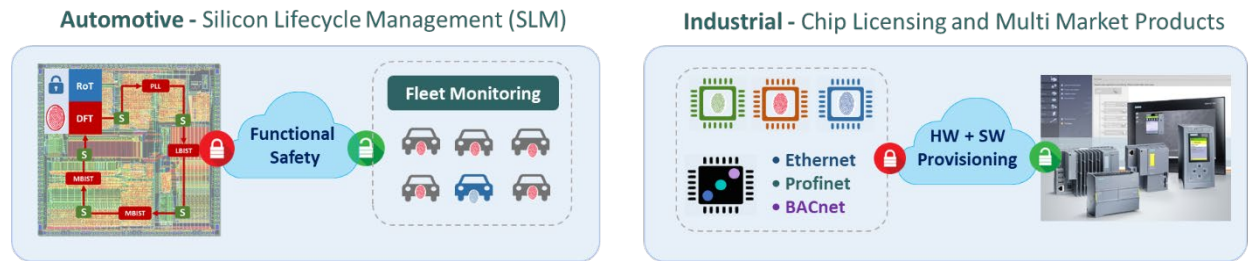
IoT Device Deployment and Field Use: IoT devices generate a wealth of data related to their operation, sensor readings, and user interactions. Data producers can aggregate and anonymize data to offer insights about consumer behavior, predictive maintenance, or setting conditions.

Electronics and Chips Lifecycle: Manufacturers, distributors, and buyers of IoT devices produce valuable data on specifications, availability, quality, and usage. This data can be monetized by companies seeking regulatory compliance or promoting sustainability efforts. The circular supply chain from chip design to device end-of-life or part recycling, benefits all stakeholders, aligning with sustainability goals..

¹⁴⁰<https://www.linkedin.com/pulse/unlock-limitless-possibilities-empower-your-customers-rochak-sethi/>

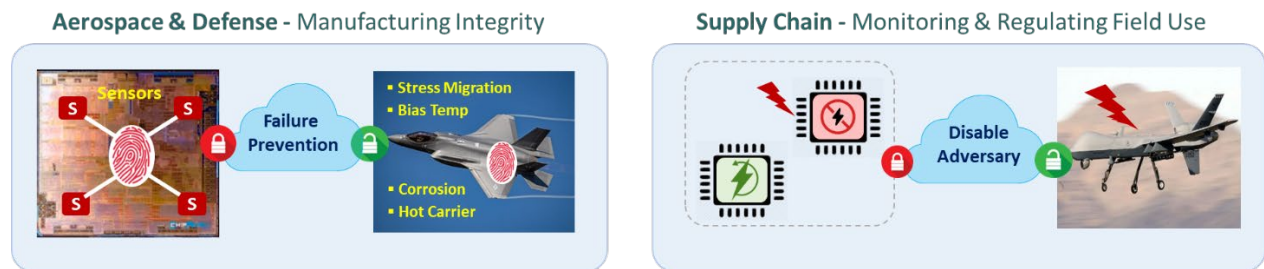
Trusted Traceability Extending to Field Use Enables “Internet of CHIPS”

Digital threads extending traceability across chip supply chains all the way to field use, enable enterprises to manage risk, establish market preference, and regulate market access and monitor field use. Enterprises can monetize data and grow new revenue streams in ways that all participants can benefit in the new era of *Internet of CHIPS*.



Automotive Field Use.¹⁴¹ Chip Designers can use chip security and fingerprint tied to Design-for-Test circuitry to gather data from chips during a self-test operation in the field and predict functional failures. Fleet Operators can analyze trusted data from connected systems and chips to manage devices in the field and develop ML/AI applications for failure prediction, risk management, updates, etc.

Industrial Field Use. Chip Suppliers can trace and authenticate chip assets in the field, configure SKUs Over-the-Air (OTA), offer pay-as-you-go business models, analyze chip data, and provide hardware and software updates¹⁴². System OEMs can securely configure devices to offer IoT services remotely and use trusted digital threads to pass data to their suppliers which they use develop digital twins of chips or devices.¹⁴³



Aerospace & Defense Field Use. Foundries and OSATs can sell test data to OEMs to save them resources for validating that chips perform as intended, increase reliability, and reduce field failures¹⁴⁴. Device makers can license test data from chip suppliers

¹⁴¹ <https://semiengineering.com/secure-silicon-lifecycle-management-architecture-for-functional-safety/>

¹⁴² <https://www.tomshardware.com/news/intel-officially-introduces-pay-as-you-go-chip-licensing>

¹⁴³ <https://min.news/en/economy/363514b98d8096e72b968a90f7a11a16.html>

¹⁴⁴ https://www.youtube.com/watch?v=hmt_7DDdHgQ

instead of relying on data sheets, thus saving time to design systems and evolve digital twin prototypes to reduce cost and time to deployment.

Monitoring Real Time During Field Use. Chip suppliers and System OEMs can track and trace allied chips when they power-up inside enemy weapons and disable them remotely (subject to security privileges) to prevent cybersecurity or physical attacks¹⁴⁵. Drones using western chips can be disabled before they attack¹⁴⁶. And IoT devices can reset their chips to factory settings upon recycling or disable them upon end of life.

Semiconductor Industry Transformation. Trusted digital threads with metadata about physical & digital chip data will accelerate IoT adoption and growth. Licensing of chips and dates can be extended to include trust and security with access rights for a variety use cases that prove the benefits and economic value. The CHIPS Acts can enable digital marketplaces and business ecosystems across IoT value chains¹⁴⁷.

Fostering Supply Chain Resilience and Economic Growth

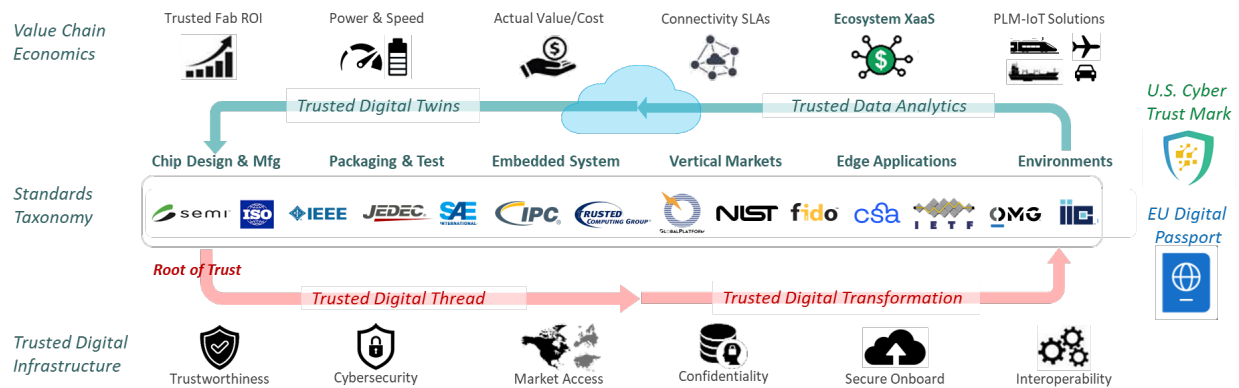
Strengthening supply chain resilience and economic value is attainable if companies and standards organizations have shared business incentives to collaborate as an orchestrated ecosystem of Public Private Partnerships. IoT adoption and growth can be accelerated through ecosystem collaboration focusing the following challenges:

A trusted digital traceability infrastructure. It starts with root of trust used to establish market preference, linked to derived security key chains for market access, linked to secure provisioning to monitor and regulate field use, linked to enterprise enabling confidentiality to protect IP, linked to secure onboarding & updates, linked to wide variety of IoT environments requiring many APIs to maximize interoperability.

¹⁴⁵<https://www.reuters.com/technology/chip-challenge-keeping-western-semiconductors-out-russian-weapons-2022-04-01/>

¹⁴⁶<https://www.wsj.com/podcasts/the-journal/cheap-drones-are-transforming-the-battlefield/44bd924e-42be-4c26-b343-6d72d881a3c6>

¹⁴⁷<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-semiconductor-transformation-study-2.0.pdf>



Taxonomy of standards across value chains. There are many standards across that provide extensive coverage across IoT value chain and minor gaps can be addressed with Private Public Partnerships. The U.S. and allied nations should collaborate to create a standards taxonomy and harmonize standards for global supply chains. NIST emphasized the need for supply chain traceability during the CHIPS R&D Digital Twin Technical Standards Workshop¹⁴⁸ which is in line with our national strategy.

Supply chain economics shared among multiple stakeholders. The transformation of physical supply chains into digital value chains is enabled by trusted digital threads and orchestrated digital ecosystems of asset/data producers, consumers, data-driven IoT applications and AI-based digital twins. Value chain economics may factor how fabs maximize ROI for trusted services, how chip designers can offer new capabilities by programming chips remotely, and how OEMs can offer high value IoT solutions.

Digital supply chains, services and IoT marketplaces. Stakeholders in the IoT and electronic supply chains can use digital threads to monetize their value-add through digital marketplaces. The EU Digital Services Act (DSA)¹⁴⁹ can extend its regulations to IoT supply chain ecosystems and data-focused digital marketplaces, by enforcing rules for intermediaries to enhance transparency and accountability. It can mandate platforms to oversee content and protect the rights of producers and consumers, promoting transparency in data exchange algorithms. A Digital Services Coordinator ensures governance, fostering a secure and transparent environment for digital IoT ecosystems, enabling scalable circular IoT value chains, and accelerating adoption.


Creating Market Awareness and “Digital Asset Trail”

Governments of allied nations can play a key role in accelerating adoption and growth of trusted supply chain traceability for IoT, by promoting initiatives like the US Cyber


¹⁴⁸<https://www.nist.gov/news-events/events/chips-rd-digital-twin-technical-standards-workshop>

¹⁴⁹https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en


Trust Mark for cybersecurity labeling, the EU Digital Product Passport (DPP) for traceability and customs controls standards using business and asset identifiers.



U.S. Cyber Trust Mark
Consumer → Industrial IoT



EU Digital Product Passport for Digital Traceability
Considerations for Data Policies Across Value Chain



Security & Privacy Overview
Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - updated on: 11/12/2020
The device was manufactured in: China

Security Mechanisms

Security updates: Automatic - Available until at least 1/1/2022
Access control: Password - Factory default - User changeable, Multi-factor authentication. Multiple user accounts are allowed.

Sensor data collection

Sensor type	Purpose
Visual	Identified
Audio	Identified - Open to date
Physiological	Manufacturer
Location	Manufacturer

Data Practices

Data stored on device: Identified

Data stored on cloud: Identified - Open to date

Shared with: Manufacturer, Government


Sold to: Not disclosed

Other collected data: Motion, Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info

Privacy policy: www.NS200.smartdeviceco.com/policy

More Information

Detailed Security & Privacy Label:
www.iotsecurityprivacy.org/features/external/manufacturer/SmartVideoDoorbell



CMU IoT Security and Privacy Label CSPL 1.0 iotsecurityprivacy.org

1 Product Groups	Product by Product	Industry by Industry				
2 Company Size	All Sizes	Large First	Large Only			
3 Application Level	Item	Batch	Product Model			
4 Data Storage	EU Federated	Company	Centralized	Decentralized		
5 Data Carrier IDs	Root of Trust	QR Code	Barcode	RFID	NFC	Marker
6 Access Security	Full	Minimum	Differentiated			
7 Requirements	Standardization	Product Spec	Combination			
8 Governance	No Assurance	Limited	Reasonable			

The U.S. Cyber Trust Mark is initially targeted for Consumer IoT. A cyber security label with a QR code is attached to IoT product raising awareness that the device is secure and protects user privacy which are top concerns of consumers¹⁵⁰. The White House created a multi-stakeholder ecosystem¹⁵¹ which gained support from industry, and academia. The same strategy applies for an orchestrated supply chain ecosystem.

The U.S. Cyber Trust Mark will be extended for industrial IoT. The White House announced that it intends to launch the Cyber Trust Mark for industrial IoT¹⁵², which may require multi-stakeholder ecosystem for traceability that may require trust metrics for HBOM, SBOM and DBOM furnished in the digital thread. Industrial IoT markets care more about trusted parts, and confidentiality to protect enterprise IP.

The EU DPP complements the Cyber Trust Mark. The DPP was originally developed for sustainability in circular supply chains. It has evolved into an elegant solution for traceability of assets for various sectors and it is most suitable for EV battery and electronics supply chains. By linking a digital thread of data with IoT track and trace technologies such as QR code, NFC, RFID, etc. with a root of trust and cybersecurity labels a the “digital paper trail” will accelerate IoT adoption¹⁵³. The EU plans to pass new regulations for DPP in 2024. To the extent Data Carrier IDs linked to immutable roots of trust, IoT technology can be used for augmented supply chain logistics of

¹⁵⁰ <https://www.cylab.cmu.edu/news/2020/05/27-iot-labels-consumers.html>

¹⁵¹ <https://www.youtube.com/watch?v=odaklOkIG8I>

¹⁵² <https://insidecybersecurity.com/share/14566>

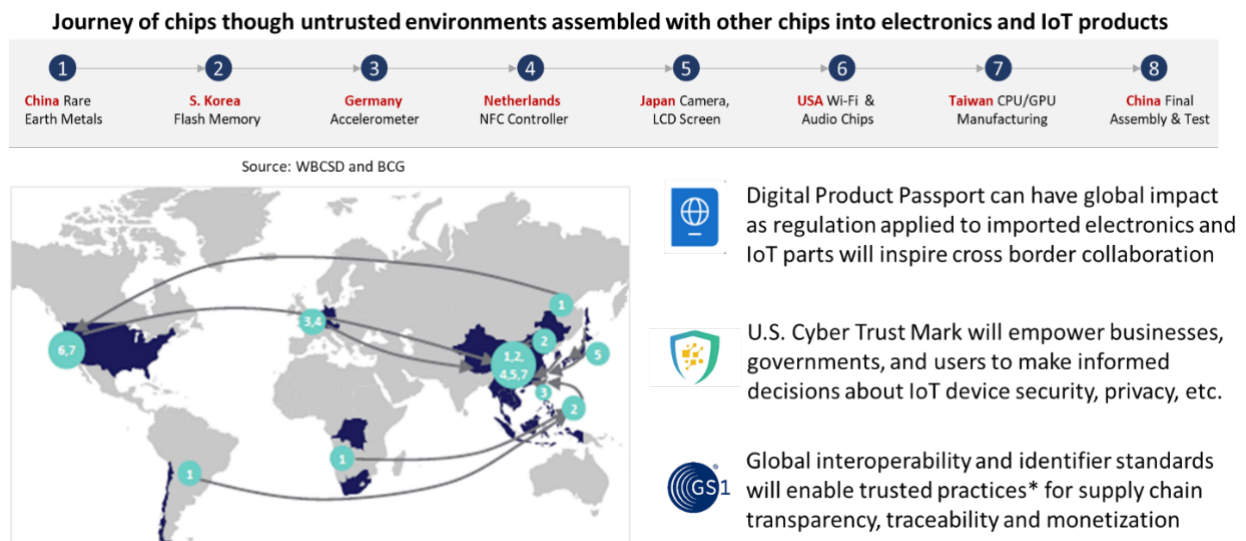
¹⁵³ www.wbcds.org/Pathways/Products-and-Materials/Resources/The-EU-Digital-Product-Passport

physical assets (HBOM) can be use for traceability of digital assets (SBOM, DBOM) and services.

Collaborative platforms in the EU such as Catena-X¹⁵⁴ for the automotive sector and Gaia-X¹⁵⁵ for infrastructure provide insights on how data related policies can speed adoption and economic growth. This also applies to fabs. The geopolitical backdrop and massive build up in fabs worldwide present the US & EU a historic opportunity to collaborate in supply chain traceability with harmonized cross-border policies.

Expanding Digital Asset Traceability Beyond Borders

Fragmented electronics supply chains around the world are complex and convoluted creating challenges for cross-border trusted supply chain traceability. Trusted digital threads enabled by Public Private Partnerships and harmonization of IoT track & trace methods can have a positive impact on supply chain risk management and fuel the growth of trusted digital marketplaces and business ecosystems.



Journey of chips through untrusted supply chains. Chips are created from rare earth metals used for to build semiconductor fabs mostly controlled by China. Several parts of an IoT device are designed in one country and manufactured in another country. The assembly of a variety of parts used in electronics and IoT devices is mostly done in China, before IoT devices are deployed. Rogue actors in the supply chain can introduce vulnerabilities that manifest into cyber or physical attacks during field use.

¹⁵⁴ <https://catena-x.net/en/>

¹⁵⁵ <https://gaia-x.eu/what-is-gaia-x/vision-and-mission/>

Governments need to collaborate in harmonizing methods. Consistent methods are needed digital product passports, cyber security labels, and global identifier standards to trace assets across borders. The U.S. and the EU made progress with the Cyber Trust Mark and Digital Product Passport. What's needed is a synergistic strategy with customs and border control protection, as it can play a role in inspiring cross-border collaboration. Imports and exports of chips and electronics need to track origin and chain of custody. Field use can be traced and managed remotely too.

EU DPP regulations will influence cross-border chips trade. EU regulations on Digital Product Passports can wield global influence in cross-border trade by setting a precedent for standardized digital product traceability. The EU's adoption of digital passports can motivate other nations to follow suit to facilitate trade with EU markets. Harmonization will simplify global digital commerce, reduce barriers, and enhance transparency by providing a common framework for product information. Global enterprises will be incentivized to adopt DPP to remain competitive and reduce costs.

The US Cyber Trust Mark is essential for raising market awareness. It will empower IoT consumers to make informed decisions about security and privacy of devices. It will enable enterprises in industrial, automotive, and aerospace-defense markets as well as governments to track and trace IoT systems, devices, and their parts, analyze vulnerabilities, uncover supply chain intrusions, and take proactive steps to mitigate risks and to create a cross-border *Digital Asset Trail* the will enable digital economies.

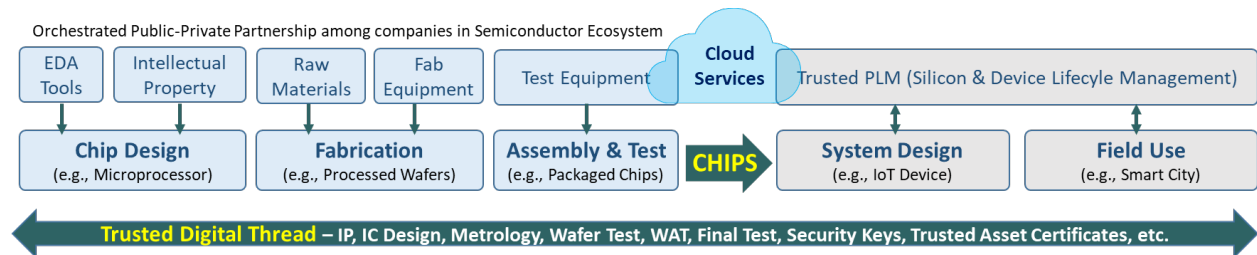
Customs and Border Protection can ease global ID harmonization. U.S. Customs and Border Protection (CBP) has initiated a Global Business Identifier pilot program¹⁵⁶ aimed at enhancing supply chain visibility and transparency. The program seeks to streamline the identification and verification of businesses involved in international trade of goods and enhance supply chain resilience. Unique business identifiers such as Enterprise IDs (producers, partners, distributors, consumers), asset IDs (HBOM, SBOM, and DBOM) workflow IDs (personas and tasks in design, manufacturing, etc.) linked with blockchain to trace transactions. The U.S. CBP tested the GSI standard to create a foundation for supply chain transparency, traceability and monetization.

The Cyber Trust Mark, Digital Product Passport, and Global Identifiers will help track and trace allied chips across supply chains regulate field use and strengthen national security and economic value.

Implementing Traceability Strategy Starting from CHIPS Acts

¹⁵⁶<https://www.cbp.gov/newsroom/national-media-release/cbp-launches-global-business-identifier-pilot-increase-supply-chain>

A strategy to establish a trusted digital infrastructure starting from chip design and manufacturing requires a multi-stakeholder, orchestrated Public Private Partnership (PPP) among companies shown in this diagram. While the individual enterprises cannot do this on their own, by collaborating they can create a digital infrastructure for traceability that enables economic value and revenue growth for all participating stakeholders. This strategy was proven to be viable with a consortium of companies.¹⁵⁷



In October 2023, the U.S.-EU joint summit statement¹⁵⁸ emphasized transatlantic collaboration on supply chain resilience, AI, and a secure digital ecosystem. The Department of Commerce can lead NIST, USTR, and the U.S.-EU TTC to coordinate CHIPS Acts subsidies on supply chain traceability by taking the following actions:

1. **Develop Standards Taxonomy:** Utilize NIST’s worldwide reach with Standards Development Organizations (SDOs) to lead in creating taxonomy of standards as part of our national strategy that facilitates trusted supply chain traceability across the electronics and IoT supply chains.
2. **Start Trusted Traceability Network:** Leverage the CHIPS Acts to orchestrate multi-stakeholder Public-Private Partnerships (PPPs) among EDA, IP, IC Design, and Foundry vendors to start a trusted digital thread from chip design and manufacturing linking business processes and assets.
3. **Promote Trusted Traceability Value:** Lead the USTR and the U.S.-E.U. TTC to promote cost-effective pilot projects with allied nations, which demonstrate the security and economic value of supply chain traceability with small-scale initiatives before committing funds for larger deployments.
4. **Increase Awareness and Cross-Border Trust:** Promote the U.S. Cyber Trust Mark along with the EU Digital Product Passport and Customs and Border Control Initiatives for supply chain visibility using Identifiers that enable “digital asset trail” and growth of trusted digital marketplaces.

¹⁵⁷ https://www.nist.gov/system/files/documents/2022/04/25/04-25-2022-GSA_TIES.pdf

¹⁵⁸ https://ec.europa.eu/commission/presscorner/detail/en/statement_23_5198

The federal government and semiconductor industry must act swiftly to adopt trusted traceability, authentication, and remote programming based on 'Root of Trust' embedded during chip design and manufacturing. Inaction could lead to dire consequences if adversaries control the Root of Trust. Conversely, embracing a trusted business ecosystem, guided by orchestration, governance, and network effects, will incentivize collaboration for economic growth among the U.S., our allies, and even adversaries adhering to the trusted ecosystem policies.

The U.S. should lead a global CHIPS-based traceability strategy with allied nations by using IoT technologies coupled with AI and cross-border digital partnerships to track and trace chips, fuel trusted digital marketplaces, strengthen national security, and contribute trillions to the global economy and our GDP.

Table of Abbreviations

(still being significantly updated)

AAM	Advanced Air Mobility
ADPPA	American Data Privacy and Protection Act
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
APEC	Asia-Pacific Economic Cooperation
AQ	Air Quality
ASCE	American Society of Civil Engineers
AASHTO	American Association of State Highway and Transportation Officials
AV	Autonomous vehicle
BABA	Buy America, Build America
BIL	Bipartisan Infrastructure Law
BIM	Building Information Modeling
BX	
CAGR	
CCPA	California Consumer Privacy Act
CESMII	
CET	Critical and Emerging Technologies
CIA	Confidentiality and Integrity and Assurance
CIO	
CISA	Cybersecurity and Infrastructure Security Agency
CPA	Colorado Privacy Act
CPAP	
CPRA	California Privacy Rights Act
CPS	Cyber-Physical System
CTDPA	
CV	Connected Vehicle
DBOM	Data IDs and Bills of Materials
DCS	
DFAR	Defense Federal Acquisition Regulation
DHHS	Department of Health and Human Services
DL	Deep learning
DoC	Department of Commerce

DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
EERE	
EIA	
EmT	Emerging Technology
EPA	Environmental Protection Agency
ERP	Enterprise resource planning
EV	Electric vehicles
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FDOT	Florida Department of Transportation
FedVTE	Federal Virtual Training Environment
FEM	
FRM	
FTC	Federal Trade Commission
GCTC	Global City Teams Challenge
GDPR	General Data Protection Regulation
GIST	Global Innovation through Science and Technology
GLS	
GSA	General Services Administration
HBOM	
HIPAA	
HVAC	Heating, ventilation and air conditioning
IAM	Identity and Access management
ID	Information and data
IoMT	Internet of Medical Things
IoT	Internet of Things
IoTAB	Internet of Things Advisory Board
IoTFWG	Internet of Things Federal Working Group
IP	Intellectual property
IRA	Inflation Reduction Act
IT	Information technology
ITU	International Telecommunications Union
KEV	Known Exploited Vulnerabilities
KPI	Key performance indicators
LEO	Low-earth orbit

LPWAN	Low Power Wide Area Networks
MBDA	Minority Business Development Agency
MEP	Manufacturing Extension Partnership
ML	Machine learning
MVA	Manufacture value added
NAAQS	
NDAA	
NEMA	
NESHAP	
NEVI	
NHTSA	National Highway Traffic Safety Administration
NICE	National Initiative for Cybersecurity Education
NIETC	National Interest Electric Transmission Corridors
NIST	National Institute of Standards and Technology
NITRD	
NOAA	
NSF	National Science Foundation
NSTC	National Science and Technology Committee
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
O&M	
ODM	Original design manufacturers
OEM	Original Equipment Manufacturers
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OSTP	Office of Science and Technology Policy
OT	Operational technology
PANDA	
PbD	Privacy by Design
PCAST	President's Council of Advisors on Science and Technology
PET	Privacy-Enhancing Technologies
PHI	
PID	
PII	Personally identifiable information
PoC	Proof of Concept
PPDSA	Privacy-Preserving Data Sharing and Analytics
PPE	Personal protective equipment
PPP	Public-private partnerships

PQC	Post quantum computing
PV	
QC	Quantum computing
RFID	
RFP	
ROI	
RSR	
SB	Small and disadvantaged businesses
SBA	
SBIR	Small Business Innovation Research
SBOM	
SCADA	
SCSEP	Smart City and Sustainability Extension Partnerships
SDO	Standards Development Organizations
SENSOR	
SMB	
SME	Small and medium enterprises
SSDF	Secure Software Development Framework
STEM	Science, technology, engineering, and mathematics
STTR	Small Business Technology Transfer
THEA	Tampa Hillsborough Expressway Authority
TMF	Technology Modernization Fund
UAS	
UF	University of Florida
UI	User interfaces
UNECE	
USDA	U.S. Department of Agriculture
USMCA	United States-Mexico-Canada Agreement
USNSS	
UX	
VC	
VOC	

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—	

Advisory Topic	Relevant Report Sections
(I) promote or are related to the privacy of individuals who use or are affected by the Internet of Things;	
(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.]