Report of the Internet of Things (IoT) Advisory Board (IoTAB)

OCTOBER 2024



Art credit: Design Consultants

Letter from the Chairs

To: The Internet of Things Federal Working Group

The United States is in the early stages of a profound transformation, one that is driven by economic, societal, and cultural innovations brought about by the Internet of Things (IoT). These innovations intertwine connectivity and digital innovation with the opportunity to drive a revolutionary metamorphosis across all parts of our nation.

We envision that this transformation will:

- Boost U.S. economic growth,
- Increase public safety and national resilience,
- Create a more sustainable planet,
- Individualize healthcare,
- Foster equitable quality of life and well-being, and
- Facilitate autonomous operations of our national infrastructure.

Today, this transformation is progressing more slowly than expected due to complex challenges and barriers that stand in our way. These challenges range from a lack of leadership and coordination, the lack of a U.S. National IoT strategy, lack of trust, technology, and infrastructure, to gaps in regulation and policy, and workforce limitations. Other challenges include potential cybersecurity concerns and trade and supply chain issues that merit special attention and should be studied further by Congress. Some of these challenges have been identified in previous efforts. For example, several IoT national security implications were outlined in a November 2014 report form the President's National Security Telecommunications Advisory Committee.[1]

The IoT Advisory Board (IoTAB) has prepared findings and recommendations to realize opportunities and overcome challenges. Development of this report adhered to the IoTAB charter and applied the IoT members' collective expertise, supported by thoughtful insights from subject matter experts and members of industry and the public. We organized our recommendations into six key enabling themes - government leadership, infrastructure modernization, security and trust, workforce development, adoption and unlocking the IoT economy.

This report is a starting point and reflects a point-in-time perspective. The IoTAB considered the topics in the charter, and the limited time and information available. Although this report is extensive, the Internet of Things is more so. Further work is required to examine and consider additional important topics in more detail, including:

- The impact of integrating IoT with critical infrastructure
- The growing impact of AI with IoT (AIoT)
- IoT technology and communications infrastructure
- Data management and governance
- Evolving from legacy systems and technologies
- The slow and uneven adoption of smart cities
- The impact of "Right to repair" on adoption and cybersecurity

Overcoming these challenges and implementing the changes needed requires national leadership. It requires a "whole-of-government" approach leading with vision, imagination, and innovation, executing with passion and relentless determination, with unwavering commitment for the betterment of all Americans. It requires a long-term commitment from government, industry, communities, and

[1] The President's National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things" (November 19, 2014) available at https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

academia working collaboratively with a sense of urgency. It requires change agents challenging "business as usual" and the status quo. It requires funding and resources.

We cannot falter. The full integration of IoT into our economy, civil society and communities is not an option; it is an imperative for the United States in order to remain relevant now and in the future. We must lead with vision, American values, imagination, and relentless determination to build a future where connectivity transcends boundaries, propelling our economy to new heights, fostering societal well-being, and ensuring that the United States remains at the forefront of global innovation. If we do not or cannot, others will lead and dictate the direction and nature of our transformation.

This report contains our findings and recommendations, based on industry experiences and perspectives from a cross-section of industry, local government, and academia. We urge the IoT Federal Working Group, Congress, and industry to study and adopt these recommendations in recognition of the critical importance of this effort at this pivotal time.

Benson Chan
Chair, Internet of Things Advisory Board
Chief Operating Officer, Strategy of Things LLC

Dan Caprio
Vice-Chair, Internet of Things Advisory Board
Co-Founder and Chairman, The Providence Group

IoT Advisory Board Members

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

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
Former Chair of Trusted IoT Ecosystem Security (TIES)
at the Global Semiconductor Alliance and
CEO of Archon Design Solutions, Inc.

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
General Partner,
Agorai Funds

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.

Table of Contents

Letter from the Chairs i

IoT Advisory Board Members iii

Table of Contents iv

Executive Summary 1

IoT unlocks economic prosperity, innovation, and societal well-being. 1

Key challenges are hindering IoT adoption and scaling. 2

Call to Action: Leading the Way Forward 3

Background 5

Introduction to the Internet of Things. 6

What is IoT? 6

What Can IoT Do? 7

The Current State of IoT 9

Market Consolidation 12

Technology Maturity 13

The IoT-enabled Economy 14

The Evolution of IoT 14

A Vision for the IoT-enabled Economy 14

Facilitating the IoT-enabled Economy 16

End-to-end IoT Solutions Platforms 16

Platform-based IoT Business Ecosystems 18

Orchestrated business partnerships 18

Evolution of IoT Economy and Potential to Gross Domestic Product (GDP). 19

Findings of the IoT Advisory Board 21

General Findings 22

Industry Specific Findings 44

Recommendations of the IoT Advisory Board 57

Government Leadership 63

Key Recommendation KR1.1: Congress and the Executive Branch should work together to establish a United States national strategy for taking full advantage of the opportunity presented by the IoT. 63

Key Recommendation KR1.2: Congress should accelerate IoT technology innovation to support an evolving IoT. 66

Key Recommendation KR1.3: The Executive Branch should promote international collaboration in IoT adoption to share knowledge, best practices, and resources; harmonize standards, policies, and regulations; and facilitate trade. 70

Key Recommendation KR1.4: The Executive Branch should lead by example by specifying, procuring, and adopting IoT by federal agencies for its internal use. 71

Modernizing IoT Infrastructure 74

Key Recommendation KR2.1: The Executive Branch should promote collaborative development across industries to adopt existing industry standards and protocols that enable IoT interoperability. 74

Key Recommendation KR2.2: The Executive Branch should establish methods to foster interoperability for IoT technology to the greatest extent possible, through the use of consistent models, protocols, application interfaces, and schemas. 78

Key Recommendation KR2.3: The Executive Branch should expand and improve programs that ensure sufficient availability, reliability, quality of service and connectivity to support IoT in all areas of the country. . . . 80

Key Recommendation KR2.4: The Executive Branch should encourage businesses and organizations to embark on initiatives to digitalize and transform their operations and processes in order to take advantage of IoT and the IoT-enabled economy. 84

Establish Trust in IoT 87

Key Recommendation KR3.1: NIST should continue to provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach. 87

Key Recommendation KR3.2: Congress should pass comprehensive federal privacy legislation. 92

Key Recommendation KR3.3: The Executive Branch should support trusted IoT architectures and infrastructure that enable supply chain provenance, and traceability of IoT systems starting from chip design and manufacturing. 97

Fostering an IoT-Ready Workforce 100

Key Recommendation KR4.1: Congress and the Executive Branch should integrate the needs of the future IoT workforce into existing initiatives and programs with industry, academia, and state and local government efforts. 100

Facilitating Industry Adoption of IoT 103

Leverage Federal Grants and Programs to Facilitate IoT Technology Adoption and Use 103

Key Recommendation KR5.1: Congress should consider new financial models for sustaining and supporting programs when evaluating IoT project feasibility in federal grants. 103

Key Recommendation KR5.2: Congress and the Executive Branch should develop a comprehensive Agricultural IoT Strategy. 104

Key Recommendation KR5.3: Congress and the Executive Branch should implement specific actions to further promote IoT adoption through smart cities and communities. 107

Key Recommendation KR5.4: The Executive Branch should promote IoT adoption that will improve public safety. 111

Key Recommendation KR5.5: Congress and the Executive Branch should promote IoT adoption in the health care industry. 112

Key Recommendation KR5.6: Congress and the Executive Branch should promote IoT adoption that will improve sustainability and environmental monitoring. 115

Key Recommendation KR5.7: Congress and the Executive Branch should promote IoT adoption in Smart Transit and Transportation. 118

Promoting an IoT-enabled Economy 120

Key Recommendation KR6.1: The Executive Branch should monitor and evaluate progress of IoT adoption for supply chain logistics 121

Key Recommendation KR6.2: The Executive Branch should facilitate public-private partnerships (PPPs) focused on IoT adoption to advance collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia developing end-to-end IoT solutions in supply chain logistics 122

Key Recommendation KR6.3: The Executive Branch should actively facilitate and support the adoption of AI in IoT applications to improve decision-making, optimize resource utilization, and enhance productivity 124

Key Recommendation KR6.4: Congress and the Executive Branch should provide overarching regulatory guidance for the unmanned aerial systems (drone) industry 125

Key Recommendation KR6.5: The Executive Branch should promote, facilitate, and monitor equity in the accessibility, realization and distribution of value and benefits created from the adoption and use of IoT 126

Closing Thoughts from the IoT Advisory Board Chairs 127

Additional References 131

Acknowledgements 132

Appendix A: IoT Stakeholders 134

Manufacturers 134

Developers 134

Implementers 135

Administrators 135

Operators 136

Consumers 136

Table of Abbreviations 137

Executive Summary

The world is undergoing a fourth industrial revolution, driven by the economic, societal, and cultural innovations of the Internet of Things (IoT). This revolution combines connectivity and digital innovation with the physical world to accelerate economic, environmental, and social benefits across the world.

The United States is at a critical juncture: the Internet of Things (IoT) is rapidly evolving and presents a historic opportunity to leverage American innovation and ingenuity to sustain economic leadership and accelerate achievement of societal benefits.

IoT adoption is not just an option; it is an imperative for the United States to lead with vision. It's a call to embrace a future where connectivity transcends borders and global trade, driving our economy to new heights, fostering societal well-being, and ensuring that America remains at the forefront of global innovation.

IoT unlocks economic prosperity, innovation, and societal well-being.

By integrating the physical with the digital to interconnect devices, systems, and people, we envision an Internet of Things that enables a more resilient nation. We can pave the way for a better tomorrow where technology serves as a powerful tool for humanity in the progress, prosperity, and a future we all can share - and:

- **Boost economic growth.** IoT can unlock possibilities and efficiencies that were once deemed unimaginable to redefine industries, create new business models, increase competitiveness, and empower innovation. Smart manufacturing keeps American factories competitive against overseas competitors. Precision agriculture innovations increase crop yields while minimizing inputs in changing climate conditions. Businesses, enabled by smart supply chains that are agile and resilient, become more profitable.
- **Increase public safety.** IoT can enable agile and effective actions to prevent, protect, mitigate, respond to, and recover from human made and natural disasters and hazards. Sensors embedded in roads and related roadside infrastructure inform engineers and planners of new ways to minimize accidents. 911 systems integrated with smart city technologies provide full situational awareness and help operators dispatch the most effective and appropriate resources. Smart buildings keep occupants safe against intruders, fires, and other hazards.
- **Create a more sustainable planet.** IoT can revolutionize the way we use natural resources and protect the environment. Precision agriculture reduces water consumption and minimizes the use of fertilizers and pesticides. Smart grids dynamically adjust energy distribution based on demand and maximize the use of renewable energy sources. Smart buildings reduce energy consumption. Smart traffic management systems optimize traffic flow while reducing congestion and emissions.
- **Individualize healthcare.** IoT is a catalyst for redefining patient care, clinical practices, and the overall healthcare landscape. Wearable devices can allow physicians to monitor patients outside traditional clinical settings, enabling early detection of health issues, personalized interventions, and a shift towards proactive, preventive care. Smart medical devices collect targeted data about a patient, which can be analyzed to deliver personalized and precision medical treatments. IoT systems can analyze patient data to predict potential health issues before they become critical. And early warnings allow for proactive, personalized interventions, potentially preventing serious health events.
- **Foster equitable quality of life and well-being.** Smart medical devices can enhance telehealth capabilities, enabling patients in rural and remote communities to receive quality healthcare from doctors hundreds of miles away. Smart homes enable seniors and disabled adults to live independently. Smart mobility businesses improve accessibility for seniors, disabled individuals, and residents with limited transportation options. Smart agriculture increases productivity and supports economic vitality in rural communities. Smart environmental monitoring systems help to identify and address pollution in marginalized communities. Smart classrooms provide educational access to all Americans, regardless of where they live.
- **Facilitate autonomous operations of U.S. critical infrastructure.** IoT provides the foundation for smart-connected applications by leveraging connectivity and real-time data essential for AI-driven systems. When combined with AI, IoT enhances data analysis, automation, and decision-making, enabling autonomous operations and smart infrastructure. This integration boosts efficiency and fosters proactive maintenance and automation, leading to more resilient infrastructure, supply chains and optimized resource management. The synergy between IoT and AI accelerates innovation across diverse fields such

as healthcare, manufacturing, energy, and smart cities, driving economic security, competitiveness, and growth.

An IoT-enabled economy can significantly boost the U.S. GDP. IoT is no longer just a device connected to the Internet but is evolving to include integrated components within larger ecosystems (i.e., systems of systems) and embedded across communities at large. The data that flows through these devices, platforms that process the data, mobile and computing applications that are used as interfaces, and the backend cloud components are all distributed across a vast array of physical infrastructure which is expanding. Technology is accelerating at an ever-increasing rate at various levels of maturity which overlap with the billions upon billions of dollars in value of the underlying data and applications that these IoT provide to Americans.

Key challenges are hindering IoT adoption and scaling.

Despite these opportunities and benefits, the adoption of IoT across industry, communities, and civil society in the United States has not evolved to its full potential. The U.S. is not alone. Over the past decade, industry analysts have noted that global economic investment in IoT has not met estimated targets due to slow adoption, with shortcomings attributed to a variety of factors, such as change management, cost, talent, cybersecurity, and privacy. However, the convergence of physical and digital worlds promises to accelerate adoption if these challenges and barriers are addressed.

This IoTAB was chartered to assess the challenges and identify recommendations that position U.S. leadership to seize economic and societal opportunities that benefit government, businesses, schools, communities, and Americans. The IoTAB identified general findings and specific considerations that reveal ways in which the U.S. can close existing gaps. The IoTAB's recommendations could have the potential to reposition the U.S. as a leader in accelerating adoption and growth of IoT, increasing capabilities and resources, bridging a future landscape, and addressing cross-sector critical gaps as called out in the charter for this report.

Each of these recommendations is linked in the report to one or more of the themes as shown in Figure 1.

The IoTAB's recommendations address the challenges identified by key findings.

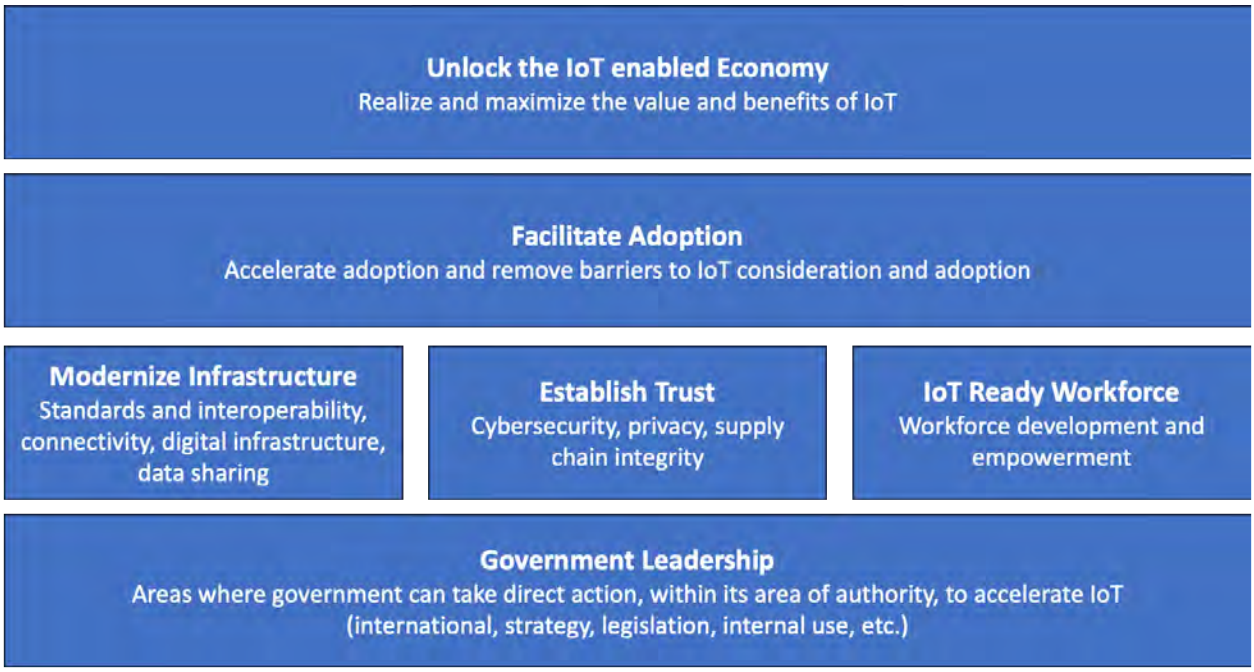


Figure 1 - Themes Used for the IoTAB Recommendations.[2]

[2] Figure credit: Benson Chan, used with permission.

CHALLENGES	FINDINGS
Adoption and Growth	• Slow industry and community adoption • Lack of national coordination • Obstacles to innovation • Limited equity and opportunities • Significant barriers for small businesses • Interoperability challenges • Connectivity challenges • Lack of trust including cybersecurity and privacy concerns
Capabilities and Resources	• Startups that drive new technology • New business models and platforms to scale • Growth of AI is critical to unlocking value of IoT • Insufficient people with the skills needed (i.e., workforce readiness) • Vulnerable supply chains
Future IoT-enabled Economy	• Evolution of business partnerships needed for solutions • Creation of open digital marketplaces to fuel economic growth • Challenges to the convergence of AI and IoT • Cybersecurity threats from quantum computing
Challenges for the Sectors Identified in the Charter	• Agriculture: uneven and slow adoption. • Smart communities in the U.S.: rollout is limited & inconsistent • Transportation: privacy, safety, and liability concerns • Healthcare: trust & interoperability challenges • Supply chain: better global visibility & transparency are needed • Environmental sustainability: Better connectivity & technology innovation • Public safety outcomes: technical, community and policy challenges

Addressing these challenges presents tangible benefits to the larger U.S. economy including job creation, workforce development, market access, resource optimization, and synergies between technological advancements. Such examples include:

- **Promoting widespread IoT adoption and growth,** offers a historic opportunity for U.S. leadership. This can be achieved by overcoming adoption hurdles and fostering a coordinated national strategy to drive innovation, inclusive growth, and a thriving business ecosystem of all sizes.
- **Developing capabilities and resources,** like nurturing innovative startups, promoting scalable business models for IoT, and integrating AI expertise, are crucial to unlocking the full potential of IoT and adjacent technologies using existing skills and sustaining American innovation leadership.
- **Investing in the Future IoT Economy,** by promoting platforms, public private partnerships and digital marketplaces leveraging IoT and integrating AI with IoT will unlock their full potential, bringing economic benefits and building a skilled workforce.
- **Addressing critical sector needs,** by paving the way for new opportunities to accelerated adoption across industries including agriculture, healthcare, transportation, environment sustainability, and public safety.

Call to Action: Leading the Way Forward

Despite the unlimited potential and benefits of this transformation, significant challenges stand in the way. It is imperative that the nation embraces the potential of IoT, acknowledge and overcome challenges, and proceed deliberately to realize IoT's benefits for our economy and society. We must act with the same qualities that built our nation - leading with vision and innovation, executing with passion and tenacity, and persevering with unwavering c ommitment for the betterment of all Americans and our allies.

The U.S. must begin to strategically examine how to bridge the gap between the present and a promising tomorrow through collective action and a nationwide commitment to embracing the transformative power of IoT and overcoming the challenges that exist today.

This report presents the IoTAB's findings and provides actionable recommendations under overarching themes that serve to guide the U.S. towards an IoT-enabled future. This includes experiences and perspectives from a cross-section of industry, local government, academia, and other private-sector experts.

The report recommends that the IoT Federal Working Group (IoTFWG) consider (and where appropriate, document the planned or existing implementation of) these findings and recommendations. The IoTAB further urges the IoTFWG and Congress to adopt those recommendations that will best serve the needs of this nation.

The IoTAB members urge the federal government to carefully consider these recommendations and findings, and act on them with vision, boldness, urgency, and decisiveness, and take a whole-of-government approach to implement the IoTAB's recommendations. Monitoring progress and measuring outcomes in a public and transparent manner is also critical to success. For a full list of recommendations, see the table at the start of the Recommendations Section on page XX. Some of the IoTAB's recommendations include:

- Develop a U.S. national IoT strategy to lead the world in IoT adoption.
- Create a National Coordination Office for IoT and adjacent technologies.
- Incorporate IoT in a comprehensive federal privacy bill.

- Investigate the impact of IoT modules and chips from adversary nations.
- Prepare and build an IoT ready workforce.
- Assess the impact of IoT on supply chains and critical infrastructure.
- Form a CEO-level IoT Advisory Board that reports to the President.
- Conduct further study of the intersection of AI, quantum computing and IoT.

Background

In January 2021, Congress enacted the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. That act established the Internet of Things Advisory Board (called the "Board" in the charter) within the Department of Commerce.[3] In accordance with the Federal Advisory Committee Act, as amended, the IoTAB was chartered in December 2021.

The IoTAB convened in 2023 and conducted 14 meetings[4] to consider the challenges and opportunities related to IoT adoption, particularly those areas described in the aforementioned legislation.

The IoTAB was chartered[5] to provide advice to the Internet of Things Federal Working Group (IoTFWG). Specifically, this charter requires the following:

Description of Duties.

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 IoTFWG 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 IoTFWG 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.

The chapters, findings and recommendations below represent the result of the work of that Advisory Board.

[3] Public Law No. 116-283, Section 9204(b)(5)

[4] Recordings and minutes of all Internet of Things Advisory Board meetings are available at https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/iot-advisory-board

[5] The IoTAB's charter is available at https://www.nist.gov/system/files/documents/2023/09/27/84643-DOC-2023-CharterRenewal-IoTAB-9.18.2023.pdf



Photo credit: Shutterstock

Introduction to the Internet of Things

What is IoT?

Generally speaking, the Internet of Things (IoT) is composed of devices or distributed systems embedded with sensors and actuators that are connected to the Internet enabling them to interact with and influence the physical world. As a result, IoT can be seen as a collection of interconnected technologies that work together to create innovative outcomes and applications fostering new business models and revenue streams.

Technologically, IoT systems are connected computing devices enhanced with sensors that gather data from the physical world, and some include actuators that take actions based on the processed data. IoT data may be processed locally on the device, on a nearby local server ("the edge"), or sent over the Internet to be handled off-premises ("the cloud").

The "cloud" collects the data, stores it, analyzes it, and acts on it. The information may then be routed or made available to business or industrial execution systems, such as enterprise resource planning (ERP) systems, operations execution software applications, for additional action.

For example, consider a sensor that measures the vibration level of an automated milling machine in a large factory. The information is sent to a cloud data center, where the vibration measurement is reviewed by algorithms. If high, out-of-spec levels are detected, a command is sent to turn off the milling machine and schedule the machine for maintenance and repair. This early detection prevents the machine from unplanned downtimes, which would disrupt manufacturing operations.

A high level IoT technical architecture is shown below in Figure 2.

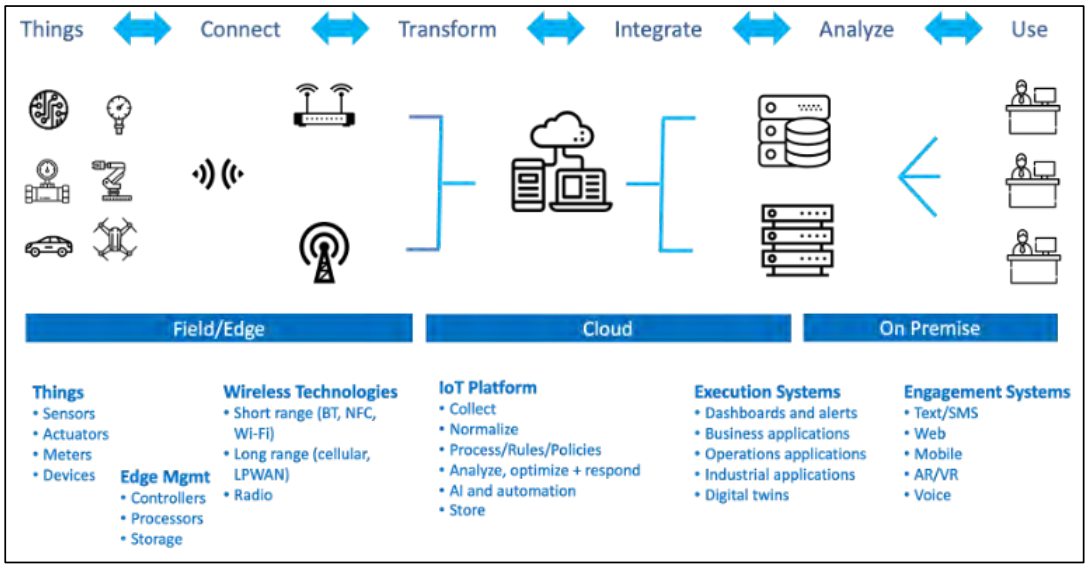


Figure 2. High-Level Internet of Things Architecture[6]

[6] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024. Included with permission of the authors.

What Can IoT Do?

IoT Transforms Product Value

IoT transforms business value by providing real-time data and connectivity that drive smarter decision-making and operational efficiency. By integrating IoT with other technologies, businesses can automate processes, enhance customer experiences, and optimize resources. This leads to innovative solutions, reduced costs, and new revenue opportunities, significantly boosting economic value.

From an economic perspective, adding sensors and actuators to the Internet creates value by enabling traditional tasks to be performed in innovative ways and by making new possibilities achievable. Examples include:

- **Asset Tracking:** IoT enables real-time tracking of assets using sensors and GPS, providing visibility into location, status, and condition. This improves operational efficiency, reduces loss, and enhances asset utilization.
- **Equipment Condition Monitoring:** IoT sensors continuously monitor equipment and machine parameters such as temperature, vibration, and performance metrics. This data helps predict potential failures, optimize maintenance schedules, and extend equipment lifespan, reducing unplanned downtime and operational costs.
- **Predictive Maintenance:** IoT collects and analyzes data from equipment to predict maintenance needs before breakdowns occur. This proactive approach minimizes unplanned downtime, improves reliability, and lowers maintenance costs by scheduling repairs based on actual usage and condition.
- **Autonomous Operations** IoT systems in sectors like agriculture automate tasks like irrigation, fertilization, and pest control based on real-time data from sensors and weather forecasts. This optimizes resource use, increases yield, and supports sustainable farming practices by reducing environmental impact.

These are just a few examples that illustrate how IoT transforms existing processes and introduces new opportunities.

IoT Enables New Business Models

Adding connectivity and sensors to traditional products create smart, connected products. These products allow suppliers to develop innovative offerings based on new business and operating models, leading to new revenue streams not possible with traditional non-connected products. In this way, suppliers transform their business from just selling "products" to become "smart connected solutions suppliers" with IoT-enabled services or by offering, "products as a service". This allows suppliers to better align with their customers' needs, increasing their competitiveness and value, and ultimately, profitability.

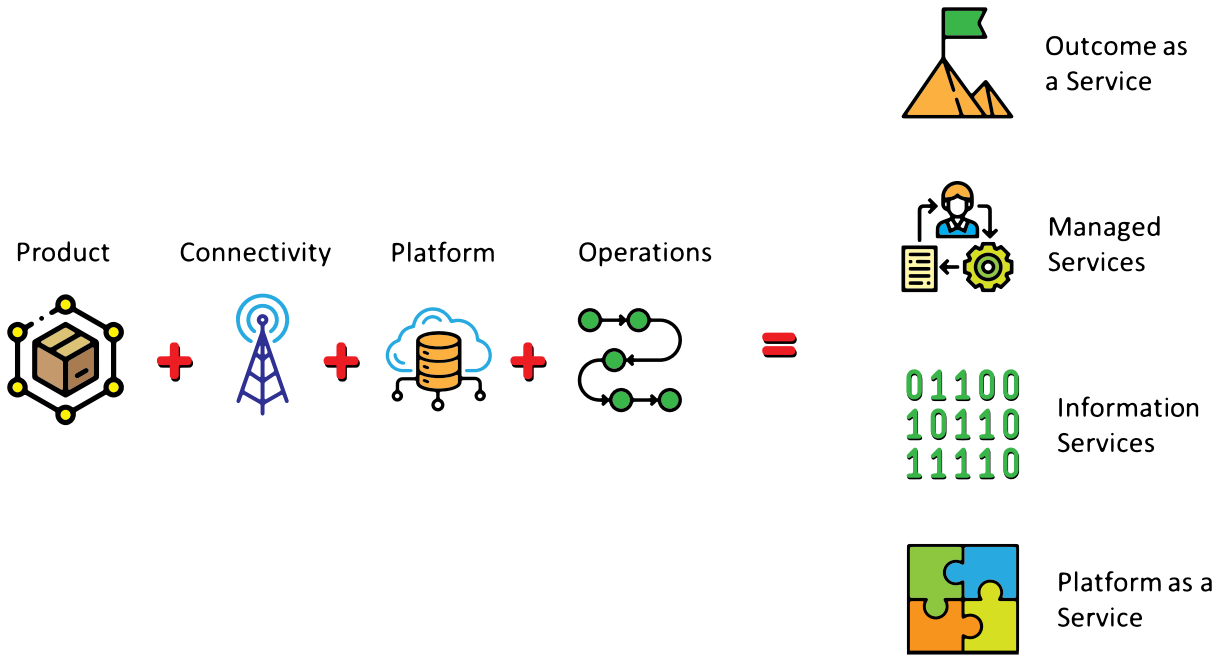


Figure 3. New offerings enabled by smart connected products.[7]

[7] Figure Credit: Benson Chan, used with permission.

For example, connected sensors on IoT-enabled equipment allows jet engine manufacturer Rolls Royce to take over engine maintenance responsibilities from the airlines. In exchange for a fixed cost per flying hour, Rolls Royce actively manages the engine, throughout its lifecycle, to ensure maximum flying availability, while providing the airlines with a predictable cost of ownership.[8]

For buyers and users, these new offerings provide increased capabilities and value (Figure 3). For example:

- **Suppliers sell "outcomes" delivered by their products.** The example cited above, sells "flying availability". The money saved by buying "outcomes" can be redeployed to another part of the business. For suppliers, this model enables focus on customer success, and provides them with a sustainable, recurring revenue stream instead of a one-time sale.
- **Connected systems allow dealers to offer new services.** Product suppliers and their dealers have traditionally relied on two sources of revenue: sales of equipment and maintenance service contracts. Connected systems allow dealers to offer new managed services, which remotely monitor equipment use and predict when maintenance is needed, to help customers proactively avoid costly unplanned equipment downtime. They can also provide remote updates and upgrades based on observing the changing customer and application needs.
- **Product suppliers become information providers.** The data aggregated from all the sensors is of value to other related participants in the industry ecosystem. For example, a shipping company can collect maritime IoT fleet data and make it available to charterers, insurance companies, classification societies, and academia.
- **Product suppliers transform to solutions providers through IoT platforms.** For example, Amazon's Alexa smart speakers allow other smart products to add voice control by allowing them to integrate to its voice platform. This extends the product ecosystem and allows other products to interoperate and collaborate to provide an end-to-end solution to customers.

IoT Enables New Business Ecosystems

Smart-connected products create new value by changing the way manufacturers compete. The basis of competition shifts from selling discrete products to offering product systems to systems of systems, to platform ecosystems and marketplaces.[9]

A car with integrated sensors, software, and connectivity adds new value beyond a traditional car. By analyzing collected data, this smart car allows the manufacturer's dealers to monitor the

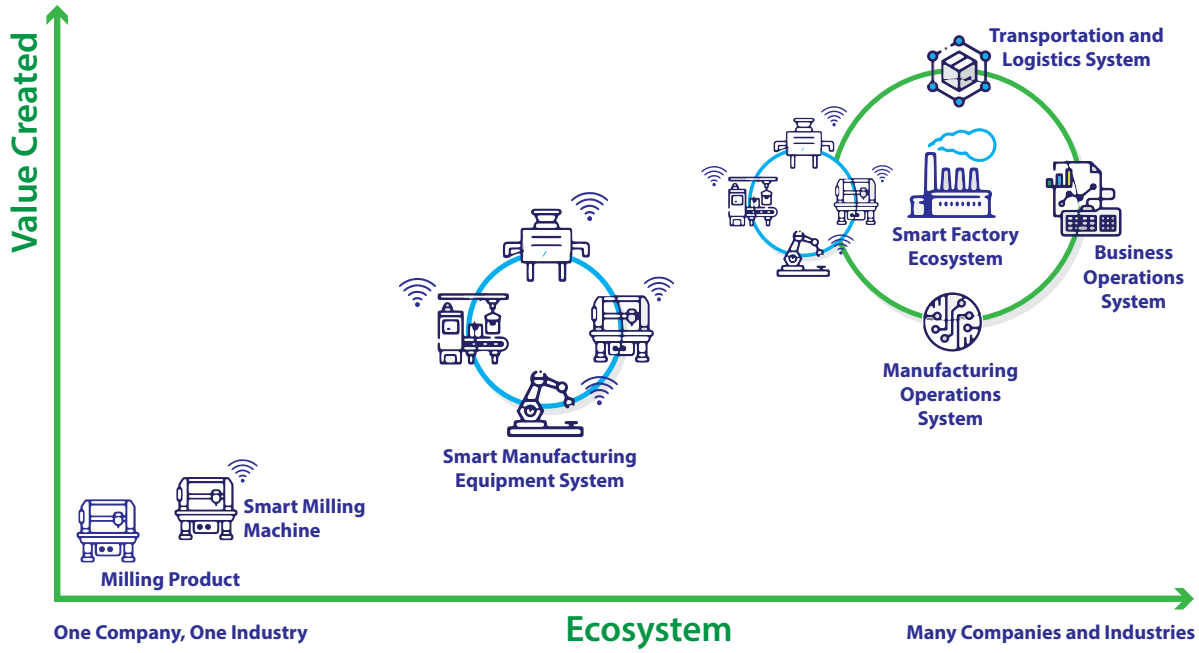


Figure 4. Evolution of smart-connected products to partner-based business ecosystem[10]

[8] "Total Care Circular Business Model", Rolls Royce, available at https://www.rolls-royce.com/media/our-stories/discover/2017/totalcare.aspx

[9] "How Smart Connected Products are Transforming Competition", Michael E. Porter and James E. Heppelman, from *Harvard Business Review* (November, 2014) available at https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition

[10] Figure Credit: Benson Chan, used with permission.

status of the car, determine its maintenance needs, and optimize gas mileage performance.

Suppliers increase their value to customers by allowing compatible products from other suppliers to use their software platform. This creates a product system where different product makers share a common platform, exchange data, and collaborate. For example, a car manufacturer can allow third-party smart speakers to be integrated with a manufacturer's smart car platform. Drivers can then use voice commands to control some car functions. Insurance companies can develop and integrate telematics systems that monitor driving behavior and create personalized insurance policies. For customers, the solutions and services from the third-party ecosystem solution providers create safer driving, personalized owner experiences, and lower ownership costs.

As these solution platforms evolve and grow in capability, they participate in a broader ecosystem beyond the original products. For example, the smart car ecosystem becomes part of the smart city ecosystem (Figure 4) where its onboard sensors and systems may communicate with traffic infrastructure, smart parking systems, charging systems, and public safety systems. Electric vehicles may connect with the local grid to store and offload electricity as needed. Onboard vehicle sensors alert city workers to street conditions.

Some benefits of these connected ecosystems include:

- **Smart-connected product businesses accelerate adoption.** Such businesses integrate innovative third-party products and services to create value and drive growth. From manufacturing to agriculture and aviation, similar opportunities and evolution are happening. Companies that deliver smart-connected solutions with ecosystem partners deliver higher value and grow faster.
- **Companies whose products connect to other systems capture more value.** Partnerships drive innovation and create new value, by expanding industry boundaries. Software platforms and applications may differ from industry to industry, but opportunities for collaborative ecosystem partnerships remain the same. 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.
- **Orchestrated end-to-end solutions partnerships accelerate growth.** Smart business ecosystems evolve through partnerships for end-to-end solutions which accelerate growth by combining stakeholder existing products with new technologies. Some ecosystems, such as smart cities and supply chains, are complex "system-of-systems" that benefit from orchestrated ecosystem collaboration. This, in turn, can incentivize businesses to participate, share the innovation burden, and deliver economic value.
- **Collaborative efforts across multiple stakeholders drive higher value** with platforms that encourage business ecosystem participation and innovation. For instance, OEMs can partner with municipalities and urban planners to deploy IoT-based smart city solutions. IoT sensors and data analytics can be used to optimize resource allocation, reduce environmental impact, and attract investment in digital infrastructure, driving economic growth.

The Current State of IoT

IoT Trends Worldwide.

The convergence of physical and digital worlds enabled by IoT has been recognized as a fundamental trend underlying the digital transformation of businesses that can fuel the global economy.

In 2014, the World Economic Forum and McKinsey and Company. projected that IoT, and adjacent technologies (analytics, cloud computing, big data, and ML/AL) would produce up to $21.6 trillion of value for the global economy by 2022.[11]

In 2021, McKinsey and Company. revised the IoT forecast downward by 42%, projecting global value of only $5.5 to $12.6 trillion, and not reaching those targets until 2030.[12] The revision was attributed to headwinds related to change management, cost, talent, and cybersecurity. Furthermore, other factors noted the slow market adoption of digitalization and cyber-resilience, particularly in large enterprises.

[11] Fon Mathuros, "Increased Cyber Security Can Save Global Economy Trillions", World Economic Forum, available at https://www.weforum.org/press/2014/01/increased-cyber-security-can-save-global-economy-trillions/

[12] Michael Chui, Mark Collins, and Mark Patel, "IoT value set to accelerate through 2030: Where and how to capture it", McKinsey and Company Report (November 9, 2021) available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

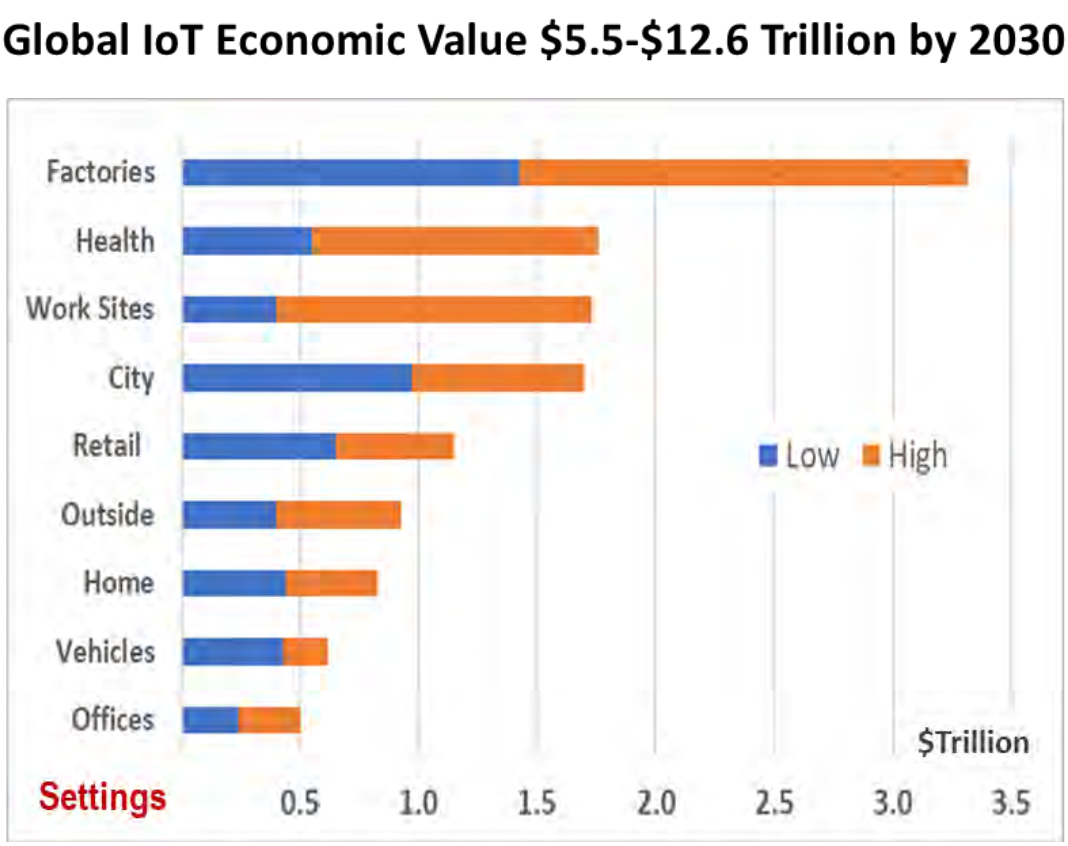


Figure 5. Estimated 2030 economic value of IoT adoption by setting.[13]

As of 2024, The global GDP stands at approximately $100 trillion,[14] with the U.S. GDP contributing around $25 trillion, or 25% of the global economy. Based on the above projection of global IoT economic value, IoT and adjacent technologies could add $1.37 to $3.15 trillion to U.S. GDP and even more if we invest in addressing barriers that accelerate adoption of IoT. Leveraging IoT's potential can significantly boost the U.S. economy by enhancing productivity, fostering innovation, and optimizing resource utilization. This economic growth can, in turn, increase national revenues, thereby contributing to reducing the national debt or $35 trillion and ensuring long-term financial stability.

Despite the potential of IoT to grow global economic value, the rate of adoption and growth has been slow as analysts did not foresee the barriers to deployment that significantly slowed IoT growth. Cited barriers to adoption include upgrading legacy infrastructure, managing enterprise silos, harmonizing technology, data, and interoperability challenges, tackling fragmented supply chains, and delivering end-to-end IoT solutions which require broad partnerships and diverse expertise.

[13] Figure Credit: Tom Katsioulas using data from Michael Chui, Mark Collins, and Mark Patel, "IoT value set to accelerate through 2030: Where and how to capture it", McKinsey and Company Report (November 9, 2021) available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it . Figure used with permission.

[14] Pallavi Rao, "Visualizing the $105 Trillion World Economy in One Chart", Visual Capitalist (August 9, 2023) available at https://www.visualcapitalist.com/visualizing-the-105-trillion-world-economy-in-one-chart/

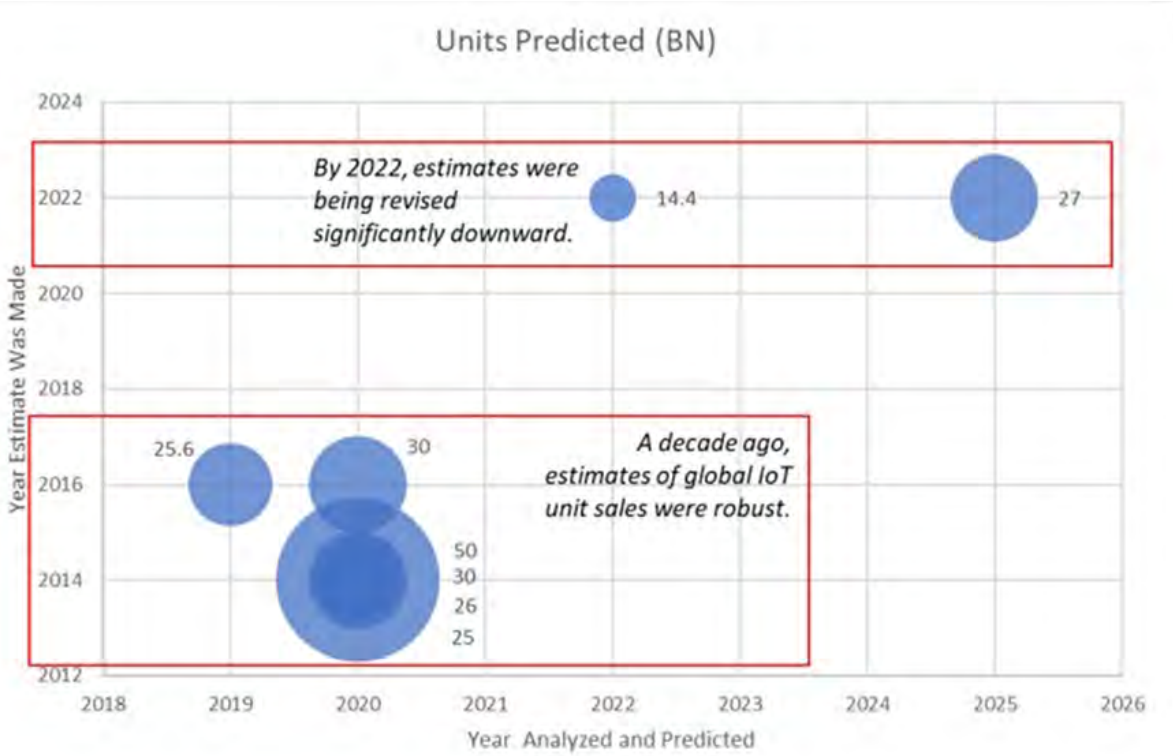


Figure 6. Changing industry forecasts on IoT adoption. Bubble size is proportional to the estimate.[15]

IoT Trends in the U.S.

The adoption of IoT is growing in the United States, likely driven by digitalization of enterprises. 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",[16] either learning about IoT, conducting a trial or proof of concept, or using IoT. Of those surveyed, 27% have projects in the "use" phase, while 78% reported that they are planning to use IoT more within 2 years. According to Fortune Business Insights, the value of the U.S. IoT market is expected to quadruple by 2030 Despite this interest, IoT adoption is still emerging, and timelines remain longer than anticipated.

IoT use and adoption rates vary for each industry, as well as the benefits and economic value. Examples include:

Manufacturing: Small manufacturers prioritize improving operational processes, cutting production costs, and addressing labor shortages. Smart manufacturing goals include better capacity utilization, cost reduction, on-time delivery, operational excellence, and improved quality.

Agriculture: IoT solutions mitigate labor shortages in farming, with an estimated 250,000 U.S. farms using IoT, mainly in livestock and crop management. Up to one-half of all U.S. farms show interest in IoT solutions, potentially representing 1.1 million farmers and a $4 billion market opportunity.

Retail: Major retailers focus on IoT to differentiate competitively, maintain margins, reduce operational costs, and enhance speed and agility. Key IoT use cases include inventory accuracy, fraud prevention, fulfillment center automation, supply chain optimization, personalized customer experience, and brand protection.

[15] Figure Credit: Michael Bergman, used with permission. This his is a custom graphic aggregating data from a variety of sources:
- Gartner (via DigiTimes), http://www.digitimes.com/news/a20140321PR201.html;
- Gartner (via Economist), http://www.economist.com/blogs/babbage/2014/05/difference-engine-1?fsrc=scn/tw/te/bl/ed/internetofnothings;
- International Data Corporation (via eMarketer), http://www.emarketer.com/Article.aspx?R=1011045;
- Gartner (via ZDNet), http://www.zdnet.com/internet-of-things-component-market-set-for-rapid-growth-7000035336/;
- Gartner (via Cellular News), http://www.cellular-news.com/story/Reports/67066.php;
- Gartner (via ZDNet), http://www.zdnet.com/article/smartphones-ultramobiles-and-iot-drive-semiconductor-sales-through-2015-says-gartner/;
- Gartner (via Cellular news), http://www.cellular-news.com/story/63407.php

[16] "IoT Signals - Edition 3|October 2021", Exhibit 3, Microsoft (October 2021) available at https://advcloudfiles.advantech.com/cms/ff14b6b1-7b24-40b5-843f-b6d43da293b4/Industry%20Focus%20%20PDF%20File/IoT-Signals_Edition-3_English_2.pdf

Transportation and logistics: IoT tracks real-time locations and quantities of goods, optimizing logistics and minimizing disruptions. Shipments of telematics devices are increasing, with an estimated 160 million units by 2026. Embedded car OEM telematics units are also growing, with 375 million units projected to be in use by 2026.

Projections continue to be robust, but it is important to see these promises fulfilled. Recent projections by vertical market are given below.[17]

Market Consolidation

The IoT market is an organically developing from a fragmented ecosystem of sensors, chips and processors, modules, devices, and software platforms.[18] The IoT platforms landscape is beginning to consolidate, as reported by IoT Analytics.[19] The fragmented nature of the market and lack of ubiquitous end-to-end solutions has created confusion for buyers who struggle with adopting IoT technology from many suppliers.

Today, this large and fragmented IoT market is consolidating to create value for buyers, scale, and profitability at the current market levels.

Evidence for this consolidation may be seen in recent mergers, acquisitions and, divestments including: IoT module maker Telit acquiring Thales cellular IoT division;[20] Semtech acquiring Sierra Wireless;[21] Google exiting the IoT services business;[22] Ericsson selling its IoT business;[23] IBM shutting down Watson IoT;[24] SAP retiring IoT platform;[25] and Cisco exiting the smart city market.[26]

Since 2019, most of the remaining IoT platforms are transitioning into IoT solutions offering significant benefits. For example, John Deere is developing an ecosystem of connected farm machinery to improve precision farming and asset monitoring. The Port of Rotterdam uses IBM Watson and Cisco IoT gear to optimize port logistics. Volkswagen has partnered with AWS and Siemens to create an Industrial Cloud that connects its supply chain and enhances it with a digital marketplace. Enel, an Italian energy company, used the C3 AI platform to double its performance by identifying unbilled energy. These solutions illustrate the transformative potential of IoT solutions partnerships in various industries.

In 2023, the top 10 platform companies controlled 65% of the market, compared to 58% in 2019 and 44% in 2016. Leading "hyperscalers" (e.g., Microsoft, Amazon Web Services or AWS, Alibaba, Google) continued to experience growth rates of

SECTOR	2021 IOT MARKETS ($BILLION)	2030 PROJECTED VALUE ($BILLION)	COMPOUND ANNUAL GROWTH RATE (CAGR) %
Industrial	326.1	1742.8	20.5%
Manufacturing	205.8	1523.9	24.9%
Automotive	82.7	621.8	25.1%
Consumer	221.7	616.7	12%
Transportation	85.2	498.5	21.7%
Aero-Defense	42.4	156.3	15.6%

[17] Data from https://www.precedenceresearch.com/iot

[18] An IoT platform is a software system facilitating the development, deployment, and management of IoT applications.

[19] Philipp Wegner, "IoT Platform Companies Landscape 2021/2022: Market consolidation has started" from IoT Analytics (November 23, 2021) available at https://iot-analytics.com/iot-platform-companies-landscape/

[20] R. Daws, "Telit acquires Thales' cellular IoT products to establish Telit Cinterion," from *IoT News* (August 1, 2022) available at https://iottechnews.com/news/telit-acquires-thales-cellular-iot-products-establish-telit-cinterion/

[21] "Semtech Corporation to acquire Sierra Wireless," Semtech (August 2, 2022) available at https://www.semtech.com/company/press/semtech-corporation-to-acquire-sierra-wireless

[22] "Google to shut down its IoT Core Services from Aug 2023; users seek options", from *Business Standard* (August 18, 2022) available at https://www.business-standard.com/article/technology/google-to-shut-down-its-iot-core-services-from-aug-2023-users-seek-options-122081800194_1.html

[23] James Blackman, "Ericsson quits IoT - agrees sale of loss-making IoT accelerator business to Aeris," from *RCR Wireless News* (December 7, 2022) available at https://www.rcrwireless.com/20221207/5g/ericsson-quits-iot-agrees-sale-of-loss-making-iot-accelerator-business-to-aeris

[24] L. Clark, "IBM to fire Watson IoT Platform from its cloud," from *The Register* (November 15, 2022) available at https://www.theregister.com/2022/11/15/ibm_set_to_retire_watson/

[25] S. Lee, "SAP IoT Retirement and SAP Asset Performance Management," from SAP (October 5, 2022) available at https://community.sap.com/t5/supply-chain-management-blogs-by-sap/sap-iot-retirement-and-sap-asset-performance-management/ba-p/13533347

[26] A. Tilley, "Cisco Systems pulls back from smart city push," from *Wall Street Journal* (December 28, 2020) available at https://www.wsj.com/articles/cisco-turns-off-lights-on-smart-city-push-11609178895

more than 50% per year,[27] in part buoyed by the fact that their platforms enable business ecosystems and scalable revenue streams, part of which are for IoT applications. Platform-based partnerships have led to successful collaborations for various market applications.

Technology Maturity

IoT-enabling technologies continue 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.[28] Others are "coming up", including edge data and app platforms, serverless/Function-as-a-Service implementations, cloud-connected sensors, edge AI chips, code/no code development platforms, and satellite IoT connectivity.[29] Still others, like data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, Quantum Random Number Generation (QRNG) chips, bio-degradable sensors, 6G and quantum computing are only just hitting the market or are still in research labs.[30]

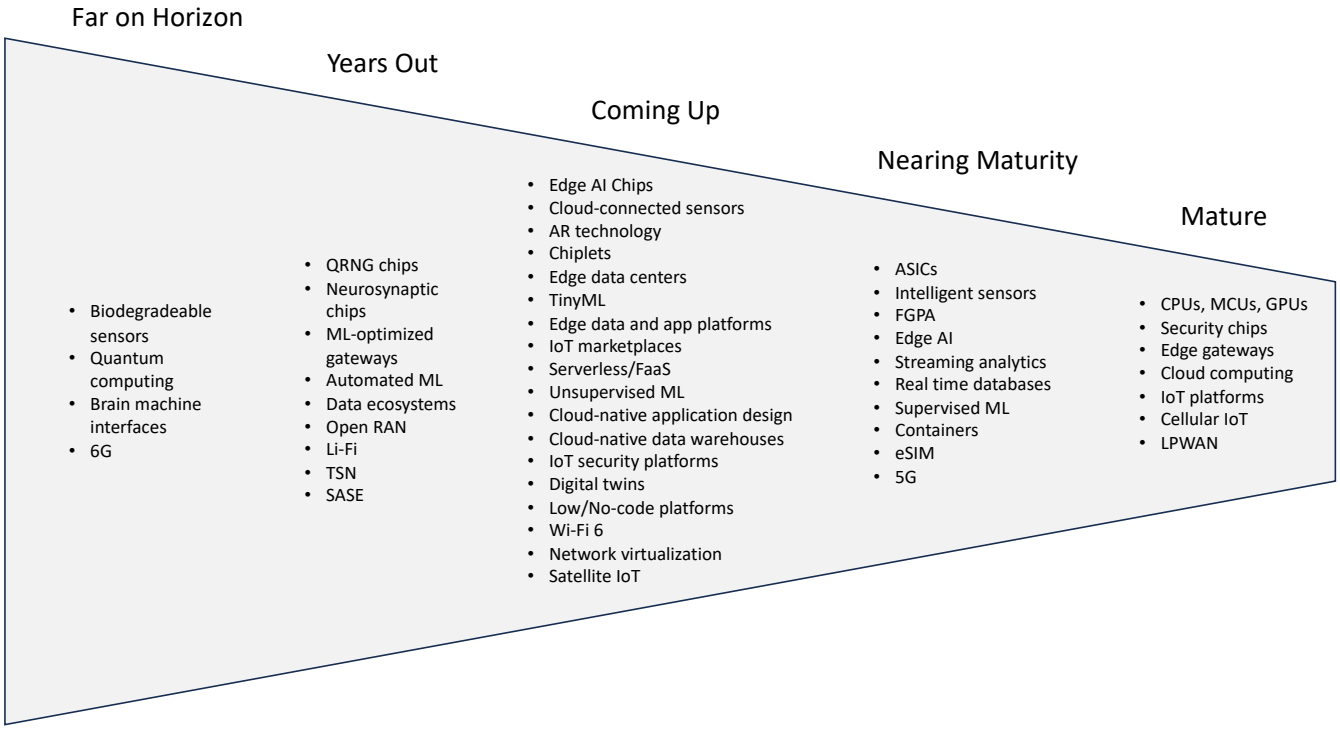


Figure 7. Maturity states of key technologies underlying the Internet of Things[31]

[27] https://iot-analytics.com/iot-platform-companies-landscape/

[28] S. Sinha, "55+ emerging IoT technologies you should have on your radar (2022 update)," from *IoT Analytics* (April 6, 2022) available at https://iot-analytics.com/iot-technologies/

[29] ibid.

[30] ibid.

[31] Figure Credit: Benson Chan, custom figure using data from S. Sinha, "55+ emerging IoT technologies you should have on your radar (2022 update)," from *IoT Analytics* (April 6, 2022) available at https://iot-analytics.com/iot-technologies/. Figure used with permission.

The IoT-enabled Economy

The Evolution of IoT

IoT will continue to evolve, driven by advancements in underlying technology (Figure 8). Today's smart devices and systems employ sensors, microprocessors, and wireless connectivity to monitor and report on the conditions of assets, operations, and the surrounding environment. The vast amounts of data collected today train machine learning and AI models that create insights, predict outcomes, and automate actions.

As IoT technologies integrate deeper into enterprise operations and systems across the economy, business ecosystems arise to create innovative solutions offered "as a service". The massive deployment of intelligent IoT in the future facilitates industry ecosystems supporting an autonomous operation and infrastructure to facilitate the future IoT economy, leading to new innovative solutions, workforce focused on value creation, operational efficiency, and growth and prosperity.

The evolution of IoT is accelerated by several enablers, including:

- **Integrated IoT devices and end-to-end platforms.** IoT devices, enabled by interoperability, link with other IoT devices forming integrated systems. These systems connect with other systems to create "systems of systems" and platforms offering "end-to-end" value across industries and communities.
- **Convergence of IoT and AI.** IoT value is unlocked with AI which analyzes the vast data collections from sensors. These AI algorithms, running in cloud servers or on the devices themselves, create insights, predict outcomes, and automate operations. The integration of the two technologies extends the value of IoT from monitoring and reporting to prediction and automation.
- **Scaling through business ecosystems.** IoT enables new innovative solutions which scale with business ecosystems, built on industry platforms and partnerships. These ecosystems broadly transform industries to smart industries, and communities to smart communities.
- **Strategic policies and regulations.** As IoT evolves, it faces various challenges, many of which are addressed by industry efforts. Well-crafted government policies and regulations, created in partnership with industry can address challenges that industry alone cannot resolve, ensuring continued IoT growth and evolution.

A Vision for the IoT-enabled Economy

The evolution of IoT will positively impact industries, leading to the emergence of an IoT-enabled economy. This section offers a perspective of one possible future.

The Internet facilitated the development of digital platform business models. A platform-based business model "creates value by facilitating exchanges between two or more interdependent groups, usually consumers and producers. To make these exchanges happen, platform-based solutions harness and create large, scalable networks of users and resources that can be accessed on demand. Platforms create communities and markets with network effects[32] that allow users to interact and transact."[33] Examples of Internet digital platform businesses include eBay, Amazon Airbnb, Uber, and Facebook (now Meta).

The continuing evolution of the IoT will facilitate the similar development of IoT-enabled digital platforms, new business models and platform-based industry ecosystems. For example, an industrial equipment manufacturer offers IoT-based "smart



Figure 8. Evolution of IoT[34]

[32] Definition of "network effects" available at https://www.wallstreetprep.com/knowledge/network-effects/

[33] Alex Moazed, "Platform Business Model Definition: What is it?" from Applico available at https://www.applicoinc.com/blog/what-is-a-platform-business-model/

[34] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024. Used with permission of the authors. [3]

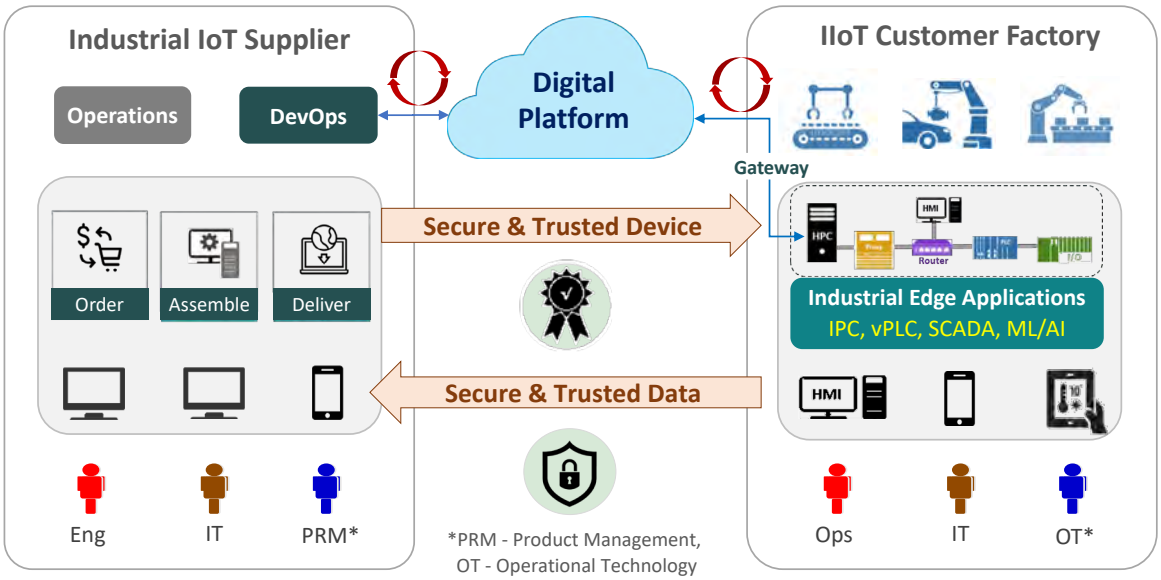


Figure 9. Smart-connected industrial IoT supplier with manufacturing customer[35]

machines" to its factory customers. Smart machines are integrated in the factory and link to cloud platforms that manage remote updates and monitor devices on the factory floor (Figure 9). The manufacturer's dealers connect to the platform to monitor their customers' real-time machine condition data and remotely service the equipment. A community or ecosystem of third-party solutions providers create and offer innovative applications and services built on top of the platform to provide additional benefit to customers.

As suppliers engage in IoT digital transformation efforts[36] to digitalize, realign, and integrate their internal and external operations with the digital platform to connect with their customers' operational processes in real time, they evolve to become smart-connected suppliers enabled by IoT.

This enables IoT-enabled solution providers and customers to achieve several benefits:

- **Improved visibility and transparency** through integrated data sharing, facilitating better inventory management and demand forecasting.
- **Real-time monitoring and analytics** of production processes, to identify inefficiencies and optimization of workflows that lead to enhanced productivity.
- **Trusted data for digital twins**[37] to ensure precise simulations, timely predictive maintenance and process optimization boosting operational efficiency.[38]
- **Growth of new revenue streams** with value-added services and solutions, leading to stronger customer relationships and economic value.

In the IoT-enabled economy, digital platforms enable new business models through sharing of trusted information linked to data (a.k.a. operational data and metadata) among customers, community members, and suppliers. This facilitates transparency and visibility across the industry ecosystem, enabling the development and delivery of more agile and responsive actions, services and offerings to support customer needs. For suppliers and solutions providers, this leads to new revenue streams from a wide variety of platform-based offerings delivered as a service. These types of connected services are known broadly as XaaS offerings (Everything-as-a-Service).[39]

Digital IoT platforms that facilitate network effects accelerate value to the global economy as they expand across the industry ecosystem and scale with more customers and third-party solutions providers and complementary partners.

[35] Figure credit: Tom Katsioulas, used with permission.

[36] Chris Angevine, Jacklyne Keomany, Jannick Thomsen, and Rodney Zemmel, "Implementing a digital transformation at industrial companies" from McKinsey and Company (May 27, 2021) available at https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/implementing-a-digital-transformation-at-industrial-companies

[37] A digital twin is a virtual representation of an IoT device, system or process, designed to accurately simulate the behavior of function of a physical object or infrastructure. Digital twins accelerate adoption with smaller investment.

[38] Kimberly Borden and Anna Herlt, "Digital twins: What could they do for your business?" from McKinsey and Company(October 3, 2022) available at https://www.mckinsey.com/capabilities/operations/our-insights/digital-twins-what-could-they-do-for-your-business

[39] Max Silber, "Everything As A Service: The Newest Addition To The Service Economy" from *Forbes* (October 12, 2022) available at https://www.forbes.com/councils/forbestechcouncil/2022/10/12/everything-as-a-service-the-newest-addition-to-the-service-economy/

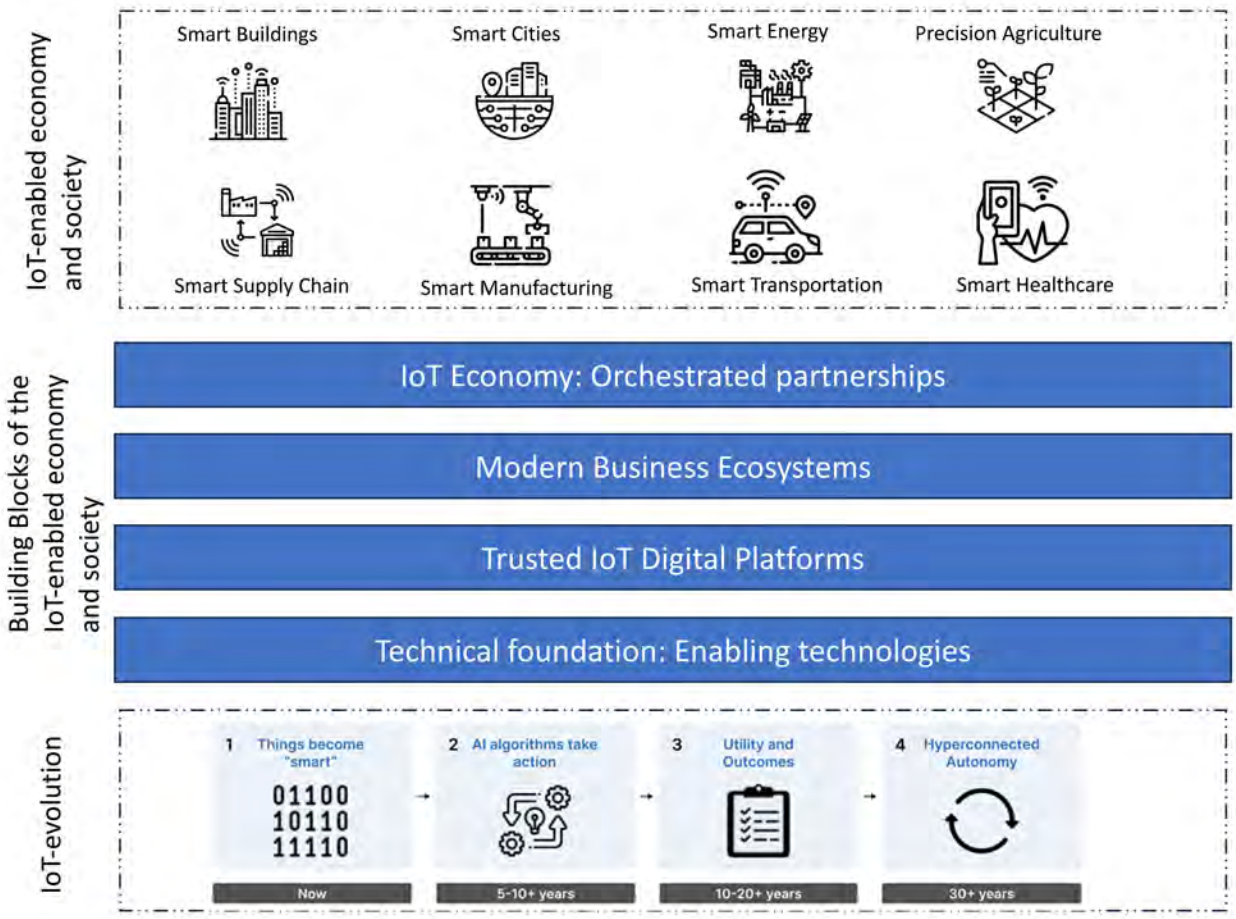


Figure 10. IoT Foundational Building Blocks that Accelerate the IoT-enabled Economy.[40]

Facilitating the IoT-enabled Economy

The IoT-enabled economy uses a key set of building blocks (Figure 10). These include:

- **Technical foundation:** Enabling technologies provide capabilities necessary for IoT to function and create value by generating data used in analytics and AI applications.
- **Trusted IoT Digital Platforms:** These platforms offer reliable services that integrate devices and hardware and software technologies together extending their value and creating comprehensive end-to-end solutions.
- **Modern Business Ecosystems:** These bring together complementary suppliers with solutions built on digital platforms, combining resources, and expertise to create and deliver sustainable value.
- **Orchestrated partnerships fueling the IoT Economy:** These partnerships link companies, technologies, digital platforms, and ecosystems to create higher value and accelerate economic growth.

End-to-end IoT Solutions Platforms

End-to-end IoT solutions platforms will evolve through increasing IoT connectivity, resulting in growth of data, and new AI applications. Such platforms could extend beyond IoT devices to encompass the entire IoT value chain, from data acquisition and analytics to application development and deployment. End-to-end IoT solutions platforms could thereby offer comprehensive toolsets and services that enable organizations to design, deploy, and optimize IoT solutions tailored to their specific needs and objectives. By integrating workflows with IoT, data sharing capabilities coupled with analytics tools, end-to-end solutions platforms can streamline the development process, accelerate time-to-market, and maximize IoT investments.

[40] Figure credit: Benson Chan, used with permission.

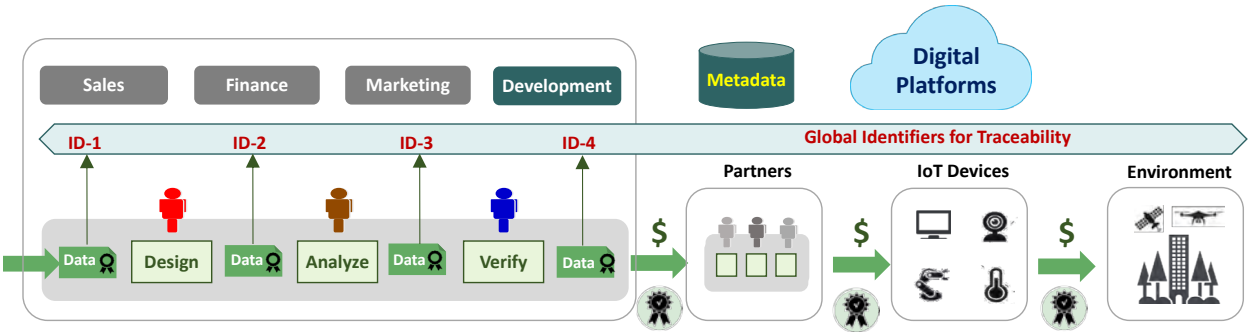


Figure 11. End-to-end Solutions Platform Digitalizing Supply Chain Workflows[41]

Digitalization of enterprise workflows exchanging cryptographically secure data across supply chains[42] create a foundation for trusted digital platform-based business ecosystems. Digital platforms can foster collaboration, partnerships, and innovation within supply chains and broader IoT ecosystems to drive economic growth. Extending these platforms to create industry ecosystems can bring together diverse stakeholders, including technology providers, developers, enterprises, and government agencies, to co-create and share the value.

Open APIs, digital tools, and mechanisms to share resources, ecosystem platforms will facilitate interoperability across diverse IoT domains, enabling new types of digital marketplaces[43] across IoT ecosystems. As the IoT landscape continues to evolve, these platforms could then enable multi-stakeholder collaboration and innovation, unlocking new opportunities for differentiation, automation, and economic growth.

[41] Figure credit: Tom Katsioulas, used with permission.

[42] Holly Briedis, Michele Choi, Jess Huang, and Sajal Kohli. "Moving past friend or foe: How to win with digital marketplaces" from McKinsey and Company (June 18, 2020) available at https://www.mckinsey.com/industries/retail/our-insights/moving-past-friend-or-foe-how-to-win-with-digital-marketplaces

[43] Global Semiconductor Alliance Trusted IoT Ecosystem Security, "Reply to NIST RFI on Evaluating and Improving Cybersecurity and the Cybersecurity Framework" available at https://www.nist.gov/system/files/documents/2022/04/25/04-25-2022-GSA_TIES.pdf

Platform-based IoT Business Ecosystems

Platform-based IoT business ecosystems[44] (discussed earlier in this report) are comprised of complementary partners, resources, standards, and tools. These have long been advocated by business scholars for their proven ability to fuel economic value by leveraging scalable digital platforms as the foundation for dynamic and interconnected business networks. By fostering symbiotic relationships and co-opetition among participants, platform-based IoT business ecosystems drive innovation, monetization, agility, and scalability through open architecture, governance, and network effects,[45] as proven by trillion-dollar platform giants.

Orchestrated business partnerships

Partnerships are critical to the development of the IoT-enabled economy. End-to-end IoT solutions across industry ecosystems are inherently complex, and involve multiple companies, technologies, and standards. By forging IoT business partnerships with complementary stakeholders, organizations can leverage each other's strengths to develop integrated solutions and accelerate the creation of data ecosystems.[46]

Orchestrated partnerships require re-thinking the roles of ecosystem participants,[47] that collectively can bridge the gaps between legacy infrastructure and IoT markets to accelerate IoT adoption. An appropriate mix of partners is needed for orchestration. Broadline suppliers bring platform orchestration capabilities. Startups push the boundaries of IoT with innovation. Domain experts provide real-world relevance optimizing for practical use in the specific context of environment or application. Such partnerships are key to economic growth because:

- With appropriate governance, they can minimize market failures such as fragmented supply chains or organizational failures such as enterprise silos that could undermine the value structure.[48]
- They accelerate network effects that are key to growing business ecosystems. A platform-based digital marketplace connects buyers and sellers. The value of the platform grows with more stakeholders and applications.
- They facilitate innovation and validation of IoT pilot proof of concept projects by bringing the right mix of partners and collective ecosystem IQ collaborating to show the economic value before investing to deploy at scale.

Proper governance of such partnerships is critical to maximizing the broad potential economic benefits.

One model of orchestrated partnerships is IoT Public-Private Partnerships (PPPs) which could include government, industry stakeholders and tech hubs[49] and encourage investment in end-to-end solutions where multiple stakeholders provide and share information. PPPs accelerate the creation of data ecosystems[50] that can share information about data, availability, and analysis to develop new business models, and an architecture[51] for services that improve customer experience, lift adoption barriers and drive economies of scale.

Below are three examples of orchestrated PPPs which can accelerate the development of their respective business use case examples that can be accelerated with orchestrated PPPs consisting of a mix of large companies, innovative startups, and domain experts collaborating on digital twins before pursuing scalable deployments. Digital twin simulations of the IoT-based physical world (such as smart transportation or manufacturing) provide great insights on the economic value that can be achieved.

---

[44] Marshall Van Alstyne and Steven Paul, "Platform Strategy and the Internet of Things" from *MIT Sloan Management Review* (November 10, 2016) available at https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/

[45] "Network Effects: a Step by Step Guide to Understanding Network Effects" from Wall Street Prep (July 17, 2024) available at https://www.wallstreetprep.com/knowledge/network-effects/

[46] Ahmed Abdulla, Ewa Janiszewska-Kiewra, and Jannik Podlesny, "Data Ecosystems Made Simple" from McKinsey Digital (March 8, 2021) available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/data-ecosystems-made-simple

[47] Maximilian Schroeck, Anne Kwan, Jagjeet Gill, and Deepak Sharma, "Evolving partner roles in Industry 4.0" from *Deloitte Insights* (September 3, 2020) available at https://www2.deloitte.com/us/en/insights/focus/industry-4-0/partner-ecosystem-industry-4-0.html

[48] Michael G. Jacobides, Carmelo Cennamo, and Annabelle Gawer, "Externalities and complementarities in platforms and ecosystems: from structural solutions to endogenous failures" from *Research Policy* (Vol. 53, Issue 1, January 2024) available at https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3Dihub

[49] "Regional Technology and Innovation Hubs (Tech Hubs)" from U.S. Economic Development Administration available at https://www.eda.gov/funding/programs/regional-technology-and-innovation-hubs

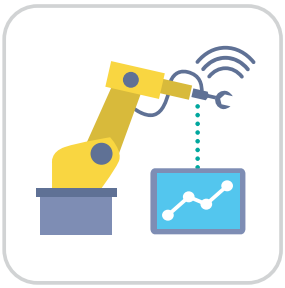
[50] Massimo Russo and Michael Albert, "How IoT Data Ecosystems Will Transform B2B Competition" from BCG (July 27, 2018) available at https://www.bcg.com/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition

[51] Ahmed Abdulla, Ewa Janiszewska-Kiewra, and Jannik Podlesny, "Data Ecosystems made Simple" from McKinsey Digital (March 8, 2021) available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/data-ecosystems-made-simple



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

For collaboration, logistics companies such as UPS, DHL and AWS 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 that helps organizations proactively identify and mitigate risks. A supply chain digital twin can provide insights of the economic value includes cost reduction, improved supply chain resilience, and enhanced efficiency, benefiting all participants through reduced operational costs.



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

For collaboration, broadline suppliers lead the with foundation IoT platforms, cloud vendors offer data storage and processing, Product Lifecycle Management (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. City governments facilitate data access and policy implementation. A digital twin enables stakeholders to simulate and optimize traffic flow and pollution reduction strategies, leading to enhanced city services, reduced congestion, improved air quality, and future economic growth. The economic value proposition for all stakeholders includes enhanced city services, reduced traffic congestion, improved air quality, and better city lifestyle.



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

For collaboration, broadline suppliers lead the with foundation IoT platforms, cloud vendors offer data storage and processing, Product Lifecycle Management (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. City governments facilitate data access and policy implementation. A digital twin enables stakeholders to simulate and optimize traffic flow and pollution reduction strategies, leading to enhanced city services, reduced congestion, improved air quality, and future economic growth. The economic value proposition for all stakeholders includes enhanced city services, reduced traffic congestion, improved air quality, and better city lifestyle.

Evolution of IoT Economy and Potential to Gross Domestic Product (GDP)

In an age of unprecedented technological advancement, IoT emerges as a transformative force that contributes to the potential to reshape our GDP. The IoT economy can learn from the experience of a prior generation of digital platform providers who created new economic value through the creation of new markets.

As of January 2024, the combined market value of seven of the largest tech companies - Apple, Microsoft, Alphabet, Amazon, NVIDIA, Meta, and Tesla - reached $13.1[52] trillion which is equivalent to half of the U.S. GDP. While the first movers disrupted markets and achieved immense growth, future economic growth will come from platforms to empower startups and SMBs to build on them creating complementary businesses and new markets. By learning from this experience startups and SMBs can play a leading role in shaping a hyperconnected planet that links industries, environments, and digital marketplaces.

[52] Stephanie Hill, "A Closer Look at Magnificent Seven Stocks" from Mellon (February 2024) available at https://www.mellon.com/insights/insights-articles/a-closer-look-at-magnificent-seven-stocks.html

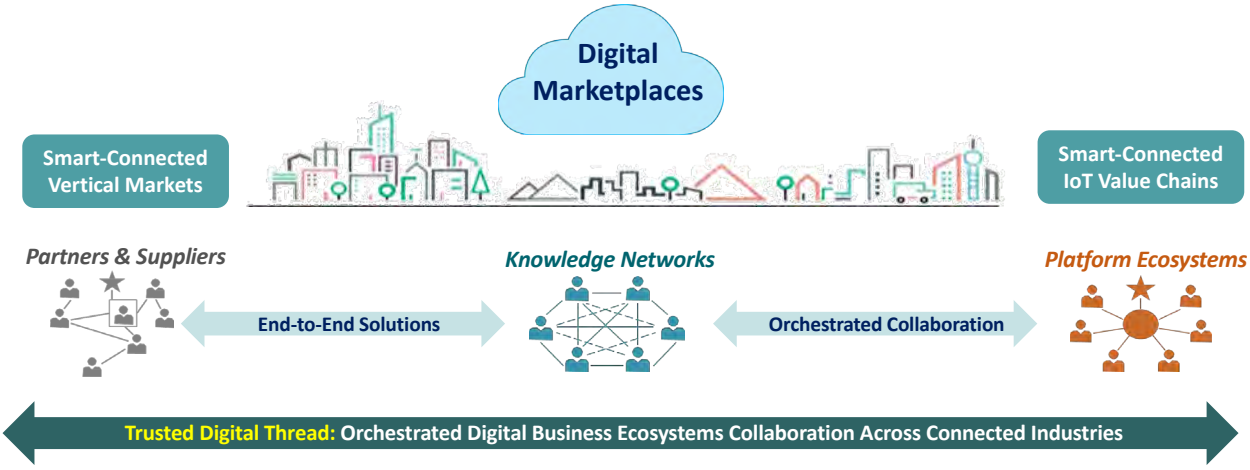


Figure 12. Evolution of IoT Economy Driven by Digital Threads and Partner Ecosystems[53]

Observation #1: Orchestrated platform-based business ecosystems bridge industries. While existing large-scale platforms have excelled in various domains, there remains a noticeable void in multi-stakeholder collaboration platforms across industry ecosystems. One of the main strategies for achieving hyperconnected growth is to encourage platform-based business ecosystems that link 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, orchestrated business ecosystems can multiply the growth of the many small and midsize businesses (SMBs) and enable the next generation platform companies.

Observation #2: IoT partnerships transform to knowledge networks and 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, IoT partnerships will evolve into connected knowledge networks, emphasizing the importance of sharing expertise and insights among stakeholders. Knowledge networks mature into collaborative platform-based business ecosystems leveraging the collective ecosystem IQ across value chains to drive new XaaS revenue streams and amplified growth driven by network effects.

Observation #3: Platforms empower SMBs to collaborate and scale rapidly. Platform-based business ecosystems that span across IoT ecosystems amplify network effects, setting the stage for a dynamic and collaborative business landscape. To unlock this potential, orchestrated platform-based business ecosystems can be incentivized to amplify and multiply the value-add of startups and SMBs to create future generations of trillion-dollar giants.

Observation #4: IoT data strengthens national security and drives economic growth. By motivating the orchestration of multi-stakeholder digital business ecosystems and hyperconnected marketplaces, the treasure trove of data generated by digital twins and AI applications can be unlocked. This data can fuel a plethora of digital services, enhancing national security and propelling the U.S, economy into the future of a hyperconnected digital planet. Large and small businesses will be able to access marketplaces where they will not only offer their products and services but also tap into a wealth of data and insights.

Observation #5: IoT circular value chain ecosystems foster 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 words, fueled by digital twins within circular business ecosystems, will foster efficiency, innovation, and environmentally responsible practices that will propel the U.S. economy to the next level.

The convergence of IoT and large-scale platforms leading to the development of orchestrated business ecosystems represents an unparalleled opportunity to grow U.S. GDP. Through collaboration, amplification of many SMBs' value, and the adept leveraging of IoT to create hyperconnected industries, the U.S can usher in an era of prosperity and innovation. It is incumbent upon us to leverage the core strengths of the existing platforms to harness the full potential of IoT and lead the charge toward a future of digital business ecosystems that unite digital marketplaces, industries, and environments and an IoT hyperconnected planet that will ensure a brighter future for generations to come.

[53] Figure credit: Tom Katsioulas, used with permission.



Photo credit: Shutterstock

Findings of the IoT Advisory Board

This section lists the major findings that informed the IoTAB's recommendations. These findings are organized into two categories: general findings (affecting everyone) and industry-specific findings. The following table provides a summary of these findings.

FINDINGS	
General Findings	
Finding 1:	Industry adoption has not met expectations due to a variety of challenges.
Finding 2:	A lack of coordination at the national level is hindering IoT adoption and operation across the economy and industry sectors.
Finding 3:	The adoption and operation of innovative IoT applications are hindered by various existing policies and regulations at local, state, and federal levels.
Finding 4:	Insufficient skilled workers are available to develop, integrate, deploy, operate, and maintain IoT devices, systems, and applications.
Finding 5:	IoT systems depend on chips sourced through vulnerable global supply chains.
Finding 6:	Establishing trust in IoT requires a multi-dimensional ecosystem perspective, extending beyond cybersecurity and privacy.
Finding 7:	Privacy concerns undermine trust in IoT and are a significant barrier to widescale adoption.
Finding 8:	IoT cybersecurity concerns are a major barrier to widescale adoption.
Finding 9:	IoT modules built by Chinese companies dominating our market poses a serious security and economic risk.
Finding 10:	Quantum computing poses a major threat to IoT cybersecurity.
Finding 11:	Interoperability is a key challenge for IoT across multiple industries.
Finding 12:	A variety of connectivity challenges are hindering IoT adoption, operation, and scaling.
Finding 13:	Artificial Intelligence (AI) is critical to unlocking and accelerating the value of IoT, but significant challenges must be addressed.
Finding 14:	The IoT-enabled economy is unlocked and accelerated with platform-based business ecosystems, which require multi-stakeholder collaborative partnerships to be successful.
Finding 15:	The convergence of AI with IoT (AIoT) is poised to drive transformation across wide sectors of the economy, but its development and use must be managed to foster the proper outcomes and minimize unintended consequences.
Finding 16:	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.
Finding 17:	Small businesses can reap significant benefits from the use of IoT, but significant barriers hinder their adoption.
Finding 18:	Small companies and startups are instrumental in developing many innovative and disruptive technology solutions and services but face a variety of barriers in getting market adoption.
Industry Specific Findings	
Finding 19:	IoT brings significant value to agriculture, but adoption is slow.
Finding 20:	The development of smart communities in the U.S. is limited, uneven and slow to develop.
Finding 21:	IoT can transform outcomes in traffic management and transit but several technical, policy and funding barriers hinder adoption.
Finding 22:	IoT is transforming healthcare and is poised to revolutionize it, but significant challenges need to be addressed.
Finding 23:	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.

Finding 24:	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.
Finding 25:	IoT can be a key technology enabler for end-to-end supply chain visibility currently hindered by the disconnected nature of supply chains.
Finding 26:	The use of IoT can transform industrial operations, but adoption is limited, and challenges need to be addressed.

General Findings

Finding 1: Industry adoption has not met expectations due to a variety of challenges.

As stated earlier, in 2021 McKinsey and company revised the forecast downward to between $5.5 trillion and $12.6 trillion by 2030.[54] It attributed the downward revision to adoption headwinds related to change management, cost, talent, and cybersecurity, as well as slow market adoption of digitalization and cyber resilience, especially in enterprises.

The adoption of IoT technologies is growing in the United States, but that growth has been incremental and slower than expected. Despite its potential, several challenges[55] and barriers have contributed to the slow pace of adoption across businesses and society. Some of these challenges, identified by IoTAB members, include:

- **Complexity and Integration.** IoT consists of sets 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" solution, and components must be assembled 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 are in short supply, especially for industries with established processes.
- **Cybersecurity Concerns.** IoT introduces a vast number of potential attack surfaces, leading to genuine concerns that hinder adoption. 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. 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.
- **Interoperability.** A significant barrier is the inability of devices to communicate with each other or with the broader enterprise, legacy systems, and operations technology systems. 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 ecosystems". One major challenge is the integration of IoT devices with legacy and operations technology systems, which are commonly found in many industrial, healthcare and enterprise environments.
- **Data Privacy and Confidentiality.** Concerns about data privacy, confidentiality and compliance are significant barriers to IoT adoption. Industries must navigate complex legal frameworks and ensure that IoT implementations comply with data protection and usage regulations, which can slow down the adoption process. While user privacy and enterprise confidentiality concerns exist across multiple markets and industries, some sectoral markets with higher-level privacy regulations are more sensitive to privacy issues (e.g., smart communities, retail, insurance, and healthcare) and other markets are more sensitive to confidentiality issues (e.g., industrial IoT and manufacturing).
- **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 account for the other 70%.[56]
- **Lack of Skilled Workforce.** Implementing and managing IoT technologies requires a skilled workforce with expertise in various areas, such as cybersecurity, data analytics, application development, cloud operations, and system integration. The shortage of professionals with these skills hinders adoption, particularly in industries that have not traditionally required digital talent. In addition, the ongoing labor shortage contributes to the struggle to attract and retain such talent.

[54] Michael Chui, Mark Collins, and Mark Patel, "IoT value set to accelerate through 2030: Where and How to capture it" from McKinsey Digital (November 9, 2021) available at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

[55] Dimitris Paraskevopoulos, "Challenges with IoT product launches: Why time time-to-market has increased 80% in 4 years", from IoT Analytics (April 25, 2024) available at https://iot-analytics.com/challenges-iot-product-launches-why-time-to-market-has-increased-80-percent-in-4-years/

[56] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

- **Uncertain About IoT Return on Investment (ROI) and Business Value.** Some industries are more hesitant to adopt IoT technologies due to uncertainty about the ROI and the overall business value. This reluctance is particularly true for mining, construction, and agriculture industries that have not traditionally incorporated digital technologies into their operations. Small businesses are disproportionately affected because they are often cash-flow constrained and have limited capital for investing in new solutions. 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 affecting adoption of IoT. Certain markets and potential adopters have limited awareness and education about 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 organizational culture are additional barriers hindering the adoption of IoT. Adoption rates vary based on market sophistication and ability to "Cross the Chasm"[57] based on organization evolution (Innovators, Early Adopters, Early Majority, Late Majority, Laggards).
- **Reliability and Stability Concerns.** IoT is still considered a new or emerging technology for many industries, particularly those in sectors such as healthcare, manufacturing, energy, and smart communities. In these sectors, reliability, stability, and longevity are essential 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 2: A lack of coordination at the national level is hindering IoT adoption and operation across the economy and industry sectors.

From consumer to healthcare, industrial to critical infrastructure, the Internet of Things is poised to transform our economy, communities, and civil society. However, the Internet of Things also brings potential known and unforeseen risks as it is deployed broadly. A strategic approach that balances innovation with risk mitigation can maximize the benefits of IoT adoption while minimizing potential risks.

No such strategic approach exists at a national level today. The need for such an approach has been called out in several previous efforts, including:

- In 2014 the President's National Security Telecommunications Advisory Committee recommended that the federal government invest in a national, long-term, multi-agency, multifaceted research initiative in these areas.[58] 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 Office of Science and Technology Policy (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.[59] They found that "Isolated efforts by mission agencies are simply not sufficient to address the underlying issues in a holistic manner." Trying to address such issues agency-by-agency or sector-by-sector would result in inefficiencies and insufficient progress relative to system development timetables. We might never get to where we need to be, and the recommendation is to create a long-range action plan.

  OSTP 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."[60]
- A report in 2015 by the Networking and Information Technology Research and Development (NITRD) program that looked at opportunities in agriculture, smart buildings, defense, emergency response, energy healthcare, manufacturing, and transportation advocated for a multi-agency, multi-sector comprehensive focus on the problematic crosscutting R&D challenges in Cyber-Physical System (CPS).[61]

[57] A definition of this term can be found at https://diffusion-research.org/research_articles/chasm-theory-development/

[58] The President's National Security Telecommunications Advisory Committee, "NSTAC Report to the President on the Internet of Things" (November 19, 2014) available at https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf

[59] Cyber Physical Systems Senior Steering Group, "Winning the Future with Science and Technology for 21st Century Smart Systems" from the Office of Science and Policy (April 2011) available from https://www.nitrd.gov/pubs/CPS-OSTP-Response-Winning-The-Future.pdf

[60] Ibid.

[61] Cyber Physical Systems Senior Steering Group, "Cyber Physical Systems" from the Office of Science and Technology Policy (June 3, 2015) available at https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

These predictions from 2011 and 2015 were accurate, and the lack of a national strategy has impacted growth and adoption. Today, IoT opportunities are even more pervasive, the economic stakes are even more enormous, and the impacts are even more profound.

Within the federal government, the lack of a strategic and coordinated approach hinders internal adoption and produces unnecessary risk. For example, the recent Office of Management and Budget Memorandum (OMB) 24-04 underscored that "[federal] agencies must have a clear understanding of the devices connected within their information systems to gauge cybersecurity risk to their missions and operations."[62] Moreover, the memorandum goes on to say, "maturing Federal cybersecurity practices for internet of things (IoT) devices is critical in today's increasingly automated world." However, how this is interpreted and implemented may differ from agency to agency. This leads to inconsistent implementation and practices, which could potentially increase the risks.

To balance the promise of transformational capabilities with the risks of AI, the federal government has implemented a variety of strategic and coordinated initiatives. No such initiative has been undertaken by the Federal Government to institute an overarching entity within the Executive Office of the President responsible for IoT and IIoT adoption.

Finding 3: 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.

IoT has the potential for significant advancements, but policies and regulations at various government levels can sometimes hinder its benefits. Conflicting or overlapping regulations between state, local, and federal levels can complicate IoT adoption. While these policies are often designed to protect users and communities, they may unintentionally create barriers due to the rapid pace of technological change. Government regulations play a crucial role in either advancing or restricting the use, growth, and benefits of IoT.

Examples of policies affecting the use of IoT include:

- Facial recognition algorithms running on a city's network of video cameras help deter and solve crimes but may lead to privacy violations when used outside of their intended purpose. Many cities have enacted laws restricting the use of video cameras and facial in smart community applications.
- Autonomous drones can perform 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 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 may be used. For example, California only allows insurance companies to use mileage data.[63]

Finding 4: Insufficient skilled workers are available to develop, integrate, deploy, operate, and maintain IoT devices, systems, and applications.

A significant challenge in scaling IoT into the national infrastructure and economy is the development of an 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 individuals with interdisciplinary expertise who can navigate the complexities of both hardware and software components. Integrating these diverse skill sets into a cohesive workforce presents 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 very different from IT. IoT is a disparate set of technologies requiring an interdisciplinary combination of existing and new technical, digital, and analytical skills. The workforce

[62] Office of Management and Budget Memorandum 24-04 can be found at https://www.whitehouse.gov/wp-content/uploads/2023/12/M-24-04-FY24-FISMA-Guidance.pdf

[63] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

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, developing a workforce of skilled data professionals is essential for managing and analyzing the large amounts of data collected to achieve the best outcomes.

- **Non-digital industries and systems go digital.** Many conventional industries have 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[64] of IT, OT and IoT systems.** Industries like manufacturing, energy and transportation employ operational 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 requires OT and IT functions and systems to come together. This convergence requires a workforce with a specific set of digital skills, including knowledge of IT and OT protocols and processes, cybersecurity, systems integration, cloud computing, programming, application development, IoT integration, and 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.
- **Harnessing the full potential of IoT and AI.** Just as personal computers transformed bookkeepers into accountants by automating calculations, IoT and AI will transform industries, necessitating new skills. Along with the skills described above, IoT-enabled AI tools designed to assist humans can significantly aid this transition. IoT provides data that enables AI to assist workers with automating routine tasks, analyzing complex data, and making informed decisions at a higher-level. By embracing and integrating these tools, the workforce can not only adapt to but thrive in the rapidly evolving landscape of IoT and AI, driving innovation and efficiency.

Finding 5: IoT systems depend on chips sourced through vulnerable global supply chains.

While global supply chains are necessary to supplying chips for IoT systems, solving chip supply chain vulnerabilities requires coordination among nations leveraging IoT to enable cross-border traceability.

The semiconductor supply chain is global. The companies that design, produce, and distribute semiconductors, and integrate them into products, including IoT devices and smart systems, operate in many countries around the world. However, there are geopolitical tensions and vulnerabilities in the global supply chain. These include:

- **Increased cybersecurity risks.** Supply chain security and trust pose major concerns due to fragmentation and vast attack surface from chip design to IoT edge applications. Often attacks experienced during field use of IoT devices such as many distributed denial-of-service (DDoS) or critical infrastructure attacks[65] can be traced back to supply chain vulnerabilities[66] due to bugs or intrusions of rogue actors in chips and electronics. The risks to national and economic security are growing.

[64] Stephen J. Bigelow, "What is IT/OT convergence? Everything you need to know?" from TechTarget available at https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence#:

[65] Vinugayathri, "Why DdoS Attacks Use IoT Devices as Weapons?" from Cybersecurity News (January 18, 2023) available at https://cybersecuritynews.com/ddos-attacks-use-iot-devices/

[66] Etay Maor, "Supply Chain Attacks and Critical Infrastructure: Achieving Resilience" from *Forbes* (April 8, 2022) available at https://www.forbes.com/councils/forbestechcouncil/2022/04/08/supply-chain-attacks-and-critical-infrastructure-achieving-resilience/

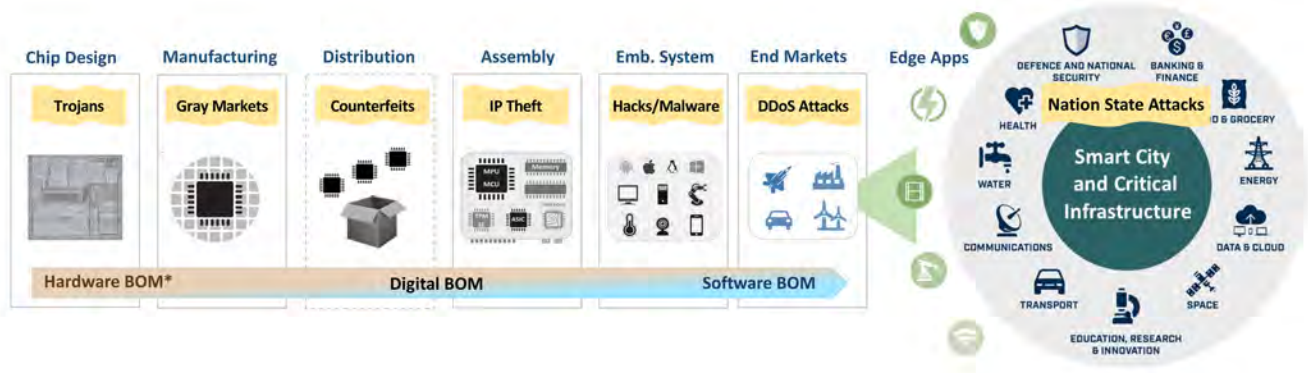


Figure 13: Supply Chain Vulnerabilities Are Experienced in Critical Infrastructure and IoT Applications[67]

- **Threatened national and economic security.** Trade restrictions on chips have proven to be largely ineffective. Despite bans, western chips[68] end up in Russian[69] and Chinese drones[70] altering modern warfare dynamics and affecting sea routes causing higher oil prices and cost of goods. Our advanced AI chips are still being sold in China despite bans.[71] Imports of Chinese legacy chips are on track to flood U.S. and EU markets which prompted the Select Committee on the CCP to urge Commerce Secretary Raimondo and U.S. Trade Representative Tai to act.[72]
- **Risk of investments in CHIPS Acts.** In December 2022, the U.S.-E.U. Technology Trade Council (TTC) officials agreed to strengthen chip supply chains[73] by coordinating semiconductor subsidies. Since then, allied nations committed $450 billion in government funds to build fabs worldwide surpassing China's $150 billion investment.[74] However, China will produce much higher volume of chips at lower prices compared to allied nations and continue to flood allied nations' markets with commodity chips. Without government incentives for market preference enabled by traceability, this puts at risk allied nations CHIPS investments, that may exceed $1.5 trillion with PPPs.[75]

Furthermore, efforts to increase visibility and traceability of the global supply chain, including Allied Nation Initiatives on Cross-border Traceability, are limited.

Chip supply chain vulnerabilities highlight the need for more visibility. Given the foundational role that semiconductors play in electronics and IoT devices, systems, and critical infrastructure, the ability to trace and verify the origin and path the chips undertook from manufacturing to field use is critical.[76] Furthermore, the global nature of the chip supply chain requires multi-nation collaboration on traceability. Geopolitical tensions create an urgency for the U.S. to act and lead allies:

- **Current cross-border chip traceability solutions are urgently needed.** A study by Kyiv School of Economics (KYSE) Institute[77] shed light on flows of chips to Russia and the urgency for traceability. Solutions proposed included PPPs on for chip supply traceability; export policy harmonization; sanctions on third-country intermediaries; enhanced cross-

[67] Figure credit: Tom Katsioulas, used with permission.

[68] Jane Lee, "Focus: The chip challenge: Keeping Western semiconductors out of Russian weapons" from Reuters (April 1, 2022) available at https://www.reuters.com/technology/chip-challenge-keeping-western-semiconductors-out-russian-weapons-2022-04-01/

[69] Sheridan Prasso, "Chips from Texas Instruments and other U.S. Makers Flow Into Russia Despite Ban" from Bloomberg (December 21, 2023) available at https://www.bloomberg.com/news/articles/2023-12-21/chips-from-texas-instruments-txn-analog-devices-adi-flow-into-russia

[70] Lara Seligman and Matt Berg, "A $2M missile vs. a $2,000 drone: Pentagon worried over cost of Houthi attacks" from Politico (December 20, 2023) available at https://www.politico.com/news/2023/12/19/missile-drone-pentagon-houthi-attacks-iran-00132480

[71] Eduardo Baptista, "China's military and government acquire Nvidia chips despite US ban" from Reuters (January 15, 2024) available at https://www.reuters.com/technology/chinas-military-government-acquire-nvidia-chips-despite-us-ban-2024-01-14/

[72] The Select Committee on the Chinese Communist Party, "Letter to Secretary Raimondo on Foundational Semiconductors" dated January 8, 2024 from the U.S. House of Representatives available at https://selectcommitteeonthecp.house.gov/media/letters/letter-secretary-raimondo-foundational-semiconductors

[73] Yuka Hayashi, "U.S., EU Agree to Coordinate Semiconductor Subsidy Programs" from *Wall Street Journal* (December 5, 2022) available at https://www.wsj.com/articles/u-s-eu-agree-to-coordinate-semiconductor-subsidy-programs-11670284917

[74] Estimated from reviewing various data sources. One consolidations can be found in Sujai Shivakumar, Charles Wessner, and Thomas Howell, "A World of Chips Acts: The Future of US-EU Semiconductor Collaboration" from Center for Strategic and International Studies (August 20, 2024) available at https://www.csis.org/analysis/world-chips-acts-future-us-eu-semiconductor-collaboration

[75] "The CHIPS Act has Already Sparked $450 Billion in Private Investments for U.S. Semiconductor Production" from Semiconductor Industry Association (December 14, 2022 updated August 28, 2024) available at https://www.semiconductors.org/the-chips-act-has-already-sparked-200-billion-in-private-investments-for-u-s-semiconductor-production

[76] The 2023 National Defense Authorization Act established the Government Traceability and Diversification Initiative demonstrating the criticality of addressing this issue.

[77] Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Natalia Shapoval, Anna Vlasyuk, and Vladyslav, "Challenges of Export Controls Enforcement" from Kyiv School of Economics Institute (January 2024) available at https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf

Journey of chips through untrusted environments assembled with other chips into electronics and IoT products



border cooperation among the U.S.-E.U. and allies; and use of IoT technology for tracing chips and updating them remotely, ensuring export control enforcement before chips are used by adversaries.

- **Traceability should be part of the ongoing U.S.-E.U. Transatlantic Cooperation Agenda:** In early 2024, the TTC convened to discuss transatlantic cooperation[78] on trade and technology, covering export controls, AI governance, secure 5G connectivity, and semiconductor strategies related to U.S.-E.U. CHIPS Acts. Later discussions at Center for Strategic and International Studies (CSIS) covered digitizing supply chains[79] and chip traceability[80] to establish market preference for chips produced by the U.S. and allied nations. However, legacy chips imports used in our critical infrastructure and leakage[81] of our advanced chips being weaponized in by adversaries[82] are still ongoing.

A holistic strategy for addressing chip traceability is necessary.

A holistic strategy for coordinating CHIPS Acts investments with the U.S.-E.U. TTC, the Executive Branch may include: (a) utilizing NIST's global reach with Standards Development Organizations (SDOs) to create taxonomy of standards, (b) orchestrating PPPs in the chip ecosystem from design and manufacturing, (c) Investing in pilot projects to prove the value of trusted traceability[83] and (d) promoting cross-border Digital Trust with programs like the U.S. Cyber Trust Mark,[84] the EU Digital Product Passport[85] and U.S. Customs and Border Protection (CBP) Global Business Identifiers[86] with a goal to achieve a global 'digital paper trail' for chips.

IoT can augment traceability initiatives to play a key role in addressing semiconductor supply chain vulnerabilities:

- **Leveraging IoT to mitigate supply chain risks and enable growth.** Enforcing export controls on chips is challenging as they can be programmed remotely. For example, Intel's pay-as-you-go chip licensing[87] based on a Root of Trust could signify the start of the *"Internet of Chips"* era. Customs controls linked to trusted digital infrastructure can incentivize chip suppliers to securely trace, monitor and update chips. IoT-enabled manufacturing systems can implement the data collection and reporting for a trusted traceability infrastructure to strengthen customs controls. The trusted infrastructure can unlock opportunities for trusted IoT services, digital marketplaces, and ecosystems to strengthen economic security.
- **Leveraging CHIPS Acts investments for global collaboration on traceability.** With 80% of global fab capacity controlled by allies, the U.S. and EU are well-positioned to pursue proven ecosystem strategies and pilot programs for traceability like the 2023 National Defense Authorization Act (NDAA) that establishes the Governmentwide Traceability and Diversification Initiative [Section 5949 (f)][88] This includes several elements[89] that require establishing provenance

[78] Emily Benson, "The Fifth Ministerial of the U.S. – EU Trade and Technology Council" from Center for Strategic and International Studies (February 7, 2024) available at https://www.csis.org/analysis/fifth-ministerial-us-eu-trade-and-technology-council

[79] "Gina Raimondo and Margrethe Vestager on future of US-EU economic ties" video from Atlantic Council (January 31, 2024) available at https://www.youtube.com/watch?v=waAkVzPzNyM

[80] "The Transatlantic Economic Security Agenda" video from Center for Strategic and International Studies (January 31, 2024) available at https://www.csis.org/events/transatlantic-economic-security-agenda

[81] "Why America's controls on sales of AI tech to China are so leaky" from *The Economist* (January 21, 2024) available at https://www.economist.com/business/2024/01/21/why-americas-controls-on-sales-of-ai-tech-to-china-are-so-leaky

[82] "China Providing 90% of Chips Used In Russia Despite Sanctions" from *Asia Financial* (April 16, 2024) available at – https://www.asiafinancial.com/china-providing-90-of-chips-used-in-russia-despite-sanctions

[83] Global Semiconductor Alliance Trusted IoT Ecosystem Security, "Reply to NIST RFI on Evaluating and Improving Cybersecurity and the Cybersecurity Framework" available at https://www.nist.gov/system/files/documents/2022/04/25/04-25-2022-GSA_TIES.pdf

[84] "Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers" from The White House (July 18, 2023) available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/

[85] "The EU Digital Product Passport shapes the future of value chains" from World Business Council for Sustainable Development (January 24, 2023) available at https://www.wbcsd.org/resources/the-eu-digital-product-passport/

[86] "CBP Launches Global Business Identifier Pilot to Increase Supply Chain Visibility" from U.S. Customs and Boarder Protection (December 2, 2022) available at https://www.cbp.gov/newsroom/national-media-release/cbp-launches-global-business-identifier-pilot-increase-supply-chain

[87] https://www.intel.com/content/www/us/en/products/docs/ondemand/overview.html

[88] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Public Law No. 117-263, Section 5949 (f)

[89] Key sections include (i) chain of custody and traceability, including origin and location of design, manufacturing, distribution, shipping, and quantities; (ii) confidentiality, including protection, verification, and validation of intellectual property included in microelectronics; (iii) integrity, and (iv) availability.

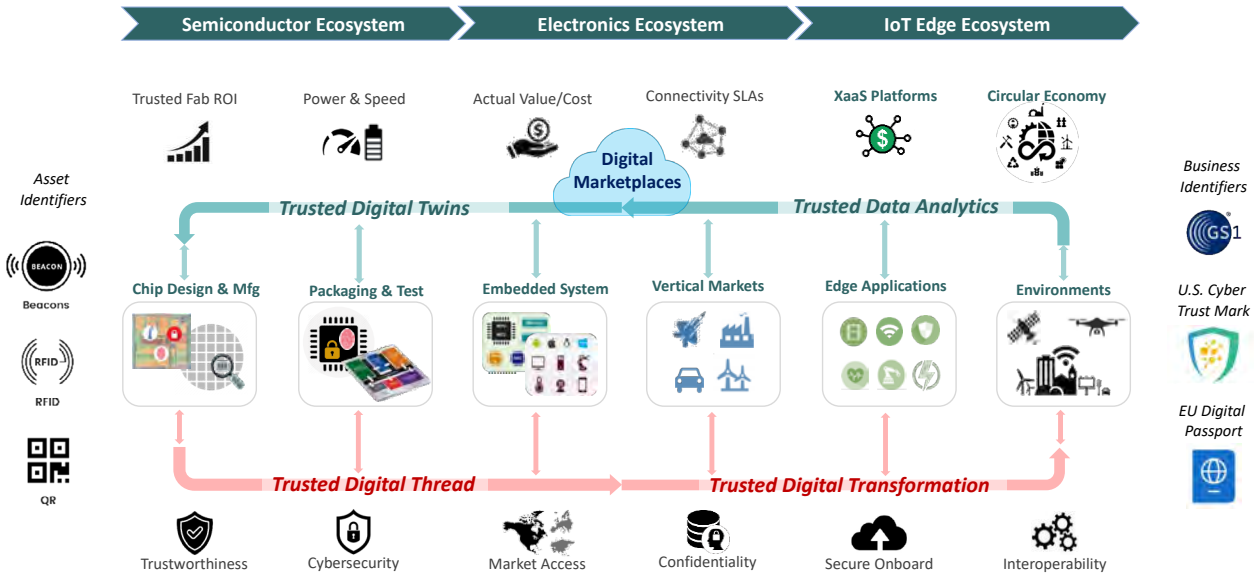


Figure 14. Supply Chain Traceability Enables Vulnerability Mitigation Across the IoT Value Chain[90]

during chip design and manufacturing; instituting global chip identifiers linking to local identifiers and chip fingerprints; using IoT technology and global microchip identifiers to track chips; creating digital twins and digital threads starting from manufacturing;[91] managing chip supply chains by using AI to improve efficiency;[92] using IoT platforms with sensors in manufacturing produce data used for AI and analytics across value chains;[93] and leveraging digital threads[94] of data that enable XaaS to create value for IoT ecosystems.

The lack of an infrastructure that supports traceability (e.g., a Root of Trust mechanism embedded in chips during manufacturing) leads to continued supply chain risks and market imbalances for chips used in IoT devices. Investments by the U.S. and its partners, including those that support voluntary participation by manufacturers and integrators, could encourage innovation and support digital transformation to better address the supply chain vulnerabilities.

Finding 6. Establishing trust in IoT requires a multi-dimensional ecosystem perspective, extending beyond cybersecurity and privacy.

Trust is paramount to the sustained adoption, use and scaling of IoT. Without it, consumers, businesses, and organizations are reluctant to embrace IoT solutions due to concerns about data security, privacy, confidentiality, and threats to our critical infrastructure using IoT systems.

[90] Figure credit: Tom Katsioulas, used with permission.

[91] NIST Notice of Intent to announce an open competition for a new Manufacturing USA Institute on the topic of Digital Twins issued in the Federal Register on February 1, 2024 available at https://www.federalregister.gov/documents/2024/02/01/2024-02025/chips-manufacturing-usa-institute

[92] Bob Violino, "How using analytics and AI can help companies manage the semiconductor supply chain" from CNBC (October 19, 2022) available at https://www.cnbc.com/2022/10/19/how-ai-can-help-companies-manage-the-semiconductor-supply-chain.html

[93] Ondrej Burkacky, Mark Patel, Nicholas Sergeant, and Christopher Thomas, "Reimagining fabs: Advanced analytics in semiconductor manufacturing" from McKinsey and Company (March 21, 2017) available at https://www.mckinsey.com/industries/semiconductors/our-insights/reimagining-fabs-advanced-analytics-in-semiconductor-manufacturing

[94] "Circular Economy Product Design and Digital Thread" program description from the National Institute of Standards and Technology available at https://www.nist.gov/programs-projects/circular-economy-product-design-and-digital-thread

The World Economic Forum, in collaboration with technology companies, government, and consumer advocates, have created a holistic framework for digital trust (Figure 15).[95] The framework considers a variety of dimensions, including cybersecurity, confidentiality, privacy, safety, transparency, and fairness.

Loss of trust can occur due to insecure devices, compromised supply chains, or inaccurate data. This impacts business operations and digital twin systems. Effective IoT solutions require trusted business ecosystems and partnerships. A broader, holistic approach is needed to build and maintain trust across technology, data and analytics, operations, and ecosystems. Examples of trust needs in these dimensions follow:



Figure 15: Holistic Framework for Digital Trust Encompasses Multiple Dimensions[96]

Technology

- **Trusted IoT Devices:** Trust in IoT starts with awareness about trustworthiness of IoT devices, ensuring security, data protection and consumer awareness.
- **Trusted IoT Networks:**[97] Securing Telco infrastructure and wireless networks, with encryption, authentication, and monitoring, are vital for trusting IoT.
- **Trusted cloud platforms:** These are key for IoT deployments, offering security, scalability, reliability, data analytics, interoperability, and cost efficiency.

Data and Analytics

- **Trusted IoT Data for Privacy:** Users have the right to control their data and its usage. Regulations like the General Data Protection Regulation (GDPR)[98] and California Consumer Privacy Act (CCPA)[99] can help increase trust.
- **Trusted Data for Confidentiality:** Safeguarding enterprise data for IoT is key for operations securing their data transport, storage, access for devices.
- **Trusted IoT Digital Twins:**[100] Trust in data for digital twins is key for reliability and integrity of analytics marketplaces and platform-based ecosystems.
- **Trusted Analytics and AI:** Trust in the data used for analytics and training models for AI algorithms is critical for assured, unbiased, and ethical insights.

Operations

- **Trusted IoT Supply Chains:**[101] Traceability from component sourcing to IoT device assembly with "Trustworthiness Score"[102] can minimize vulnerabilities.
- **Trusted IoT Digital Transformation:** Digital trust in operations and business is a key enabler for IoT adoption and key for successful digital transformation.
- **Trusted Digital Threads:** Continuous flow of trusted data throughout product lifecycles supply chains is the backbone of trusted IoT ecosystems.[103]

---

[95] "Digital Trust" initiative from the World Economic Forum available at https://initiatives.weforum.org/digital-trust/home

[96] "Digital Trust" initiative from the World Economic Forum available at https://initiatives.weforum.org/digital-trust/home . Figure used per World Economic Forum License Terms available at https://www.weforum.org/about/licence-terms-on-the-use-of-forum-publications-and-materials/

[97] Jeffrey Caso, Zina Cole, Mark Patel, and Wendy Zhu, "Cybersecurity for the IoT: How trust can unlock value" from McKinsey and Company (April 7, 2023) available at https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value

[98] "What is GDPR, the EU's new data protection law?" from GDPR.EU available at https://gdpr.eu/what-is-gdpr/

[99] "California Consumer Privacy Act" (CCPA) from Office of the Attorney General of California available at https://oag.ca.gov/privacy/ccpa

[100] Roberto Argolini, Federico Bonalumi, Johannes Deichmann, and Stefania Pellegrinelli, "Digital Twins: The key to smart product development" from McKinsey and Company (July 31, 2023 available at https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/digital-twins-the-key-to-smart-product-development

[101] Vishal Guar and Abhiva Gaiha, "Building a Transparent Supply Chain" from *Harvard Business Review* (May-June 2020 Issue) available at https://hbr.org/2020/05/building-a-transparent-supply-chain

[102] January 2023 IoTAB Invited Speaker: Shokubai, Francois-Frederick Ozog - "IoT Trustworthiness Score". Written Comments from Francois-Frederick Ozog available at https://www.nist.gov/system/files/documents/2023/03/01/Public%20Comments%20-%20Francois-Frederic%20Ozog.pdf

[103] "Enabling the End-to-End Digital Thread" from Semi (March 25, 2021) available at https://www.semi.org/en/blogs/technology-trends/Enabling-End-End-Digital-Thread

Ecosystems

- **Trusted IoT Digital Marketplaces:** Secure online platforms enable trustworthy marketplaces for sharing information and IoT data with traceable transactions.
- **Trusted IoT Business Ecosystems:** Trust in business ecosystems requires platforms supporting governance rules[104] and mechanisms that foster trust.[105]
- **Trusted IoT Partnerships:** Building trust for end-to-end IoT solutions requires trusted PPPs prioritizing security, privacy, confidentiality, and collaboration.

A holistic approach to trust is paramount to the acceptance of IoT technologies. Ensuring trustworthiness is key to speeding adoption, proliferation, and growth. Building and maintaining trust is an ecosystem responsibility, from manufacturers to end-users, as it unlocks IoT's potential for informed decision-making, and innovation.

Finding 7: Privacy concerns undermine trust in IoT and are a significant barrier to widescale adoption.

IoT devices present significant data privacy challenges as the data they collect can be stolen, improperly accessed, or used for unintended purposes. To address these issues, initiatives like Privacy Transparency for IoT have been introduced to enhance the visibility and comprehension of privacy practices for consumers. Additionally, specific measures such as including IoT privacy information on automobile Monroney Labels and introducing a Location Tracking Notice in IoT e-labeling are instrumental in informing consumers about the privacy features of IoT-enabled vehicles. For example, in a 2023 McKinsey and Company article titled "IoT Cybersecurity: How Trust Can Unlock Value"[106] 61% of IoT buyers surveyed deem digital trust and privacy as a critical element of their purchase decisions.

Lack of Comprehensive Privacy Laws Hinders Consistent Implementation and Adoption of Protections

The absence of comprehensive privacy laws significantly hinder the consistent application and adoption of IoT technologies. Without clear and uniform regulations, businesses and consumers face uncertainties regarding data security and privacy, leading to hesitancy in fully embracing IoT solutions. This regulatory gap creates a fragmented landscape where companies struggle to implement standardized practices, ultimately slowing down the growth and potential benefits of IoT innovations.

Children's Privacy and IoT

The intersection of children's privacy and the Internet of Things (IoT) highlights a critical concern as IoT devices, such as smart toys and educational tools, become more embedded in children's daily lives. These devices often collect extensive personal and sensitive information, yet this data collection is typically opaque, raising substantial privacy risks. These risks include breaches of privacy and unauthorized data sharing, which can create long-lasting digital footprints. The main challenge lies in the design of these devices, which prioritize continuous data collection and connectivity over privacy, necessitating alignment with privacy-centric guidelines, particularly for diverse age groups and developmental stages.

One federal privacy recommendation that addresses these concerns is the Minimization of Data Collection and Retention, which advocates collecting only necessary data and retaining it for the shortest time required. By embracing this minimization principle, manufacturers can play a pivotal role in enhancing privacy protections in IoT devices for children. They can provide guardians with clearer, age-appropriate privacy information and control options, fostering a safer, trust-rich digital environment for young users.

Extended Reality (XR), Privacy and IoT

Extended Reality (XR) and the Internet of Things (IoT) represent the forefront of digital innovation, merging Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) with connected devices to reshape our interactions in both digital and physical worlds. Despite their benefits, these technologies raise significant privacy concerns, collecting vast amounts of personal data, which can impact user trust and hinder technology adoption. Exploring real-world scenarios illustrates how implementing privacy recommendations can address these concerns, fostering trust and encouraging broader acceptance of XR and IoT applications.

Privacy is a central issue in integrating XR and IoT into everyday life, which involves complex data types and extensive device interconnectivity. This report acknowledges the transformative impact of plain language policies and transparent data sharing on user comprehension and trust. Principles like Privacy by Design and the use of Privacy Enhancing Technologies (PETs) ensure that privacy considerations are embedded in technology development from the start, providing a foundation for responsible innovation and helping users enjoy advanced technologies without compromising their privacy.

[104] Governance Rules steer community behavior for collaboration. Key principles include transparency, accountability, IP rights management, conflict resolution, compliance protocols, scalability provisions, and feedback mechanisms.

[105] Marcos Aguiar, Ulrich Pidun, Santino Lacanna, Niklas Knust, and François Candelon, "Building Trust in Business Ecosystems" from BCG (February 10, 2021) available at https://www.bcg.com/publications/2021/building-trust-in-business-ecosystems

[106] Jeffrey Caso, Zina Cole, Mark Patel, and Wendy Zhu, "Cybersecurity for the IoT: How trust can unlock value" from McKinsey and Company (April 7, 2023) available at https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value

Finding 8: IoT cybersecurity concerns are a major barrier to widescale adoption.

IoT raises several cybersecurity 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 computing provides the technical infrastructure for IoT to scale, a trusted infrastructure is necessary for IoT market adoption to evolve and scale.

IoT cybersecurity challenges are exacerbated by:

- **Wide range of IoT devices and systems for diverse applications.** IoT devices, ranging from smart home appliances and wearables to industrial sensors, come with diverse specifications and configurations from multiple vendors. This diversity complicates the implementation of a universal security solution. Moreover, larger multi-vendor environments make it increasingly challenging to manage, track, and secure each device continuously.
- **IoT devices are often resource constrained.** Many IoT devices have limited computing power, memory, and battery life. This restricts their ability to implement robust security measures such as encryption, authentication, and intrusion detection, leaving them vulnerable to attacks.
- **Large numbers of unpatched devices.** The sheer number of IoT devices in use is vast and growing rapidly. This makes it challenging for manufacturers and users to keep track of and manage all the devices on their networks and ensure they are properly secured. Some devices may lack over-the-air update capabilities, while others are in remote and hard-to-reach locations making software updates impossible.
- **Legacy Systems.** Millions of connected legacy devices that are built on outdated or proprietary operating systems and software platforms without cybersecurity in mind. Furthermore, other devices have reached the end-of-life, but are still in use, and do not receive regular security updates or patches. This leaves them vulnerable to known exploits and vulnerabilities.
- **Interoperability Issues.** IoT devices often need to communicate with each other and with other systems and services. Ensuring secure communication and interoperability between devices from different manufacturers can be complex and prone to vulnerabilities.
- **Need to adopt and harmonize standards.** The IoT industry lacks standardized security protocols and best practices that are widely adopted and globally harmonized, leading to inconsistencies in security implementations across different devices and manufacturers.
- **Human Factors.** IoT and connected devices may expose vulnerabilities due to a variety of reasons. For example, the devices may be installed, integrated, and configured improperly. Users may not have implemented the latest IoT cybersecurity best practices. Additionally, IoT devices are often deployed in physically unsecured environments where they may be easily tampered with or physically compromised.
- **Evolution of Cyber Threats.** Cyber threats targeting IoT devices are constantly evolving, with attackers exploiting new vulnerabilities and attack vectors. This requires continuous monitoring and adaptation of security measures to stay ahead of emerging threats.

Finding 9: IoT modules built by Chinese companies dominating our market poses a serious national security and economic risk.

IoT modules are communication components that allow a smart device to communicate with the network. IoT components, modules and technologies built by Chinese companies are a significant part of the market. For IoT modules the top 6 companies are Chinese account for 64% of the global market.[107] The remaining 22.4% includes a limited number of U.S. companies that offer IoT modules.[108] The top 2 Chinese companies account for 46% of the market and are likely to dominate the $67 billion IoT module market by 2030.[109]

Cybersecurity

There are cybersecurity concerns from industry and government about IoT equipment and components (including modules) produced by companies in China, especially if such modules are used in our critical infrastructure. The majority market share controlled by Chinese companies raises significant cybersecurity risks.[110]

[107] "Quectel tops charts as cellular IoT module shipments soar" from IoT M2M Council (April 5, 2023) available at https://www.iotm2mcouncil.org/iot-library/news/iot-newsdesk/quectel-tops-charts-as-cellular-iot-module-shipments-soar/

[108] Qualcomm, Silicon Labs, Skyworks Solutions, Semtech Corporation, Digi International

[109] Taha Bin Masood, "Cellular IoT module market Q1 2024 update: Demand recovery, market trends, and competitve landscape" from IoT Analytics (June 13, 2024) available at https://iot-analytics.com/global-cellular-iot-module-market/

[110] G. Noone, "China's cornered the IoT market. That could be a cybersecurity nightmare." from *Tech Monitor* (January 27, 2023) available at https://www.techmonitor.ai/technology/cybersecurity/chinas-cornered-the-iot-market-that-could-be-a-cybersecurity-nightmare?cf-view&cf-closed

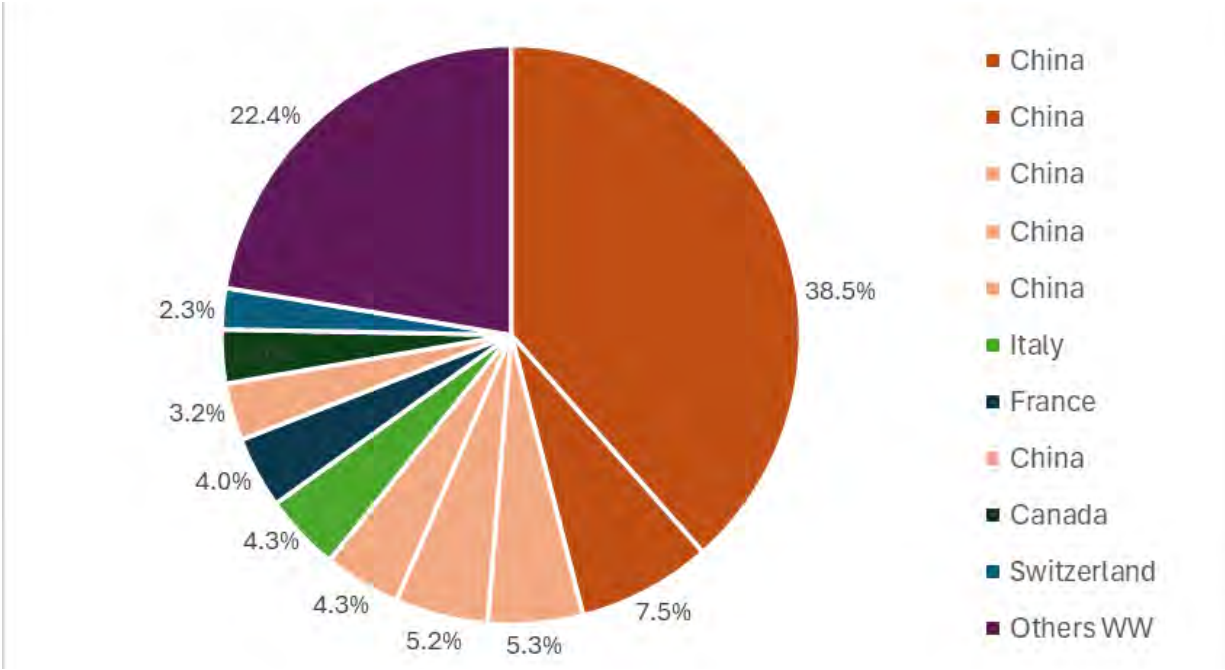


Figure 16: Global cellular IoT module shipments share by country in 2022.[111]

These concerns were highlighted in a letter[112] dated August 7, 2023, from Chair Mike Gallagher (R-WI) and Ranking Member Raja Krishnamoorthi (D-IL) of the House Select Committee on the Chinese Communist Party (CCP) to Federal Communications Commission (FCC) Chair Jessica Rosenworcel. The letter raised a series of questions regarding the Federal Communications Commission's (FCC) ability to track Chinese-made IoT modules and the potential risks of Chinese-made IoT modules. The members were concerned about the way in which IoT devices could be remotely accessed posing opportunities for malicious use. Specifically, People's Republic of China (PRC)-based companies could, under the direction of the government, exfiltrate data from U.S. IoT devices and products or shut them down entirely. To demonstrate the implications of connectivity modules in IoT, they cited an example from the conflict in Ukraine, where tractors were remotely shut off after being captured by Russian forces. Underscoring their concerns about IoT, they asked the FCC chair:

- Whether the FCC can track cellular IoT modules and if so, share information about the number of PRC-based companies operating in U.S. networks.
- Whether the FCC is concerned about the presence of PRC-based IoT modules operating in U.S. networks.
- Whether requiring certification for modules would effectively counter PRC-based modules from affecting the U.S. networks.
- Whether the FCC needs additional statutory authority from Congress to address this concern.

These cybersecurity concerns raised are consistent with other recent and related actions, including:

- U.S. Department of Commerce Begins Regulatory Process to Consider National Security Risks Posed by Information and Communications Technology and Services (Information and Communications Technology [ICTS]) Integral to Connected Vehicles.[113]
- Lawmakers urge Biden Administration to investigate Chinese light detection and ranging (LiDAR) companies to determine whether they should be on government-restricted entities list.[114]

[111] Figure credit: Tom Katsioulas, custom figure using data from Quectel tops charts as cellular IoT module shipments soar" from IoT M2M Council (April 5, 2023) available at https://www.iotm2mcouncil.org/iot-library/news/iot-newsdesk/quectel-tops-charts-as-cellular-iot-module-shipments-soar/ . Figure used with permission.

[110] Figure credit: Tom Katsioulas, custom figure using data from Quectel tops charts as cellular IoT module shipments soar" from IoT M2M Council (April 5, 2023) available at https://www.iotm2mcouncil.org/iot-library/news/iot-newsdesk/quectel-tops-charts-as-cellular-iot-module-shipments-soar/ . Figure used with permission.

[112] Letter from Mike Gallagher, Chairman and Raja Krishnamoorthi, Ranking Member of the Select Committee on the Chinese Communist Party to The Honorable Jessica Rosenworcel, Chairwoman, Federal Communications Commission available at https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2023-08-07-cellular-iot-modules.pdf

[113] "Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles" from U.S. Department of Commerce (February 29, 2024) available at https://www.commerce.gov/news/press-releases/2024/02/citing-national-security-concerns-biden-harris-administration-announces

[114] Edward Graham, "Lawmakers raise concerns over Chinese-made LiDAR tech" from Nextgov/FCW (November 29, 2023) available at https://www.nextgov.com/defense/2023/11/lawmakers-raise-concerns-over-chinese-made-lidar-tech/392355/

- Draft legislation has been written covering federal procurement prohibition on covered IoT modules or devices manufactured in a country the government of which is a foreign adversary.[115]

Trade Concerns

Trade concerns result from the deep penetration of Chinese manufacturers into the western IoT modules market. The dominant position drives other competitors out of the market and reduces the diversity of products available to businesses and consumers.

If foreign entities are supporting their manufacturers to the point where normal market forces are unbalanced, it could lead to an unhealthy monopoly. The American Enterprise Institute cited the broader practice of overcapacity as "state interference in the market."[116]

One industry stakeholder shared that while the Chinese module makers have full access to the U.S. and other markets, American companies do not have the same access to the Chinese IoT market. Another stakeholder stated that "they are selling the modules at the price that it costs us to make them."

A January 5, 2024, letter from the Select Committee on the CCP to Secretary of Commerce Gina Raimondo and U.S. Trade Representative Ambassador Katherine Tai stated that the "People's Republic of China (PRC) is on track to flood the United States and global markets with foundational (commonly referred to as "mature" or "legacy") semiconductors. While the Administration has taken strong actions to ensure U.S. advanced semiconductor technology is not transferred to the PRC, far less attention has been given to the risk that a surge of PRC-made foundational chips poses to U.S. economic security."[117]

Notably, while the ubiquitous nature of these IoT modules may provide short-term price benefits for buyers, there may be potential cybersecurity risks that result from externally made components. The apparent concentration of the market with four Chinese firms only exacerbates these concerns.

Finding 10: Quantum computing poses a major threat to IoT cybersecurity.

Public key encryption, which protects Internet data and communications, is based on the difficulty of solving a mathematical problem in a realistic time. Once quantum computing has advanced to a certain point, that assumption is no longer valid. A classical computer looking to "crack" RSA-2048 encryption would require about 300 trillion years due to one very slow step (that of "factoring" a very large number); a sufficiently powerful quantum-enabled computing system running Shor's Algorithm is expected to do it in on the order of hours.[118]

Quantum computers have the potential to bypass the encryption locks that currently protect the world's communications and data. According to the White House National Security Memorandum/ NSM-10 on Quantum Computing, "a quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet- based financial transactions."[119]

Like server and client computers, IoT devices are vulnerable to the risks posed by quantum computing for a variety of reasons:

- Much of encrypted Internet traffic is at risk for the so-called "harvest now, decrypt later" approach, where data are captured today and saved for when quantum computers have advanced to be able to decrypt.
- Moreover, IoT devices often have limited computational and energy resources, making them ill-equipped to handle the sophisticated "post-quantum" encryption algorithms required to resist quantum attacks.
- Additionally, the sheer scale and diversity of IoT deployments make it challenging to implement security updates and patches uniformly across all devices. As a result, cybercriminals could exploit vulnerabilities in IoT devices to gain unauthorized access to sensitive data or launch large-scale attacks, potentially causing widespread disruption and damage.
- Despite IoT's extremely low/non-existent baseline level of security, IoT is used in a variety of industries and applications. Of particular concern are IoT used in critical infrastructure, manufacturing, defense, and healthcare where the potential

[115] As defined by section 8(c) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1607(c))

[116] L. Ya, "China's overcapacity results from state interference in markets, say analysts" from Voice of America (April 5, 2024) available at https://www.voanews.com/a/china-s-overcapacity-results-from-state-interference-in-markets-say-analysts-/7559251.html

[117] Letter from Mike Gallagher, Chairman and Raja Krishnamoorthi, Ranking Member of the Select Committee on the Chinese Communist Party to The Honorable Gina Raimondo, Secretary, U.S. Department of Commerce available at https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/1.05.24-legacy-chips-letter.pdf

[118] Marin Ivezic, "Q-Day Predictions: Anticipating the Arrival of Cryptanalytically Relevant Quantum Computers (CRQC) from *Post Quantum* (July 27, 2023) available at https://postquantum.com/post-quantum/q-day-crqc-predictions/

[119] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," NSM-10, The White House (May 4, 2022) available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

for the use of quantum computing to conduct cyberattacks is high (either for access to their data or to spoof/corrupt the data). They also tend to have long useful lives when installed.

However, much IoT data today is not valuable enough to collect ("harvest now"). Today's sensor readings and security camera footage will be of limited value in the future. When quantum computers can crack classical encryption in real time, there will be a significant issue with the visibility of sensitive traffic such as credentials. But that situation is well in the future.

As a result, IoT devices are not as high a priority as enterprise IT systems, when considering and prioritizing the mitigation of the threats posed by quantum computing.

While there are valid concerns about quantum computers breaking today's encryption algorithms, cryptanalytically relevant quantum computers (CRQC) powerful enough to do so may not be developed until at least the 2030s.[120] The response to post-quantum cybersecurity is in its initial stages of evolution. For example, NIST is in the process of standardizing a set of post quantum cryptographic algorithms. Three standards were announced in August 2024 with evaluation continuing on two other sets of algorithms.[121]

Even though the 2030s are not that far away, there are no candidate low-complexity post-quantum encryption algorithms that would work for smaller IoT devices. Further research is needed to develop IoT-suitable post- quantum cryptography solutions.

Finding 11: Interoperability is a key challenge for IoT across multiple industries.

Interoperability allows heterogeneous devices and systems to 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 varied 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.

Many areas of IoT technology still need data model standardization, and reaching consensus on standards takes time. It is important to recognize that there are existing communications and protocol standards, though the data and commands carried ("application layer") are often proprietary to a manufacturer or integrator.

For example, an IoT soil sensor and hub might collect humidity data and communicate with the "home" server via 5G data with additional Transport Layer Security (TLS) encryption. This is a stack of protocols that are fully standardized in industry. However, the data itself may be meaningless to any application other than the original manufacturer's.

While open standards for data models could enable seamless interoperability, the market is currently dominated by products with proprietary standards, "walled garden"[122] ecosystems and varying standards. Some vendors believe their proprietary standards are superior, others entered the market before standards emerged, and some fear commoditization.

But integrating devices and systems is challenging. Even older and newer systems from the same vendor sometimes do not work together. These issues create "siloed" data trapped within a specific device or vendor's ecosystem. As a result, integrating systems to enable communication and data exchange is complex and costly, requiring additional middleware and custom integration.

This inability to integrate IoT with existing legacy and modern systems hinders innovation and the full benefits of interconnected, automated systems. Examples include:

- Factories face operational inefficiencies and higher costs due to this lack of integration. In cities, different municipal agencies operate IoT systems independently, preventing city-wide benefits. In healthcare, interoperability issues can delay responses to patient conditions, leading to errors. In transportation and logistics, the lack of data exchange across the supply chain limits agility and resilience, making it difficult to respond to disruptions.
- The lack of interoperability in IoT systems prevents significant cost savings and revenue opportunities. For example, in healthcare, it could result in $35 billion in missed annual savings in the U.S.[123] In renewable energy, achieving interoperability could save up to $10 billion by reducing transaction costs and increasing efficiency. Without it, there may be $59 billion in lost opportunities from innovative energy applications not being deployed in buildings.[124]

[120] E. Parker, "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret," from RAND (September 13, 2023) available at https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html

[121] Notice of Issuance of Federal Information Processing Standards(FIPS): FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard from the Federal Register (August 14, 2024) available at https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based

[122] 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.

[123] "The value of medical device interoperability," from West Health Institute (2013) available at https://www.westhealth.org/wp-content/uploads/2015/02/The-Value-of-Medical-Device-Interoperability.pdf

[124] "The National Opportunity for Interoperability and its Benefits for a Reliable, Robust, and Future Grid Realized Through Buildings," from the U.S. Department of Energy (February 2016) P. ii available at https://www.energy.gov/eere/buildings/articles/national-opportunity-interoperability-and-its-benefits-reliable-robust-and

- Interoperability challenges in IoT lead to adverse environmental impacts due to inefficient operations. In renewable energy, they hinder the integration of energy-efficient technologies, resulting in higher emissions, increased costs, and less energy security. In transportation and logistics, improved interoperability and real-time data sharing could reduce global freight emissions by 22%.[125]
- The lack of interoperability in IoT creates vendor lock-in and switching barriers, resulting in a fragmented market of "walled garden" solutions. These solutions only work with a limited set of compatible equipment, reducing choices and forcing buyers to stick with specific vendors. IoT technologies based on proprietary standards do not work with other systems, compelling buyers to continue using the same vendor and its partners, often leading to higher costs, fewer innovative features, and limited capabilities. Migrating from these systems to other lower cost or more innovative alternatives is difficult and may require significant switching costs.

Finding 12: A variety of connectivity challenges are hindering IoT adoption, operation, and scaling.

Connectivity challenges limit IoT deployment. Connectivity service coverage is essential for IoT adoption and operation. The COVID-19 pandemic highlighted the digital divide and the need for connected communities. Ongoing government and private initiatives aim to make connectivity ubiquitous. For example, the federal Bipartisan Infrastructure Law allocates part of its $65 billion to infrastructure in underserved areas, and California is investing $6 billion in a middle mile fiber network.[126] The FCC is exploring the use of TV white spaces for rural IoT connectivity, and satellite operators are launching low earth orbit (LEO) broadband services. Private enterprises are also establishing long-term evolution (LTE) and fifth-generation technology (5G) networks for campuses, factories, and other facilities.

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 in rural and remote areas. 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 (asymmetric) 100/20 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 access to 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 many building structures, high wireless device density, are most susceptible to disruptions and issues.
- The sunsetting of connectivity technologies is a major challenge for IoT. Millions of IoT devices in the U.S. still use 2G and 3G networks, which are being phased out as 4G and 5G become prevalent. Carriers have turned off 2G networks (AT&T in 2017, T-Mobile in 2022) and 3G networks (2021-2022), rendering many devices obsolete since they cannot be upgraded. Replacing these devices is a costly and complex task for IoT users. Additionally, reliable wireless coverage in specific operational areas, such as agriculture, environmental monitoring, rural emergency services, and remote infrastructure, is critical. For example, agricultural sensors require connectivity across vast lands, far beyond the reach of typical broadband to farmhouses.
- Lack of "last acre" service hinders the deployment of IoT in the field. Enabling "last acre" wireless service availability is also a major challenge. Not all areas can be covered due to geography and topographic constraints. In addition, signal attenuation and interference from hills and tree foliage is a common challenge. According to one technology solution provider, soil moisture sensors placed underneath leafy vegetables in a farm had experienced difficulties communicating with a nearby gateway.
- Unfavorable economics and permitting challenges hinder service availability. Finally, many wireless operators face unfavorable economics, construction challenges and inability to secure suitable "right of ways." Privately owned wireless networks are financially infeasible to all but the largest farms who have the capital and resources to operate this network.

[125] M. Westervelt, R. Aland, and I. Dupraz, "Solving the Global Supply Chain Crisis with Data Sharing" Center for Reimagined Mobility, June 28, 2022. https://reimaginedmobility.org/freight-data-report/

[126] "California All: Middle Mile Broadband Initiative" from the California Department of Technology available at https://middle-mile-broadband-initiative.cdt.ca.gov/

Finding 13: Artificial Intelligence (AI) is critical to unlocking and accelerating the value of IoT, but significant challenges must be addressed.

IoT and Artificial Intelligence (AI) are two distinct technologies that complement each other to create value. IoT devices collect data and report about their physical environments. AI (including machine learning) algorithms act on the collected data to create insights for decision-making and initiate autonomous responses. These two technologies are beginning to converge to form Artificial Intelligence of Things (AIoT).

Analytics and AI unlock the value of IoT by transforming sensor data into actionable insights. In factories, IoT sensors monitor equipment status while AI predicts maintenance needs. In public spaces, video cameras capture data, and AI detects suspicious activities. In agriculture, AI-enabled cameras on robots identify ripe fruits and command picking. IoT sensors in smart meters and energy systems use AI to balance electricity supply and demand.

AI is ideal for two types of IoT applications:

1. Data analysis and subsequent predictive recommendations and actions: Machine Learning and Deep Learning 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 tasks (clerical work, order taking, food service), freeing up human resources to focus on higher value, human-exclusive skills (creative thinking, problem solving, people skills, emotional intelligence, reasoning, negotiation, and decision-making).

In practice, processing AI algorithms may occur on the IoT devices itself, a nearby gateway or server, or in a remote server in a cloud data center. As the microprocessors in the IoT devices become more powerful, more of the algorithm processing is occurring on the edge (i.e. device, gateway, and nearby servers), instead of the cloud. Processing algorithms at the edge overcome latency issues for real-time IoT applications, as well as limited or unreliable wireless connectivity service. The collected data may be stored for later analysis or analyzed immediately but not stored.

AI Technologies

Artificial Intelligence (AI) is a collection of technologies and algorithms. They include machine learning (ML), deep learning (DL), natural language processing and understanding (NLP/NLU), computer vision (CV), machine reasoning (MR) and generative AI. 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 patterns to make predictions, classify data, recognize objects or images, and understand speech or text.

Generative AI (GenAI) offers exciting new possibilities for IoT. While "traditional" AI is trained on large data sets with human input, conversations, user queries and responses, GenAI is trained on different sets of data to learn predictive patterns to produce various types of content, including text, imagery, audio, and synthetic data.

GenAI makes sense of IoT data to achieve desired outcomes. For instance, a city planner can ask how to adjust traffic signals to reduce accidents and congestion. AI can recommend specific signal timings by analyzing IoT data, road types, historical traffic patterns, and projected weather. This integration of AI with IoT technologies allows small communities to achieve results like those of larger cities with more resources.

Challenges

Despite the value offered by AI in IoT, several complex challenges may hinder its effectiveness and use. Examples of key challenges include:

- **Data ownership.** AI needs a significant amount of data to train its algorithms and models. Some of the data needed may come from owners that do not want to share. For example, if a farmer uses an IoT application to help improve its production yields, the IoT developer may collect the grower's information to further tune the algorithm. However, the data collected and used may contain information on the farmer's proprietary processes, which, if not properly secured, may inadvertently help their competitors.
- **Data Management.** Proper data management is foundational to successful AI implementation, as highlighted by IoT Analytics.[127] The report identifies seven key components of data management including sources, ingestion, storage, transformation, analytics, governance, and orchestration—that are essential for AI success. These elements ensure data integrity, accessibility, and usability, allowing AI models to operate optimally. The growing focus on AI and ML underscores the need for a comprehensive U.S. data strategy and for consideration of data strategies being pursued elsewhere.[128] Without a data strategy, AI initiatives risk failure. Investing in data

[127] Oktay Demir, "How global AI interest is boosting the data management market" from IoT Analytics (May 28, 2024) available at \https://iot-analytics.com/how-global-ai-interest-is-boosting-data-management-market/

[128] European Commission, "A European strategy for data", available at https://digital-strategy.ec.europa.eu/en/policies/strategy-data

management is crucial for companies aiming to leverage AI's transformative potential fully.

- **Accuracy.** AI algorithms for IoT may generate outcomes that may not be equitable or available to everyone, or it may adversely affect members of certain communities disproportionately. For example, a large retail chain was banned by the Federal Trade Commission (FTC) from using facial recognition video systems for five years because its algorithms generated false positives, leading to false detentions and unfair treatment of some of its customers.[129]
- **Explainability of outcomes.** AI algorithms for IoT may generate outcomes that are neither transparent nor explainable. For example, an Internet of Medical Things (IoMT) device operating autonomously may create a recommendation that may lead to some unfavorable outcome for a patient. However, how it arrived at the recommendation is unknown. In critical situations, especially those that impact human safety, this "black box" processing brings distrust and reluctance to proceed and is a major barrier.
- **Algorithm disruption.** While a lot of attention is focused on the cybersecurity aspects of IoT, less attention is directed at protecting the integrity of the AI algorithm. Someone wishing to disrupt an IoT application can "trick" the algorithm by presenting "poisoned data". For example, scientists have disrupted self-driving cars by making subtle changes to stop signs.[130] Protestors have immobilized self-driving vehicles by placing traffic cones on vehicle hoods. [131]
- **IoT device constraints.** AI algorithms require powerful microprocessors to process data. However, many IoT devices are power and computationally constrained, limiting their capabilities to process complex algorithms. Industry efforts to address this challenge include development of algorithms designed to run on constrained devices (e.g., tinyML) and development of more AI-capable processors. Continued research is necessary to address this challenge.
- **Open-source large language models (LLMs) and AI algorithms.** The "open source" aspect of this category adds benefits such as increased accessibility, transparency, and the potential for collaborative innovation, enabling a wide range of applications and advancements. However, there are also additional significant risks, including misuse for malicious purposes, lack of accountability, and issues with data privacy, security, reliability, uneven quality, as well as challenges in ensuring ethical use and compliance with regulations.
- **Governance.** Balancing the above benefits and risks is crucial for the responsible development and deployment of IoT and AI technologies. For example, the use of AI to support autonomous IoT applications raises a variety of issues, including ethical use of AI, fairness, transparency, accessibility, and equitable distribution of value. Addressing these challenges with governance is necessary for the further scaling of autonomous IoT.

Finding 14: The IoT-enabled economy is unlocked and accelerated with platform-based business ecosystems, which require multi-stakeholder collaborative partnerships to be successful.

The potential opportunity of the future IoT-enabled economy can be extrapolated by examining the Internet and its impact on the economy. The Internet connected people with people, businesses with businesses, and people with businesses. In doing so, the Internet facilitated the development of digital platforms and business models and services enabled by connectivity.

A platform-based business model "creates value by facilitating exchanges between two or more interdependent groups, usually consumers, partners, and producers. To accelerate adoption, platform-based solutions harness and create large, scalable networks of users and resources that can be accessed on demand. Platforms create communities and markets with network effects that allow users to interact and transact."[132] Examples of Internet digital platform businesses include eBay, Amazon Airbnb, Uber, and Facebook (now Meta).

The growing adoption and evolution of IoT will facilitate the similar development of IoT-enabled digital platforms, new business models and IoT platform-based industry ecosystems. For example, an industrial equipment manufacturer offers IoT-based "smart machines" to its factory customers. The smart machine is integrated with its cloud software platform. The manufacturer's dealers connect to the platform to monitor their customers' real-time machine condition data and remotely service the equipment. Business ecosystem strategies[133] involving

[129] "Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Safeguards" from the Federal Trade Commission (December 19, 2023) available at https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

[130] Patrick Cain, "Here's how scientists convinced self-driving cars that stop signs were speed limit signs" from Global News (August 8, 2017) available at https://globalnews.ca/news/3654164/altered-stop-signs-fool-self-driving_cars/

[131] https://www.npr.org/2023/08/26/1195695051/driverless-cars-san-francisco-waymo-cruise

[132] Alex Moazed, "Platform Business Model – Definition: What is it?" from Applico available at https://www.applicoinc.com/blog/what-is-a-platform-business-model/

[133] Ulrich Pidun, Martin Reeves, and Balazs Zoletnik, "What is Your Business Ecosystem Strategy?" from Digital Ecosystems (March 11, 2022) available at https://www.bcg.com/publications/2022/what-is-your-business-ecosystem-strategy

communities and third-party solutions providers create and offer innovative applications and services built on top of the platform to provide additional benefit to customers.

A key challenge hindering the scaling of economic benefits from IoT is that legacy technology infrastructure and processes pose barriers for new IoT-enabled services and business models. Legacy hardware and software systems often use proprietary protocols, create data silos, are vulnerable to cybersecurity attacks, and are not architected to scale. In addition, old processes designed for non-connected services need to be re-engineered to support new "XaaS" business models. However, replacing these deeply entrenched systems is costly and time-consuming, leading many companies to stick with them despite potential gains from modernization.

To advance the IoT digital economy, it is crucial to build a foundation of connectivity and IoT platforms that promote interoperability, digital transformation, and collaboration across business ecosystems.[134] History shows that platform-based economies accelerate the evolution of such ecosystems. Business ecosystems must attract resources of all types, drawing in capital, partners, suppliers, and customers to accelerate growth through cooperative networks and ecologies of competition.[135] Hardware and software value chains evolve from foundational platforms into partnerships[136] and platform-based, scalable business ecosystems.

The following types of business platforms have emerged from the Internet revolution that are also applicable to IoT:

- **Innovation Platform:** A digital ecosystem that fosters the development and adoption of new products, services, or technologies by connecting creators, developers, and end-users.
- **Transaction Platform:** A digital marketplace that facilitates the exchange of goods, services, or information between buyers and sellers, enabling secure and efficient transactions.
- **Collaboration Platform:** A digital environment shared among multiple stakeholders that enhances cooperation, communication, and coordination among them to achieve shared goals and economic benefits.
- **Hybrid Platform:** A multi-functional digital ecosystem that combines elements of innovation, transaction, and collaboration platforms to provide integrated solutions and services across different industries and ecosystems.

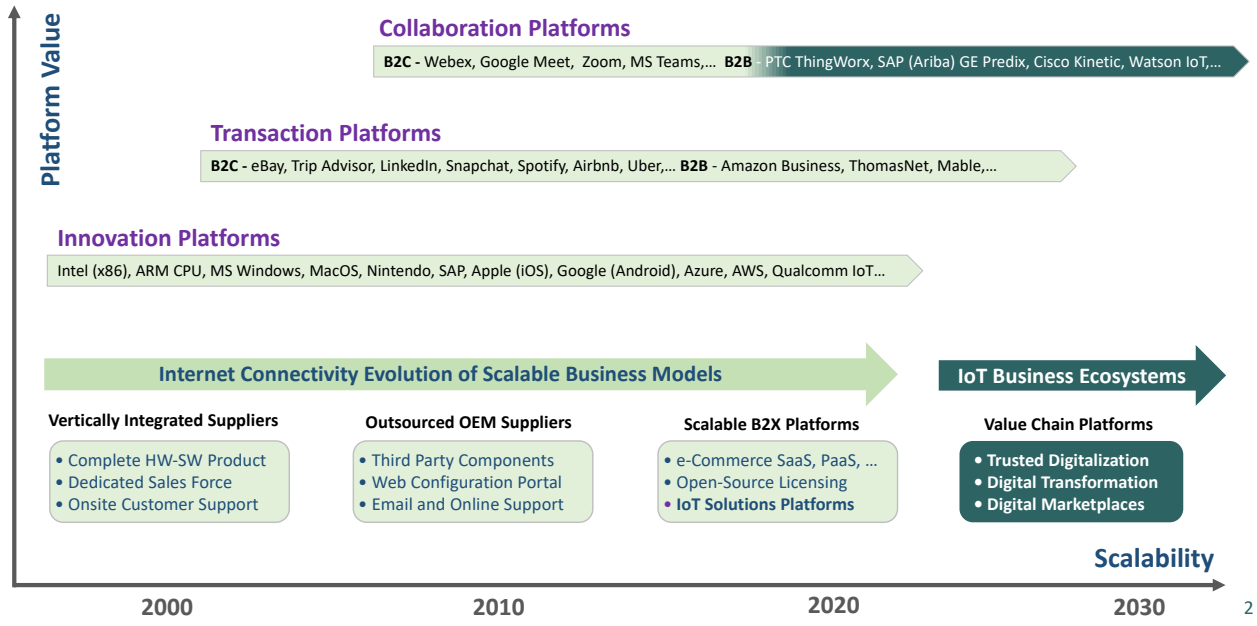


Figure 17: Evolution of the Electronics and IoT Value Chain Platforms driven by Connectivity[137]

[134] Ibid.

[135] James F. Moore, "Predators and Prey: A New Ecology of Competition" from *Harvard Business Review* (May-June 1993 Issue) available at https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition

[136] Steven Davidson, Martin Harmer and Anthony Marshall, "The new age of ecosystems: Redefining partnering in an ecosystem environment" from IBM Global Business Services (2014) available at https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ecosystem-partnering

[137] Figure credit: Tom Katsioulas, used with permission.

Applying the parallels with the Internet economy, and recognizing the value of foundational platforms in the future IoT economy, leads to the following learnings:

1. IoT platforms are the foundation of the IoT-enabled economy, similar to what previous digital platforms did for the economy. Past platform-based business ecosystems created trillion-dollar contributions to GDP. Business scholars have advocated platform-based business ecosystems and their potential to fuel economic value driven by architecture, governance, and network effects.[138] Architecture platforms like Intel x86 and Apple iOS and Android enabled third parties to add software apps on top. Transaction platforms like Airbnb and Uber enabled supply-demand matchmaking for the exchange of goods, or services. Hybrid Platforms[139] combined the advantages of both. Collaborative platforms like MS Teams, Zoom, Ariba, and GE Predix facilitated innovation, but not ecosystem orchestration across value chains.
2. IoT creates opportunities for collaboration across value chains. B2B ecosystems formed around IoT platforms create new offerings. For example, IoT provides the potential to transform linear supply chains and silos workflows to dynamic value chains and data-connected organizations. Transformative IoT platforms enable scalable ecosystems[140] where enterprises collaborate to provide end-to-end solutions that benefit all stakeholders. Platform-based B2B ecosystems based on Group Orchestration, Governance Rules and Network Effects can accelerate adoption of IoT and fuel economic growth. As such, companies offering emerging B2B collaboration platforms,[141] need to evolve their business strategies supporting open value chain partnerships where all stakeholders monetize from proven higher value offerings and shared revenues streams.[142]
3. Multi-stakeholder partnerships where participants have an economic incentive to collaborate evolve through learnings which are key to the growth of the IoT-enabled economy. For example, the IBM-Maersk TradeLens[143] IoT blockchain platform failed to gain stakeholder support in the maritime supply chain because it was not open. Successful IoT consortia that foster open and participatory partnerships among members (e.g., LoRa Alliance,[144] FIWARE,[145] Eclipse,[146] and OpenFog[147]) can facilitate the evolution of collaborative business platforms. Collaborative business platforms and ecosystems emerge as new organizational forms that provide distinct ways to cope with market failures (e.g., fragmented supply chains) or organizational failures (e.g., silos). Distributional and functional failures arise from self-interested actions by members, undermining the overall value structure.[148] Learning from these failures is crucial for designing effective governance in multi-stakeholder IoT platforms that create economic value across IoT value chains.

The future of IoT-enabled economy business will be driven by the convergence of innovation, transaction, collaboration, and hybrid platforms, each playing a crucial role in the broader IoT digital ecosystem. These platforms provide opportunities to fuel the creation of new products and services, streamline business exchanges, and enhance cooperative efforts across industries. Multi-stakeholder IoT partnerships enabled by platforms are key to accelerating widespread adoption and contributing trillions to our GDP.

---

[138] Marshall Van Alstyne and Steven Paul, "Platform Strategy and the Internet of Things" from *MIT Sloan Management Review* (November 10, 2016) available at https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/

[139] Michael A. Cusumano, David B. Yoffie, and Annabelle Gawer, "The Future of Platforms" from *MIT Sloan Management Review* (February 11, 2020) available at https://sloanreview.mit.edu/article/the-future-of-platforms/

[140] Ulrich Pidun, Martin Reeves, and Edward Wesselink, "How Healthy is your Business Ecosystem?" from *MIT Sloan Management Review* (March 9, 2021) available at https://sloanreview.mit.edu/article/how-healthy-is-your-business-ecosystem/

[141] For example: PTC ThingWorx, SAP Ariba, GE Predix, Cisco Kinetic, Azure IoT, Bosch IoT, IBM Watson IoT, Siemens MindSphere

[142] For example: Revenue Share, Marketplace Services, Data Monetization, Co-Innovation Joint Ventures, Ecosystem Branding, etc.

[143] Dan Robinson, "IBM and Maersk to shut down TradeLens supply chain platform" from *The Register* (November 30, 2022) available at https://www.theregister.com/2022/11/30/ibm_and_maersk_tradelens_shutdown/

[144] LoRa Alliance is a global association of companies that support the LoRaWAN standard using LoRa technology network server platform, for large-scale IoT networks, serves smart cities, agriculture, and industrial automation. (https://lora-alliance.org/)

[145] FIWARE is an open-source platform designed for building smart applications for smart cities, industrial IoT, and agriculture. This ecosystem allows multiple stakeholders to deploy IoT solutions using a common platform. (https://www.fiware.org/foundation/)

[146] Eclipse IoT is an open-source working group that provides frameworks, standards, and tools for IoT development. The ecosystem supports many industries by enabling the creation of interoperable IoT solutions by stakeholders. (https://www.eclipse.org/)

[147] OpenFog (now part of the Industry IoT Consortium) created an open architecture for fog computing in IoT environments the serves multiple markets, including smart cities, autonomous vehicles, and industrial automation. (https://opcfoundation.org/markets-collaboration/openfog/)

[148] Michael Jacobides, Carmela Cennamo, and Annabelle Gawer, "Externalities and complementarities in platforms and ecosystems: From structural solutions to endogenous failures" from *Research Policy* (Vol. 53, Issue 1, January 2024) available at https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3Dihub

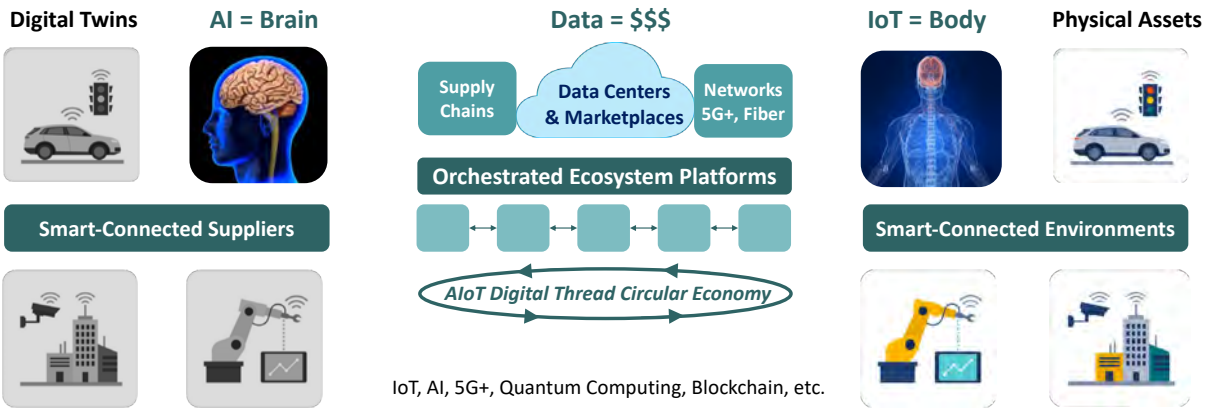


Figure 18: Data flowing in supply chains and networks used by AI creates economic value.[149]

Finding 15: The convergence of AI with IoT (AIoT) is poised to drive transformation across wide sectors of the economy, but its development and use must be managed to foster the proper outcomes and minimize unintended consequences.

The massive amounts of data generated by IoT devices across supply chains and networks, when processed by AI, is poised to drive transformative growth of the economy. However, this potential for disruption necessitates careful management and thoughtful well-crafted regulation to ensure it benefits industries while mitigating risks with IoT and AI accelerating the circular economy.[150]

AIoT is integral to the future functioning of our national economy.

If the U.S. economy was human, then IoT is the body, AI is the brain, and supply chains and networks are the arteries which data flows through.

AI and IoT data are intricately interconnected in a rapidly evolving landscape.[151] IoT devices gather vast amounts of data, such as temperature readings and user interactions, which are analyzed to optimize operations. AI uses these extensive datasets to train machine learning models that provide insights and predictions. By integrating AI with IoT, real-time data is analyzed to detect anomalies, predict failures, and enhance decision-making in smart systems.

Orchestrated business ecosystems that combine IoT and AI will accelerate adoption and growth of digital economies. AIoT digital 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 short period of time.

The convergence of AI with IoT 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, and use cases:

- **Smart Cities:** Implement AI-powered analytics on IoT sensor data to optimize traffic flow, waste management, energy usage, and public safety in urban environments.
- **Industrial Automation:** Use AI to analyze data from IoT sensors in manufacturing processes, to optimize production, quality control, and resource utilization.
- **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.
- **Predictive Maintenance:** Use AI algorithms to analyze IoT data from industrial machinery and equipment to predict maintenance needs, reducing downtime and improving operational efficiency.

[149] Figure credit: Tom Katsioulas, used with permission.

[150] Shirley Lu and George Serafeim, "How AI Will Accelerate the Circular Economy" from *Harvard Business Review* (June 12, 2023) available at https://hbr.org/2023/06/how-ai-will-accelerate-the-circular-economy

[151] Pratibha Kumari, "The Transformative Power of Data, AI, and IoT: Shaping the World's Future" available at https://www.linkedin.com/pulse/transformative-power-data-ai-iot-shaping-worlds-future-jha/

- **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. Use AI algorithms to optimize irrigation, planting, harvesting, and 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 supply and demand forecasting, predictive analytics and better supply chain visibility leading to competitive advantage.

Sustainability can be enhanced with AIoT.

Emerging trends in digital platforms include sustainability, connected manufacturing, creator economies, and new regulations:[152]

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.
2. **Growth of Circular IoT + AI Platforms**: Digital platforms can 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), and logistics.
3. **Platform Regulations:** Platforms face new regulatory oversight that varies among geographic regions. For example, the EU Digital Services Act requires transparency and holds platforms liable for violating terms of service. Some harmonization is needed globally especially handling fake data used by AI.
4. **Connected IoT + AI Manufacturing:** Manufacturing is adopting digital technologies with platform-based solutions leveraging data for smarter factory operations, optimized

The explosive growth of AIoT requires monitoring and management to ensure proper outcomes.

While the benefits from the convergence of AI with IoT are enormous and significant, the potential and risks for intentional and unintentional harm are also significant. The unpresented growth of data projected to exceed 570 Zettabytes[153] in less than 10 years will require the U.S. and E.U. to coordinate on a unified data strategy for IoT and AI where E.U. is making progress.[154]

AI is IoT's killer app.[155] Three key trends driving IoT applications must be monitored and managed as they evolve rapidly: AI enhancing IoT solutions and devices, off-the-shelf IoT platforms simplifying development and deployment, and IoT companies shifting from a focus on connectivity to delivering business-centric applications that optimize operations and generate valuable insights.

For example, the convergence of AI and IoT can enhance sustainability by enabling circular supply chains that track product use, analyze materials to reduce waste, and increase recycled material usage to lower carbon emissions. Trusted digital twins and AI need reliable data from trustworthy devices, which depend on secure hardware and software (hardware bills of materials, or HBOM, and software bills of materials, or SBOM). Ensuring trust involves reliable design and manufacturing of physical assets.

Digital platforms connecting smart connected suppliers, customers, and third-party solution providers, are a key component of the IoT-enabled economy. However, many developers and rogue actors can connect remotely to these same AIoT platforms. As an example, while the convergence of generative AI with IoT is still growing, the number of generative AI users and developers is exploding. ChatGPT quickly reached 100M users, surpassing Twitter, and Facebook, and 2M developers are creating numerous APIs and apps.[156] Monitoring, managing, and regulating these ecosystems is crucial to mitigating risks and driving growth.

[152] Beth Stackpole, "5 trends for 2024 from the MIT Platform report" from MIT Sloan school of Management (November 2, 2023) available at https://mitsloan.mit.edu/ideas-made-to-matter/5-trends-mit-platform-report

[153] Steven Balnojan, "The Future of Good Data – What You Should Know Now!" from *Medium* (October 7, 2020) available at https://towardsdatascience.com/the-future-of-good-data-what-you-should-know-now-f2a312a0e469

[154] European Commission, "European Approach to Artificial Intelligence" available at https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[155] Bill Curtis, "AI is IoT's Killer App" from *Forbes* (August 19, 2024) available at https://www.forbes.com/sites/moorinsights/2024/08/19/ai-is-iots-killer-app/

[156] David F. Carr, "ChatGPT Tops 25 Million Daily Visits" from Similarweb (February 3, 2023) available at https://www.similarweb.com/blog/insights/ai-news/chatgpt-25-million/

Finding 16: 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 can benefit people, communities, businesses, and organizations, these benefits are not equally shared. Some communities may experience more harm than others. Ensuring equity in access, opportunities, benefits, and outcomes is crucial for the sustainable integration of IoT. Policymakers, regulators, and financiers must consider equity when promoting IoT adoption. Likewise, IoT builders, developers, and operators should prioritize equity to create relevant, effective, and sustainable products and services.

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 unique challenges, such as being "medical deserts" with inadequate access to medical services. About thirty million Americans live over an hour away from a hospital with trauma care. IoT-enabled telehealth can significantly improve healthcare access in these areas, especially for chronic health conditions. However, rural regions often lack the necessary connectivity infrastructure, workforce, and resources to support IoT operations. The shortage of local expertise and trained personnel hampers the development, integration, and maintenance of IoT, limiting the potential benefits for rural economies.

Equitable opportunities for small cities and communities. Small cities and communities often lack the capital, resources, and capabilities of larger cities. While IoT and other innovations can help them "do more with less," they are often less aware of these technologies and lack the budget, funding access, and in-house expertise to implement them. Additionally, the absence of innovation programs and funding sources further prevents these smaller communities from accessing the same benefits as larger cities.

Equitable outcomes from data. IoT devices collect substantial amounts of data to make decisions and drive actions, but this can lead to negative outcomes. For example, facial recognition technology has a higher error rate for people of color, resulting in more negative impacts for this group. Similarly, vehicle telematics data can lead to personalized insurance premiums, benefiting good drivers but making it hard for bad drivers to get insurance. Equity considerations and protections are essential to ensure data usage creates beneficial outcomes for everyone.

Equitable access to IoT for small businesses. Small businesses are vital to American commerce and could benefit from IoT integration, but they often lack the staff, expertise, resources, and funds to do so. For example, small farms prefer investing in tangible inputs like seeds and fertilizer over uncertain IoT outcomes. Similarly, small retail businesses prioritize inventory investment for immediate profits. These financial constraints and practical priorities trap small businesses in a cycle that hinders their ability to adopt and benefit from IoT technologies.

Equitable access to opportunities for small business and start-up IoT innovators. Start-ups and SMBs drive many disruptive innovations that benefit the economy and society. However, they often struggle to bring these innovations to market. Many businesses and government agencies are unaware of these innovations and lack the funds, policies, and processes to evaluate them. Innovations frequently face a "valley of death" between pilot success and securing contracts. Procurement policies favor established products and companies, creating barriers that small businesses and start-ups cannot easily overcome, causing many innovative offerings to fail despite their potential.

Equitable access to workforce development and employment opportunities. The integration of IoT into the economy creates new jobs requiring both new and existing skills, such as digital integration, programming, cloud development, cybersecurity, and data science. Additionally, jobs will be needed to manufacture, install, service, and maintain IoT devices. However, these opportunities may bypass socioeconomically challenged and rural communities due to lack of language proficiency, digital literacy, education, and broadband access. Current labor shortages and unequal access to these new jobs hinder the full realization of IoT's economic and societal benefits.

Finding 17: Small businesses can reap significant benefits from the use of IoT, but significant barriers hinder their adoption.

IoT offers significant benefits for both small and large businesses. Small businesses, lacking the resources of larger counterparts, can see immediate impacts from IoT adoption. For example, soil moisture sensors help farmers direct irrigation efficiently, saving costs that can be redirected elsewhere. In manufacturing, IoT

sensors monitor equipment performance, optimizing production, reducing scrap, and minimizing downtime. This helps small factories meet customer commitments, expand their business, increase profits, and manage cash flow more effectively. Several barriers hinder the adoption of IoT by small businesses. These include:

- **Financial Constraints.** 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.
- **Inadequate 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 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 competition for the same talent.
- **Lack of Infrastructure.** Small businesses often lack the infrastructure to support the integration, operation, and scaling of IoT. Existing infrastructure and legacy systems 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.
- **Cybersecurity and privacy concerns:** SMBs often lack the resources and expertise to implement robust security measures, making them vulnerable to cyberattacks. They are also worried about how their proprietary data, crucial for competitive advantage, is used and shared. Navigating complex regulations and ensuring compliance with data protection laws adds to their challenges.
- **Limited Awareness:** Many small businesses have little to no understanding of IoT solutions due to limited time, budget, and exposure to industry trends. Marketing efforts of IoT providers often target larger enterprises, leaving small businesses unaware of beneficial solutions. Finding relevant case studies or success stories is also challenging for them.
- **Adoption resistance:** Small businesses prioritize immediate operational needs over new technologies. IoT is often seen as complex, leading to hesitancy among those not well-versed in IT. Owners may be overwhelmed by the technicalities and uncertain about the ROI, with misperceptions about the costs further discouraging exploration and investment.

Finding 18: Small companies and startups are instrumental in developing many innovative and disruptive technology solutions and services but face a variety of barriers in getting market 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:** IoT start-ups and small businesses struggle to secure funding needed for research and development (R&D). Investors are hesitant with emerging technologies, and customers rarely have budgets for pilot projects. Unlike larger companies, small firms cannot afford to fund development projects or offer free pilots, leading many to fail in the "Valley of Death"[157] phase between pilot success and contracting.
- **Customer Procurement Processes:** Government and enterprise procurement policies favor established products from mature companies, not risky, innovative offerings from start-ups. Larger solution provider companies can offer discounts or free proof of concept to mitigate potential risks incurred by buyers, but small solution provider businesses lack the financial means to do the same.
- **Legacy Regulations and Standards:** Industries like energy, healthcare, and transportation follow outdated regulations that conflict with innovative IoT solutions. For instance, FAA regulations restrict the use of autonomous drones in farming by requiring one drone per operator and line-of-sight operation.
- **Market Incumbents:** Start-ups face competition from established incumbents who hinder market adoption of innovative solutions by limiting access to infrastructure and creating "walled garden" ecosystems. Some incumbents even encrypt data traffic to block access by other devices.
- **Low Market Awareness:** Novel IoT technologies have limited market awareness. Start-ups spend significant resources to educate their target market and establish credibility, which is often lower than that of established companies. Government adoption of IoT solutions can help boost credibility for these start-ups.

[157] Valley of Death refers to the time period where a company has successfully developed and tested a commercial product and the securing of a commercial contract. In some cases, especially in selling to government agencies, a commercial contract award may take years.

Industry Specific Findings

Finding 19: IoT brings significant value to agriculture, but adoption is slow.

Agriculture is transforming with the integration of IoT, data analytics, automation, and robotics, boosting productivity, efficiency, and competitiveness while adapting to climate changes. IoT sensors on tractors, drones, and in soil collect data on moisture, nutrients, and crop health. IoT irrigation systems monitor weather and soil conditions, while wearable devices track livestock health and behavior. Field sensors continuously monitor environmental conditions, providing data for predictive analytics.

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.
- **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 and animal and crop health in real-time, along with 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.

IoT in agriculture and forestry suffers from a variety of challenges. The top barriers include:[158]

- **Connectivity:** Agricultural and forestry producers face three connectivity challenges: limited broadband in rural areas, inadequate broadband bandwidth for precision agriculture applications, and the need to provide "last acre" wireless connectivity to farms. While the FCC has updated the broadband benchmark definition to be 100/20 Mbps (download/upload) service, this asymmetric level of performance is insufficient for precision agriculture needs which send vast amounts of data (e.g., drone imagery data). Similarly, in densely forested areas and large farms, the lack of wireless connectivity service throughout the land poses a significant barrier to connecting and uploading and downloading data and applications necessary for in-field work. The high cost of satellite imagery data restricts the ability to proactively monitor changes in leaf area index.[159] Weather stations, which are crucial for collecting accurate environmental data, are often not set up in forests due to the prohibitive costs of satellite connectivity service involved.
- **Digital Skills:** As agriculture integrates digital technologies, workers need new skills in data analytics, precision agriculture, robotics, and systems integration, shifting from low-skill physical work to higher-skill digital tasks. Many farmers and agricultural workers may not have access to the education and training needed to develop the digital skills required for modern agriculture. For example, the U.S. faces a significant gap in apprentice and General Educational Development (GED) programs tailored for the forestry and timberland industry. These programs are crucial for recruiting talent adept at using IoT devices integrated into various machinery and trucks.
- **Lack of funding.** Some farmers and agricultural workers, especially small sized farms may not have the financial resources to invest in training and new technology. Small farms have shown a lower level of technology adoption compared to medium and large farms, pointing towards a lack of skills and resources to effectively deploy agricultural technology.
- **Interoperability:** Farms use a mix of modern and legacy equipment, creating interoperability issues. Older equipment often lacks connectivity and may be incompatible with newer machines, hindering IoT adoption. Furthermore, equipment from one brand is not compatible with other brands, limited interoperability, and exchange of data.
- **Adoption Resistance:** IoT and precision agriculture adoption is slow, especially among small farms due to limited broadband, "right to repair" concerns, trust in personal expertise, and past negative technology experiences. Large

[158] 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

[159] The Leaf Area Index (LAI) is defined as the one-sided green leaf area per unit ground area in broadleaf canopies. More information is available from https://modis-land.gsfc.nasa.gov/lai.html

producers are more likely to adopt these technologies due to better education and economies of scale.

- **Coordination:** Lack of a cohesive national research and coalition group is hindering the industry's progress in adopting IoT technologies. Business margins are narrow, making cost-sharing initiatives vital. While companies have equipped their machinery with IoT devices to monitor greenhouse gas emissions, many contractors lack the training to utilize these advanced features.

  As a result, these devices are often turned off, and the workforce continues their work using traditional methods.

Finding 20: The development of smart communities in the U.S. is limited, uneven and slow to develop.

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

Examples of IoT-enabled smart community applications in use today include:

- Smart streetlights employ LED bulbs, connected sensors and a controller to dim and brighten the streetlamps as needed. Smart streetlights also determine if the lamp has malfunctioned and notify 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 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 such as communities directly adjacent to freeways or industrial plants.
- Intelligent traffic management systems help manage the flow of traffic, minimize congestion, and decrease accidents and injuries. 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.

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

- **Awareness and Vision.** Many community and political leaders lack awareness of IoT and smart community 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, require significant investment. While larger cities may have the capabilities and some funding vehicles to support these projects, America's small and medium size cities do have 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 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 community. Political leaders are re-elected if they are responsive to the needs of their constituents. Smart community initiatives that do not align with the city's strategic and near-term priorities are likely to prove challenging to implement.

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 artificial 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 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 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.

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, a slight improvement from the previous report card (2017), which rated the state of American infrastructure as D+. 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. Many of America's wastewater treatment plants were built in the 1970's and have an average life span of 40-50 years. This aging infrastructure and inadequate capacity lead to the discharge of 900 billion gallons of untreated sewage into U.S. waterways each year.

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 airgaps. 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. The utility industry averaged 736 cyberattacks per week and experienced a 46 per cent year-over-year increase in cyberattacks in 2021. 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 photovoltaic (PV) generation in California, Utah, and Wyoming. 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." 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.

Finding 21: IoT can transform outcomes in traffic management and transit but several technical, policy and funding barriers hinder adoption.

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.".[160] Back in January of 2022, the Department of Transportation (DOT) released the comprehensive National Roadway Safety Strategy, a roadmap to address the national crisis in traffic fatalities and serious injuries.[161] One of the key actions in that

[160] "NHTSA Estimates for 2022 Show Roadway Fatalities Remain Flat After Two Years of Dramatic Increases" from National Highway Traffic Safety Administration (April 20, 2023) available at https://www.nhtsa.gov/press-releases/traffic-crash-death-estimates-2022

[161] "U.S. Transportation Secretary Pete Buttigieg Announces Comprehensive National Roadway Safety Strategy" from U.S. Department of Transportation (January 27, 2022) available at https://www.transportation.gov/briefing-room/us-transportation-secretary-pete-buttigieg-announces-comprehensive-national-roadway

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. 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.

In addition to addressing traffic needs, IoT technologies can facilitate and support multimodal transit and other innovative transportation models (including ride-share, e-scooters, drones, etc.). Furthermore, they also facilitate the safe testing and operation of automated 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 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 highlight the technology's ability to improve work zone and intersection safety.[162]
- 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. [163]
- A project with an auto maker and a bicycle safety platform maker to highlight the benefits of C-V2X-powered bicycle use cases.[164]
- 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.[165]
- A project with the Florida Department of Transportation (FDOT) to test and implement connected vehicle and pedestrian/bicyclist safety applications (active or passive) at thirteen signalized intersections and eight mid–block crossings within the core of the University of Florida (UF) campus.[166]
- The New York City Department of Transportation (NYCDOT) Traffic Safety Network. a large-scale Intelligent Transportation System (ITS) upgrade, replacing their entire citywide traffic communications network with a cellular IoT system. NYCDOT'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.[167]
- 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 phases.[168]

[162] Jacob Levin, "Virginia Tech Transportation Institute researchers to deploy smart work zone in Wise, Virginia," from Virginia Polytechnic Institute and State University (May 19, 2022) available at https://vtx.vt.edu/articles/2022/05/vtt-smart-work-zone.html?utm_source=cmpgn_news&utm_medium=email&utm_campaign=vtUnirelNewsDailyPublicCMP_052022-public

[163] "Blue Bird, Fulton Co. Schools join Audi, Applied Information on connected vehicle deployment to boost school bus and school zone safety" from Audi USA (March 30, 2021) available at https://media.audiusa.com/releases/465

[164] "Audi joins Spoke Safety, Qualcomm, Commsignia to help protect bicyclists through connected technology" from Audi USA (March 15, 2022) available at https://media.audiusa.com/releases/514

[165] "Connected Vehicle Pilot Deployment Program" from the U.S. Department of Transportation available at https://www.its.dot.gov/pilots/pilots_thea.htm

[166] "Gainesville Bike and Pedestrian Safety Project" from Florida Department of Transportation available at https://teo.fdot.gov/architecture/architectures/d2/html/projects/projarch47.html

[167] "New York City DOT Deploys Digi Solutions to 14k Intersections with Digi Remote Manager" from Digi available at https://www.digi.com/resources/customer-stories/new-york-city-dot-deploys-digi-solutions

[168] "TriMet Enhances Bus Fleet Management with Digi Connectivity and Remote Management Solutions" from Digi available at https://www.digi.com/resources/customer-stories/trimet-bus-fleet-management-with-digi-connectivity

- 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.[169]

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 stakeholders 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 orderly flow of traffic as well as increased productivity (drivers spend less time stuck in traffic).[170] Other stakeholders 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 stakeholders seeking to implement these technologies. On the policy side, clarity is needed with respect to data governance and privacy and what types of data districts and municipalities 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 undeserved areas. Interoperability and fragmentation are also challenges when dealing with different areas and it is important to address cybersecurity implications of all the connected devices that can be used as a gateway. 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 22: 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.

For disease prevention and early detection to diagnosis, treatment, and prognosis evaluation to become the norm for all patients, IoMT devices, high-performance computing genomics, and personalized data will help genomic and clinical concepts to co-exist. Examples of such systems include:

- **Wearable on-body devices,** including consumer health devices (fitness watches, sleep trackers), and clinical-grade devices (regulated by health agencies, and prescribed by healthcare professionals).
- **In-home devices supporting telemedicine** applications such as remote patient monitoring, and emergency response.
- **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, and others.
- **In-clinic IoMT systems** that support administrative functions that allow medical workers to help patients remotely, track hospital assets and equipment, and others.

Some other examples of top IoMT applications include:

- **Remote patient monitoring.** This is an essential IoT application in healthcare, enabling continuous tracking of patients outside traditional settings. Wearable devices monitor vital signs, medication adherence, and other

[169] "Digi Helps Septa Comply with Federal Mandate for Positive Train Control (PTC)" from Digi available at https://www.digi.com/resources/customer-stories/digi-helps-septa-comply-with-federal-mandate

[170] See Carnegie Mellon Study for an example: Ken Walters, "Smart Signals: Pilot Study on Traffic Lights Reduces Pollution, Traffic Clogs" (October 16, 2012) available at https://www.cmu.edu/piper/news/archives/2012/october/smart-signals.html

health metrics, allowing healthcare providers to offer timely interventions and reduce hospital visits. This is especially beneficial for individuals with chronic conditions, as it helps manage their health remotely, reduces hospital readmissions, and improves overall patient well-being. In addition, this improves access to healthcare services, especially for those living in rural areas.

- **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.
- **Increased Access to Healthcare Services.** The ability for IoT to monitor patients remotely provides patients living in rural and remote areas, where medical facilities are limited and often far away, with improved access to services. In addition, it provides services to those patients who have limited transportation options, as well as those who are homebound.

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 serious concerns about data security and patient privacy. Ensuring robust cybersecurity measures and compliance with privacy regulations is crucial. This is exacerbated by the number and continued use of legacy medical devices, with limited cybersecurity measures, in healthcare organizations.
- **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.
- **Edge AI Technologies.** Advancements in sensory, motor, and control networks link neurons to train and operate models at the edge. Edge AI frameworks identify resources for biomedical genomic research and drive better healthcare outcomes for patients using a variety of machine learning algorithms. The ability for device technologies and AI to learn, remember, and adapt in ways like our human brains will reduce the large computational power needs and training of large data sets to address the Internet connectivity and adaptive learning challenges AI brings to enable greater IoT adoption.

IoMT 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 23: 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 devices monitor environmental conditions, optimize resource usage, 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 data informs communities about the safety of outdoor activities like exercise. City and health officials may use the data to identify areas of poor air quality, and to devise programs to mitigate its effects or reduce sources of emissions (such as planting trees, restricting traffic at certain hours, banning idling cars at certain hours, providing residents with respiratory healthcare information, etc.).
- **Optimize water use.** Soil moisture sensors in farming integrated with automatic irrigation systems, measure moisture levels and activate the irrigation systems only in those spots where the water is needed. This saves water and costs. IoT monitoring can also detect leaks and other issues in water transport.
- **Reduce carbon emissions.** IoT can measure, collect, and compile data regarding manufacturing, transportation, agriculture production, and end-of-life practices associated with upstream and downstream supply chains. This data can be used to calculate the scope 3 emissions[171] associated with a product or process. Greater transparency for scope 3 emission can enable the implementation of effective mitigation strategies and contribute to national and global efforts to reduce carbon dioxide (or equivalent) emissions.
- **Reduce energy use.** Automated demand response systems, connected to building automation and energy management systems, automatically reduce energy use while minimizing impact on building occupants. Examples of energy use reduction include room occupancy sensors turning off lights in empty rooms and smart thermostats autonomously managing ambient temperatures by learning the behavior patterns of 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 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, minimize waste, and enhancing efficiency.
- **Agile and proactive response.** Real-time monitoring of environmental conditions, such as water contamination and air quality levels, allows the community to plan for and respond to changes swiftly. This enhances the effectiveness of the response and minimizes resource needs and the extent of the adverse impacts.
- **Informed and data-driven decision making.** IoT device collected data informs 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 several challenges. These include:

- **Data accuracy.** Environmental sensors vary widely in quality, from low-cost consumer-grade to expensive

[171] For a definition of scope 3 emissions, see https://www.epa.gov/climateleadership/scope-3-inventory-guidance

regulatory-grade units. Despite measuring the same things, these sensors have different accuracy levels, calibration issues, drift, or reliability due to the underlying sensing technologies used.

- **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 in areas with no infrastructure. These remote areas have limited to no connectivity which hinders IoT deployment.
- **High initial implementation costs.** The upfront 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.
- **Data management.** Environmental monitoring sensors collect a large volume of data over time. This can be exacerbated by increased collection such as might be done by sensors monitoring rising river water levels during a storm. Managing this data is complex and challenging. This is complicated when combining sensor data from distinct types of sensors. Sensors can 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 interoperability hinders seamless integration and data exchange among different IoT platforms and devices, limiting the holistic view required for comprehensive environmental monitoring. The lack of standardized communication protocols leads to increased complexity in managing and maintaining these systems and hinders the ability of environmental monitoring networks to expand and scale. The challenge is further exacerbated 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 which can enable more accurate and comprehensive assessments of environmental conditions.

Finding 24: 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 improve 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 can be 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 before any 911 call is placed. Smart cameras detect and report suspicious behaviors, such as unattended luggage or packages, trespassing into secure areas, fighting, display of a gun and other illegal activities. These smart applications enable accurate monitoring and reviewing of thousands of cameras 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 disaster areas to provide responders with a fast assessment of the scene to inform deployment of resources. 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. 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 focusing 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 consider responder exertion and stress levels. Body cameras on police provide a record of how officers respond to activities, document actions, and hold officers accountable.

- **Connected patient monitoring**. Emergency response vehicles equipped with IoT devices monitor the health of the patients being treated at accident or disaster scenes, as well as those critically injured transported by ambulances. This 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 and enable treatment to start immediately upon arrival at 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 staff 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,[172] 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 several challenges, including:

- **Cybersecurity Concerns.** The use of connected devices leads to increased cybersecurity vulnerabilities and risks. Cybercriminals exploit vulnerable devices to gain unauthorized access to the systems used by law enforcement and other public agencies. This could lead to the exposure of sensitive information, and the 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 their 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 and be reliable for use under harsh 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 costs limit agencies as 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.

[172] "Air pollution linked with higher COVID-19 death rates" from Harvard T.H. Chan School of Public Health available at https://www.hsph.harvard.edu/news/hsph-in-the-news/air-pollution-linked-with-higher-covid-19-death-rates/

Finding 25: IoT can be a key technology enabler for end-to-end supply chain visibility currently hindered by the disconnected nature of supply chains.

The COVID-19 pandemic highlighted the importance of supply chain resilience, prompting reshoring and diversification to mitigate risks. Geopolitical tensions and trade restrictions have underscored the need for resilient supply chains to ensure market preference and regulatory compliance.

IoT plays a vital role in supporting supply chain operations.

Connected IoT sensors provide real time location information, allowing goods and freight to be tracked and traced as it moves from location to location. In addition to location information, IoT sensors can monitor the conditions of the goods, assets, and freight being transported. For example, sensors can monitor the temperature of pharmaceuticals and produce, to ensure that they are within the required environmental conditions during transportation.

While IoT can track the movement of goods, its effectiveness in supporting end-to-end supply chain visibility is hindered today due to some structural reasons.

Despite the potential to track freight with IoT technologies, end-to-end supply chain visibility, a basic capability for a resilient supply chain, is still not possible today. There remains a critical need for cross-domain visibility and transparency to bolster supply chain resilience. Reasons for this include:

- **Decentralized Systems**: The Brookings Institute highlights that U.S. supply chains are decentralized, each with its own goals and visibility. Coordinating multiple supply chains with diverse logistics infrastructure is challenging due to issues with data quality, availability, interoperability, and immediacy.
- **Intermediary Network:** Between shippers and customers lies a network of logistics service providers, carriers, warehouse operators, and terminal operators worldwide. Freight is moved from one party to another in the supply chain. Harmonizing their IT systems, standards, and knowledge levels requires significant organizational effort.
- **Lack of data sharing between supply chain participants.** Data sharing across supply chains and firms is rare. This is attributed to many factors, including data interoperability, the many intermediaries in the supply chain who "touched" the freight, and reluctance to "share information that could help the competition". The latter is particularly prevalent in an industry where margins are low, and pricing is the basis of competition.
- **Lack of Interoperability:** The flow of supply chain information is hindered by a lack of interoperability among systems, technologies, and software used across the supply chain network. This results in inefficiencies, increased costs, delays, and limited real-time visibility and traceability.
- **Standards Issues:** Interoperability issues stem partly from the lack of universally adopted standards. Different transport modes, like ocean and truck or air and truck, each use their own set of standards, complicating coordination.
- **Legacy Systems:** Another issue is the use of legacy systems by various supply chain participants, including manufacturers, shipping companies, carriers, and customs agencies. These systems often lack IoT capabilities and use outdated communication protocols, further hindering interoperability.
- **Challenges in Multimodal Supply Chain Visibility.** Consider the scenario of a product journeying through a multimodal supply chain—from manufacturing to distribution, crossing borders and involving multiple parties. At each stage, the lack of standardized protocols and information silos among shippers, freight forwarders, and other stakeholders hinder end-to-end visibility. The absence of seamless communication and data sharing exacerbates the challenge of tracking goods across disparate supply chain domains. One current example of an efficient IoT enabled multimodal supply chain has been documented.[173]

New approach is needed to create end-to-end supply chain visibility with IoT.

Three things are needed to facilitate end-to-end supply chain visibility. These are IoT to monitor and track the location and state of freight and goods along the supply chain, global business identifiers that uniquely identify a product or good that is recognized by parties within the supply chain, and the sharing of information between all the participants in the supply chain.

Some of these are currently in play:

- **Data Sharing. Freight Logistics Optimization Works (FLOW) Program Overview:** The White House FLOW pilot program[174] aims to boost supply chain resilience by enhancing data transparency and collaboration among

[173] "An Insight into Amazon Supply Chain Strategy" from DFreight (April 27, 2023) available at https://dfreight.org/blog/an-insight-into-amazon-supply-chain-strategy/

[174] "Freight Logistics Optimization Works" from the U.S. Department of Transportation available at https://www.bts.gov/flow

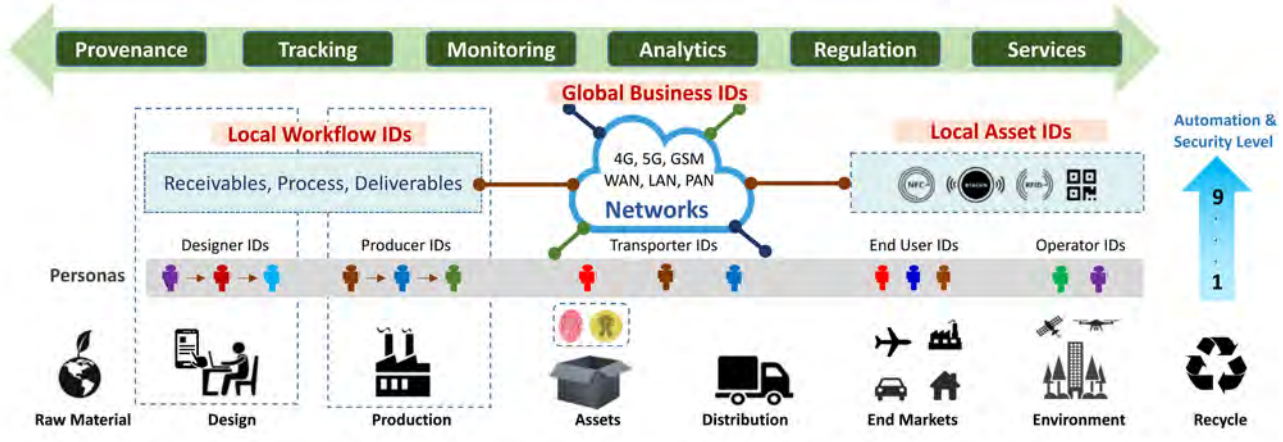


Figure 19. Leveraging IoT Technologies and Digital Identifiers for Supply Chain Resilience[176]

supply chain stakeholders. FLOW is an information sharing initiative to pilot key freight information exchange among parts of the goods movement supply chain to help speed up delivery times and reduce consumer costs.[175] Unlike Amazon's integrated model, FLOW focuses on sharing freight data across supply chains involving government agencies, private firms, and industry partners.

Benefits of Supply Chain Data Sharing: This data sharing can promote proactive responses to disruptions and enhance market efficiency. For example, transparent data on agricultural shipments can help anticipate and manage disruptions, stabilizing food prices, and ensuring food security. FLOW's decentralized approach relies on cooperation among stakeholders, but it faces barriers in standardization, data sharing, and decision-making.

- **Global digital identifiers.** Identifiers enable trusted traceability of businesses, products, workflows, and data across borders, facilitating market preference by monitoring imports of essential goods and distribution of key technologies. By linking Global Identifiers to Local Identifiers, which carry metadata about businesses, assets, and data cryptographically linked to a root of trust, supply chain visibility, trust and traceability can be enhanced. As traceability methods improve over time the sharing of data related to product lifecycle and field use will foster trusted digital marketplaces and fuel digital economies.

Achieving end-to-end supply chain visibility is challenging and requires a variety of initiatives. However, one current "quick win" opportunity exists to integrate IoT, global business identifiers and the data sharing enabled by FLOW to create end-to-end supply chain visibility.

The FLOW pilot addresses a specific challenge in the supply chain, including data sharing and collaboration. There is an opportunity for IoT to leverage this program's future data sharing capability to provide cross-border end-to-end visibility by using Global Business Identifiers, which can enhance the tracking and management of goods across disconnected supply chains. Global Identifiers can cryptographically link to Local Identifiers of businesses, products, and data leveraging existing standards and infrastructure. The Department of Homeland Security (DHS) Customs and Border Protection has initiated pilot programs on Global Business Identifiers[177] for a variety of physical goods including pharmaceuticals, electronics, and chips.

Finding 26: The use of IoT can transform industrial operations, but adoption is limited, and challenges need to be addressed.

IoT technologies are used in industrial operations that are heavily monitored and controlled. Examples can be found in the manufacturing, energy, mining, chemicals, and transportation industries. The operations being monitored and controlled include processes in product handling, production, distribution, and supply chain management.

This monitoring and control are performed by Industrial Control Systems, (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and programmable logic controllers (PLC) that incorporate IoT technologies. These technologies are often commonly referred to as 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

[175] Lori Ann LaRocco, "How Walmart, Target, and the White House are tracking consumer demand and inflation in real time" from CNBC (March 20, 2024) available at https://www.cnbc.com/2024/03/20/biden-administration-is-expanding-its-real-time-supply-chain-tracker.html

[176] Figure credit: Tom Katsioulas, used with permission.

[177] "CBP Launches Global Business Identifier Pilot to Increase Supply Chain Visibility" from U.S. Customs and Border Patrol (December 2, 2022) available at https://www.cbp.gov/newsroom/national-media-release/cbp-launches-global-business-identifier-pilot-increase-supply-chain

industrial equipment.[178] These systems have traditionally been proprietary, not connected to the Internet, and operate independently of the Information Technology (IT) network. In contrast, IoT-based systems are interoperable, scalable and connect to other systems and applications through the IT network and the Internet.

IoT offers several advantages over legacy OT and industrial control systems. These include:

- Supports heterogeneous devices. A variety of disparate devices, as well as those from different brands and suppliers, can be integrated into IoT networks to support operations. Legacy devices are based on proprietary protocols and do not work with systems from another supplier.
- Multiple connectivity methods. Devices based on IoT technologies can support multiple connectivity methods by changing communication modules. For example, IoT devices can communicate through WiFi, cellular (4G/5G), LoRaWAN, NB-IoT, Cat-M, and other methods. In contrast, many legacy devices employ proprietary communication protocols.
- Scalability. IoT devices connect to edge and cloud-based servers. As more data is collected and processed, additional computing and storage resources can be dynamically added to support growing needs and scaling to large numbers of devices now and in the future.
- Open standards and interoperability. IoT systems comply with a variety of open and industry standards, from connectivity, to messaging protocols, and cybersecurity and platforms. Devices based on these standards can integrate into a variety of IoT platforms.
- Integration with business and corporate IT systems. While legacy and non-IoT devices can only connect with proprietary and vendor systems, IoT systems do not have that restriction and can be integrated with various business and operational systems through the IT network.
- Data sharing. Cloud and edge IoT platforms can integrate data from a variety of devices, as well as data from external sources. These data sets are integrated in the IoT platforms and can be combined and analyzed to yield deep insights.
- Cybersecurity. Because legacy and industrial control systems typically run on proprietary and air-gapped networks, they were not built with modern cybersecurity practices in mind. IoT devices and systems, built to operate on IT networks and connect to the Internet, incorporate cybersecurity practices and protections.

Despite their connected nature, OT and industrial IoT devices are different from their 'consumer IoT' counterparts. Industrial IoT devices integrate into industrial control systems and legacy systems. They operate in harsh environments and have high reliability and performance standards that consumer products are not subject to.

The integration of IoT devices, which connect to the Internet, creates a convergence of OT with IT functions and systems. This convergence offers many advantages and benefits, but also creates several significant challenges.

There are numerous benefits from the use of IoT in an industrial context, including:

- Increased efficiency, productivity and quality in manufacturing operations, and associated cost reduction
- Facilitation and support of autonomous operations.
- Reduction of errors.
- Prevention of unplanned shutdowns through Predictive maintenance.
- Improved Worker and Equipment Safety.
- Data-driven insights that support reporting and compliance.

Adoption and improvement of industrial IoT also brings challenges that should be addressed, including:

- The need to ensure **interoperability** with existing substantial legacy and OT systems representing billions of dollars of prior investment.
- **Reliability** for IoT technologies operating in conjunction with or monitoring industrial devices including those vital to the operation of critical infrastructure that must often operate reliably and continuously in harsh environments.
- **Protection** of individual privacy-related information and confidential organizational information including 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.
- Considerations regarding **scalability**, as industrial systems with IoT technologies often involve a large number of devices representing years of investment and multiple generations of technology.

[178] "operational technology" from NIST Computer Security Resource Center Glossary available at https://csrc.nist.gov/glossary/term/operational_technology

- Introducing Internet connectivity to industrial OT systems that were formerly "air gapped" creates **larger attack surfaces** that must be protected from cyber threats such as hacking, malware, and ransomware; and,
- In many industrial organizations, **IT and OT systems are siloed** operations maintained by different teams that do not interact with each other, have different skill requirements, and come from different organizational cultures. The convergence of IT and OT requires that these silos be integrated, and digital skills be acquired.
- Many companies struggle to build the **digital skills** needed necessary to operate and maintain the connected equipment needed for industrial operations.

The advancement of IoT and adjacent 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.



Photo credit: Shutterstock

Recommendations of the IoT Advisory Board

As the IoTAB examined these subjects in depth, several topics and, eventually, themes surfaced repeatedly across the IoT landscape. The IoTAB's recommendations are organized around six major themes. These themes (depicted in Figure 20) represent fundamental elements to facilitate, accelerate, and sustain the adoption and integration of IoT into the American economy and society. These themes are:

1. Government Leadership
2. Modernizing IoT Infrastructure
3. Establishing Trust in IoT
4. Fostering a IoT-ready Workforce
5. Facilitating Industry Adoption of IoT
6. Unlocking an IoT-Enabled Economy

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

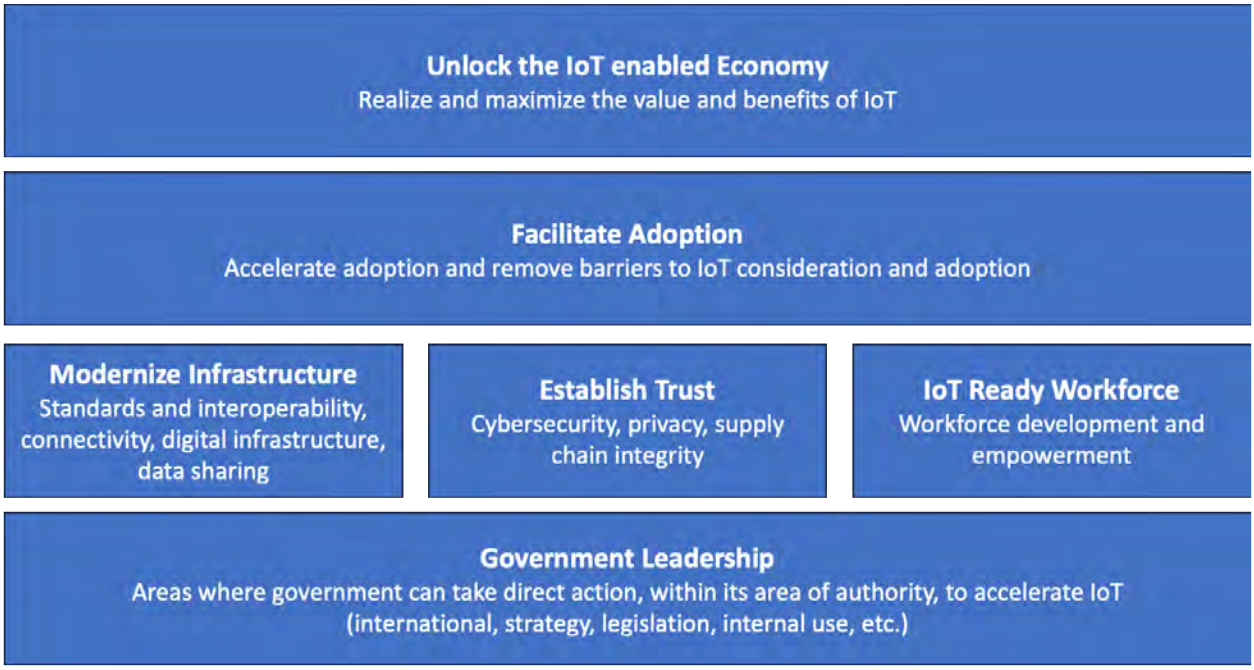


Figure 20. Themes Used for the IoTAB Recommendations[179]

[179] Figure credit: Benson Chan, used with permission.

The IoTAB recommends that the IoTFWG consider (and, where appropriate, act to implement or document the existing implementation of) the findings and recommendations in this report. The table below provides a high-level description of each recommendation; the sections following contain more detail about the specific Key and Enabling Recommendations of the IoTAB.

RECOMMENDATION	DESCRIPTION
Government Leadership	
Key Rec. KR1.1	Congress and the Executive Branch should work together to establish a United States national strategy for taking full advantage of the opportunity presented by the IoT.
Enabling Rec. ER1.1.1	Congress and the White House should further improve and elevate interagency coordination including an IoT National Coordination Office and appoint a full time Chief Technology Officer.
Enabling Rec. ER1.1.2	The White House should include IoT in the federal Critical and Emerging Technology (CET) List.
Enabling Rec. ER1.1.3	Congress should study the impact of IoT components and modules produced by Chinese companies and other foreign adversaries to assess, understand, and mitigate the risks to cybersecurity, the IoT supply chain, and economic and national security.
Enabling Rec. ER1.1.4	Congress and the Executive Branch should establish a CEO-level ongoing advisory board to advise the federal government on matters pertaining to IoT.
Enabling Rec. ER1.1.5	The Executive Branch should integrate IoT considerations into the development of the national AI strategy and strategic AI initiatives.
Key Rec. KR1.2	Congress should accelerate IoT technology innovation to support an evolving IoT.
Enabling Rec. ER1.2.1	Congress should fully fund existing IoT research, development, deployment, and demonstrations.
Enabling Rec. ER1.2.2	Congress should facilitate and accelerate adoption of IoT technologies by small businesses.
Enabling Rec. ER1.2.3	The Executive Branch should accelerate the adoption of IoT technologies developed and manufactured by small business and startup organizations.
Enabling Rec. ER1.2.4	Congress and the Executive Branch should specify and use innovative IoT technologies and applications in federally funded projects.
Enabling Rec. ER1.2.5	Congress should continue to support and fund technology research, through industry, university, and national labs, to further advance and accelerate the development of IoT technologies and its enabling infrastructure.
Key Rec. KR1.3	The Executive Branch should promote international collaboration in IoT adoption to share knowledge, best practices, and resources; harmonize standards, policies, and regulations; and facilitate trade.
Enabling Rec. ER1.3.1	The Executive Branch should create internationally compatible data minimization guidance related to IoT devices, aligning with the NIST Privacy Framework and NIST Cybersecurity Framework principles.
Key Rec. KR1.4	The Executive Branch should lead by example by specifying, procuring, and adopting IoT by federal agencies for its internal use.
Enabling Rec. ER1.4.1	The Executive Branch should lead the way in facilitating IoT adoption by adopting and promoting IoT technologies and systems for its own internal operations and needs.
Enabling Rec. ER1.4.2	Congress and the Executive Branch should upgrade legacy federally owned or operated IoT infrastructure that is integrated into government facilities, assets, and operations.
Modernizing IoT Infrastructure	
Key Rec. KR2.1	The Executive Branch should promote collaborative development across industries to adopt existing industry standards and protocols that enable IoT interoperability.
Enabling Rec. ER2.1.1	The Executive Branch should advocate and facilitate standards development and adoption that leads to interoperability for public safety IoT.
Enabling Rec. ER2.1.2	The Executive Branch should advocate and facilitate standards development and adoption that leads to interoperability for medical devices.
Enabling Rec. ER2.1.3	The Executive Branch should promote the development and use of standards for supply chain logistics, traceability, and assurance.
Enabling Rec. ER2.1.4	The Executive Branch should promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across IoT systems and devices.
Key Rec. KR2.2	The Executive Branch should establish methods to foster interoperability for IoT technology to the greatest extent possible, through the use of consistent models, protocols, application interfaces, and schemas.

RECOMMENDATION *continued*	DESCRIPTION
Enabling Rec. ER2.2.1	The Executive Branch should facilitate interoperability through the development of a consistent data taxonomy for the sharing and exchange of transportation, traffic and other data collected from IoT and non-IoT sources.
Enabling Rec. ER2.2.2	The Executive Branch should promote and adopt industry-led standards, guidelines, and protocols for IoT technologies to the greatest extent possible.
Key Rec. KR2.3	The Executive Branch should expand and improve programs that ensure sufficient availability, reliability, quality of service and connectivity to support IoT in all areas of the country.
Enabling Rec. ER2.3.1	The Executive Branch should promote continued U.S. leadership on spectrum policy by continuing to make licensed and unlicensed spectrum available via spectrum sharing, repurposing underutilized federal spectrum and spectrum auctions.
Enabling Rec. ER2.3.2	Congress should increase funding and accelerate implementation of broadband deployment across rural America.
Enabling Rec. ER2.3.3	The Executive Branch should actively promote and support the adoption of satellite narrowband IoT systems to support "last acre" IoT in rural and remote areas.
Key Rec. KR2.4	The Executive Branch should encourage businesses and organizations to embark on initiatives to digitalize and transform their operations and processes in order to take advantage of IoT and the IoT-enabled economy.
Enabling Rec. ER2.4.1	The Executive Branch should facilitate the creation of IoT business ecosystems that enable new business models and revenue streams.
Enabling Rec. ER2.4.2	The Executive Branch should lead collaboration with international allies to develop, promote and adopt a Global Digital Identifier that can link to Local Identifiers of businesses, products, and data, to enable cross-border trade, supply chain resilience, and ultimately trusted digital marketplaces.
Establishing Trust in IoT	
Key Rec. KR3.1	NIST should continue to provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach.

RECOMMENDATION *continued*	DESCRIPTION
Enabling Rec. ER3.1.1	The Executive Branch 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.
Enabling Rec. ER3.1.2	The Executive Branch should consider additional ways to highlight the vulnerabilities most likely to be applicable to IoT product developers.
Enabling Rec. ER3.1.3	Congress should study the impacts of Quantum computing and post-quantum cryptography on IoT cybersecurity.
Enabling Rec. ER3.1.4	The Executive Branch should accelerate the promotion and adoption of IoT technologies to enhance the electric grid's security, reliability, and resilience.
Enabling Rec. ER3.1.5	Congress and the Executive Branch should support domestic IoT cybersecurity labeling initiatives by establishing incentives for manufacturers to participate.
Enabling Rec. ER3.1.6	Congress must ensure adequate and ongoing funding for the Cyber Trust Mark consumer education campaign.
Enabling Rec. ER3.1.7	The Executive Branch should establish appropriate U.S. representation regarding international harmonization of IoT cybersecurity programs and requirements as such programs are established for domestic market sectors.
Enabling Rec. ER3.1.8	The Executive Branch should recognize and promote existing standards and conformity assessment schemes that facilitate cybersecurity in industrial IoT applications.
Key Rec. KR3.2	Congress should pass comprehensive federal privacy legislation.
Enabling Rec. ER3.2.1	Congress should include IoT in proposed comprehensive privacy legislation.
Enabling Rec. ER3.2.2	The Executive Branch should promote "Privacy by Design" in IoT device development, deployment, and implementation.
Enabling Rec. ER3.2.3	Congress and the Executive Branch should establish clear policies for third-party data sharing and IoT device data use.
Enabling Rec. ER3.2.4	Congress and the Executive Branch should encourage the use of plain language in IoT privacy policies.
Enabling Rec. ER3.2.5	Congress and the Executive Branch should develop and implement privacy transparency mechanisms.

RECOMMENDATION *continued*	DESCRIPTION
Enabling Rec. ER3.2.6	Congress and the Executive Branch should endorse universal opt-out signals for IoT devices and companion apps.
Enabling Rec. ER3.2.7	Congress and the Executive Branch should require IoT privacy information on new car automobile "Monroney Labels".
Enabling Rec. ER3.2.8	Congress should add "Location Tracking Enabled" disclosure to future U.S. device labeling initiatives.
Enabling Rec. ER3.2.9	The Executive Branch should promote the use, development, and implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.
Enabling Rec. ER3.2.10	The Executive Branch should follow NIST sanitization standards for government automobiles before resale and encourage NIST sanitization standards for automobiles before resale.
Key Rec. KR3.3	The Executive Branch should support trusted IoT architectures and infrastructure that enable supply chain provenance, and traceability of IoT systems starting from chip design and manufacturing.
Enabling Rec. ER3.3.1	The Executive Branch should encourage trusted digital twins and digital threads for accelerating IoT adoption across supply chains and IoT application markets.
Enabling Rec. ER3.3.2	Congress and the Executive Branch should incentivize trusted multi-stakeholder alliances and collaboration networks to speed development and adoption of connected end-to-end IoT solutions.
Fostering a IoT-ready Workforce	
Key Rec. KR4.1	Congress and the Executive Branch should integrate the needs of the future IoT workforce into existing initiatives and programs with industry, academia and state and local government efforts.
Enabling Rec. ER4.1.1	The Executive Branch should review the National Cyber Workforce and Education Strategy and align and integrate any special or unique needs and considerations of the IoT workforce.
Enabling Rec. ER4.1.2	The Executive Branch should collaborate with industry, academia, and state and local government to create an IoT trained workforce embedded in target high priority industry sectors.
Enabling Rec. ER4.1.3	The Executive Branch should collaborate with industry, academia, state and local governments and private investors to create and place workforce in industries and areas of opportunity.
Enabling Rec. ER4.1.4	Congress and the Executive Branch should advocate development and implementation specialized data privacy training programs to equip the IoT workforce with the necessary skills and knowledge to protect sensitive information, ensuring compliance with current privacy regulations and standards.
Facilitating Industry Adoption of IoT	
Key Rec. KR5.1	Congress should consider new financial models for sustaining and supporting programs when evaluating IoT project feasibility in federal grants.
Enabling Rec. ER5.1.1	The Executive Branch should encourage federal grant applications to consider other financial or funding models to help adopting organizations to sustain and support IoT projects.
Enabling Rec. ER5.1.2	Congress and the Executive Branch should develop programs and grants to help underserved and less developed communities adopt IoT.
Key Rec. KR5.2	Congress and the Executive Branch should develop a comprehensive Agricultural IoT Strategy.
Enabling Rec. ER5.2.1	Congress should fund the deployment of a "farm of the future" setup in representative universities nationwide. This nationwide test-farm IoT network should span different forms of agriculture, including, but not limited to broadacre, horticulture, livestock, and aquaculture.
Enabling Rec. ER5.2.2	The Executive Branch should support and promote industry and Standards Development Organization (SDO) efforts to address interoperability of agricultural systems and machinery.
Enabling Rec. ER5.2.3	Congress and the Executive Branch should facilitate small farm/ranch adoption of IoT technologies.
Enabling Rec. ER5.2.4	Congress should support enactment of federal "right to repair" legislation to address the inability of agricultural producers to service their smart equipment.
Key Rec. KR5.3	Congress and the Executive Branch should implement specific actions to further promote IoT adoption through smart cities and communities.
Enabling Rec. ER5.3.1	The Executive Branch should facilitate and support the development and use of smart community and "IoT-related sustainable infrastructure" reference models.
Enabling Rec. ER5.3.2	Congress and the Executive Branch should develop Smart Community and Sustainability Extension Partnerships (SCSEP) to provide technical advice to cities and communities adopting IoT.

RECOMMENDATION *continued*	DESCRIPTION
Enabling Rec. ER5.3.3	The Executive Branch should facilitate opportunities for adoption of IoT and smart technologies for local communities.
Enabling Rec. ER5.3.4	The Executive Branch should facilitate smart community opportunities and IoT adoption for rural communities that have broadband infrastructure, have received broadband infrastructure funding, or have completed broadband infrastructure buildouts.
Enabling Rec. ER5.3.5	The Executive Branch should support and promote industry and SDO efforts to address interoperability of smart communities (including smart buildings, energy and utilities, traffic).
Enabling Rec. ER5.3.6	The Executive Branch should facilitate small to medium city adoption of smart community technologies.
Enabling Rec. ER5.3.7	The Executive Branch should facilitate equity in realization of smart community benefits.
Key Rec. KR5.4	The Executive Branch should promote IoT adoption that will improve public safety.
Enabling Rec. ER5.4.1	The Executive Branch should require the development and implementation of privacy and data usage policies in federally funded public safety and smart community projects that use IoT technologies.
Enabling Rec. ER5.4.2	Congress and the Executive Branch should include IoT considerations (including IoT adoption and utilization plans) in federal procurements that support public safety applications.
Enabling Rec. ER5.4.3	Congress and the Executive Branch should create a program that advises and enables local communities to purchase IoT systems or IoT-enabled systems for public safety applications.
Key Rec. KR5.5	Congress and the Executive Branch should promote IoT adoption in the health care industry.
Enabling Rec. ER5.5.1	The Executive Branch should promote the Internet of Medical Things (IoMT) as an enterprise priority, including to healthcare facilities' leadership teams.
Enabling Rec. ER5.5.2	Congress and the Executive Branch should facilitate cybersecurity in IoT in smart medical devices and equipment, including wearables, in-home devices, community IoT-related healthcare systems, and a continuum of care.
Enabling Rec. ER5.5.3	Congress and the Executive Branch should facilitate and support the use and adoption of healthcare IoT in rural communities.
Enabling Rec. ER5.5.4	Congress should facilitate the adoption of AI in IoT in healthcare through improved AI research, development, and workforce improvement.
Enabling Rec. ER5.5.5	Congress should enact HIPAA-like protection for users' medical data in mobile applications and IoT devices.
Key Rec. KR5.6	Congress and the Executive Branch should promote IoT adoption that will improve sustainability and environmental monitoring.
Enabling Rec. ER5.6.1	Congress should study the feasibility of the concept of an open repository for environmental data generated from IoT sensors.
Enabling Rec. ER5.6.2	Congress should facilitate and support the research, development, and deployment of low-cost Air Quality sensors.
Enabling Rec. ER5.6.3	Congress should implement a nationwide IoT-based Water Monitoring Infrastructure) to expand the nationwide water monitoring system, including water treatment facilities.
Enabling Rec. ER5.6.4	The Executive Branch should use IoT Technologies to facilitate carbon transparency across economic sectors.
Enabling Rec. ER5.6.5	The Executive Branch should facilitate and promote the use and integration of IoT technologies to monitor environmental conditions and hazards.
Key Rec. KR5.7	Congress and the Executive Branch should promote IoT adoption in Smart Transit and Transportation.
Enabling Rec. ER5.7.1	The Executive Branch should promote development and application of policies, procedures and funding methods that can accelerate the adoption of smart, connected, and electrified transportation technologies.
Promoting an IoT-Enabled Economy	
Key Rec. KR6.1	The Executive Branch should monitor and evaluate progress of IoT adoption for supply chain logistics.
Enabling Rec. ER6.1.1	The Executive Branch should encourage businesses to adopt IoT technologies in their supply chain operations by reducing the initial investment costs and perceived risks associated with the implementation of IoT solutions.
Enabling Rec. ER6.1.2	Congress and the Executive Branch should apply an appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic IoT manufacturing supply chain.
Key Rec. KR6.2	The Executive Branch should facilitate public-private partnerships (PPPs) focused on IoT adoption to advance collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia developing end-to-end IoT solutions in supply chain logistics.

RECOMMENDATION *continued*	DESCRIPTION
Enabling Rec. ER6.2.1	The Executive Branch should promote collaborative IoT platforms that align stakeholder business incentives and encourage businesses to work together, fostering innovation, efficiency, and competitiveness.
Enabling Rec. ER6.2.2	The Executive Branch should promote the enablement and use of IoT trusted digital marketplaces and platform-based business ecosystems.
Key Rec. KR6.3	The Executive Branch should actively facilitate and support the adoption of AI in IoT applications to improve decision-making, optimize resource utilization, and enhance productivity.

RECOMMENDATION *continued*	DESCRIPTION
Enabling Rec. ER6.3.1	The Executive Branch should promote trusted AI-IoT platforms across supply chains and ecosystems to improve transparency and sustainability and drive economic growth.
Key Rec. KR6.4	Congress and the Executive Branch should provide overarching regulatory guidance for the unmanned aerial systems (drone) industry.
Key Rec. KR6.5	The Executive Branch should promote, facilitate, and monitor equity in the accessibility, realization and distribution of value and benefits created from the adoption and use of IoT.

Government Leadership

The Internet of Things (IoT) is revolutionizing industries and daily life through interconnected devices that facilitate communication and data exchange. A National IoT Strategy is vital for the U.S. to fully leverage IoT, guiding the Executive Branch and Congress in maintaining a competitive global stance. Key recommendations include establishing a cohesive national strategy through collaboration between Congress and the Executive Branch, accelerating IoT innovation via congressional support for R&D and favorable regulations, promoting international collaboration to harmonize standards and facilitate trade, and federal agencies adopting IoT technologies to lead by example and enhance governmental efficiency.

Objective 1: A coherent, comprehensive, and coordinated national IoT strategy that can guide Executive Branch in action and in working with Congress on the future of IoT in the U.S.

Key Recommendation KR1.1: Congress and the Executive Branch should work together to establish a United States national strategy for taking full advantage of the opportunity presented by the IoT.

Supported by Findings 2 and 3.

The United States is undergoing a profound transformation - one that is driven by economic, societal, and cultural innovations brought about by the Internet of Things (IoT). This fourth industrial revolution intertwines connectivity and digital innovation with the opportunity to drive a revolutionary metamorphosis across all parts of our nation. By integrating the physical with the digital to interconnect devices, systems, and people, we envision an Internet of Things that will enable a more resilient nation, spur economic growth, increase public safety, create a more sustainable planet, individualize healthcare, and facilitate an equitable quality of life and well-being. A strategic national approach for IoT will best facilitate this progress.

In 2010, the President's Council of Advisors on Science and Technology (PCAST) recommended that the federal government invest in a national, long-term, multi-agency, multifaceted research initiative in these areas.[180] 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 Office of Science and Technology Policy (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.[181] They found that "Isolated efforts by mission agencies are simply not sufficient to address the underlying issues in a holistic manner." Trying to address such issues agency-by-agency or sector-by-sector would result in inefficiencies and insufficient progress relative to system development timetables.

We might never get to where we need to be, and the recommendation is to create 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 opportunities in Agriculture, smart building, defense, emergency response, energy healthcare, manufacturing, and transportation advocated for a multi-agency, multi-sector comprehensive focus on the problematic crosscutting R&D challenges in Cyber-Physical System (CPS).[182]

[180] The President's Council of Advisors on Science and Technology, "Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology" (December 2010) available at https://www.nitrd.gov/pubs/PCAST-NITRD-report-2010.pdf

[181] "Winning the Future with Science and Technology for 21st Century Smart Systems" from the Office of Science and Technology Policy (April 2011) available at https://www.nitrd.gov/pubs/CPS-OSTP-Response-Winning-The-Future.pdf

[182] Cyber Physical Systems Senior Steering Group "Cyber Physical Systems" from the Office of Science and Technology Policy (June 3, 2015) available at https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

As shown in the earlier section of this report, "The Current State of IoT", these predictions from 2011 and 2015 were accurate, and the lack of a national strategy has impacted growth. Today, IoT opportunities are even more pervasive, the economic stakes are 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 and within sectors and agencies in advancing national priorities and solving economic and social challenges – across health, transportation, manufacturing, energy, communities, and cities, 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 catalogs the game-changing work the administration is already doing across many agencies in fundamental research, development, demonstration, and deployments – and the essential role agencies are playing in meeting our critical needs;
- outlines clear goals and objectives for IoT adoption in supply chain management;
- identifies potential opportunities and synergies across agencies, and identifies remaining gaps; and,
- outlines an R&D roadmap around the often multidisciplinary R&D needs to push new frontiers and achieve significant grand challenges.

The United States is undergoing a transformative era powered by the Internet of Things (IoT), which combines connectivity and digital innovation to boost resilience, drive economic growth, enhance public safety, and support sustainability. A strategic national IoT approach will accelerate this progress by integrating devices, systems, and people, addressing key national challenges, and promoting a more equitable quality of life. This strategy should include a comprehensive federal vision, clearly define IoT's role across various sectors, ensure U.S. leadership in IoT technologies, and document existing government efforts in research, development, and deployment. It must also set goals for IoT adoption in supply chain management, identify opportunities and gaps across agencies, and provide a roadmap for interdisciplinary R&D challenges. The benefits of successful implementation include enhanced coordination, optimized resource utilization, and accelerated technological adoption, all facilitated by dedicated focus, authority, and a central online presence to share strategies, engage stakeholders, and monitor progress. Like the nano.gov, ai.gov, and websites, stakeholders will benefit from a central Internet presence (e.g., iot.gov) that will help them follow the achievement of key outcomes of the IoT strategic approach.

Enabling Recommendation ER1.1.1: Congress and the White House should further improve and elevate interagency coordination including an IoT National Coordination Office and appoint a full time Chief Technology Officer.

Supported by Finding 2.

For more than a decade, there was a Cyber-Physical System (CPS) Interagency Working Group, which made some important contributions and recommendations to advance IoT fields. But in 2019, its focus was diluted. It is important to ensure that 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 the 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 interagency endeavors.

Congress should create and fund a new National Coordination Office for IoT/CPS to advance this strategy, as it has in Nanotechnology, Quantum, and AI. In doing so, it should also ensure that OSTP is fully resourced and funded to be able to take on these tasks – or risk losing focus on other critical needs.

The White House should appoint a Chief Technology Officer to coordinate IoT, Quantum, AI, and other emerging technologies. Note that the Critical and Emerging Technologies List would be a suitable scope for the Chief Technology Officer (CTO) office provided that IoT is added back, as recommended elsewhere in this document.

Enhancing interagency coordination will provide numerous benefits. A dedicated NSTC IoT committee, empowered and properly named, will ensure focused and strategic oversight of IoT initiatives, similar to existing committees for AI, Quantum, and Nanotechnology. Improved coordination will prevent siloed planning and resource inefficiencies, leading to more effective policy implementation and optimal utilization of resources. Establishing a National Coordination Office for IoT/CPS and appointing a Chief Technology Officer will streamline efforts across various emerging technologies, fostering innovation and accelerating the integration of IoT into the U.S. economy and infrastructure. This comprehensive approach will maximize economic, social, and security benefits, ensuring the U.S. remains a global leader in IoT.[183]

Enabling Recommendation ER1.1.2: The White House should include IoT in the federal Critical and Emerging Technology (CET) List.

Supported by Finding 2.

While IoT is critical to U.S. prosperity and socioeconomic success and still faces many barriers to adoption. IoT must be added to the Federal list of Critical and Emerging Technologies (CET) to ensure that the government remains aware of new opportunities to apply IoT and ensure adequate oversight.[184]

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 maturity.[184] Others are "coming up", including edge data and app platforms, server-less/Function-as-a-Service, cloud-connected sensors, edge AI chips, and low code/no code development platforms and satellite IoT connectivity.[185] Still others like data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, QRNG chips, biodegradable sensors, 6G and quantum computing are "years out" and require continued research investments.[186]

Adding IoT in the federal CET list ensures the government remains aware of new IoT opportunities and maintains adequate oversight. It will highlight IoT's critical role in U.S. prosperity and socioeconomic success, addressing barriers to adoption. By recognizing IoT as a key technology, the government can better support its development across various maturity levels—from mature technologies like cloud computing and IoT platforms to emerging ones like edge AI chips and biodegradable sensors. This approach fosters continued research investments, promotes innovation, and ensures that the U.S. remains a leader in IoT technologies, ultimately enhancing economic growth and societal well-being.

Enabling Recommendation ER1.1.3: Congress should study the impact of IoT components and modules produced by Chinese companies and other foreign adversaries to assess, understand, and mitigate the risks to cybersecurity, the IoT supply chain, and economic and national security.

Supported by Findings 5, 6, 8 and 9.

There are numerous independent government efforts examining the concerns with IoT technologies manufactured by companies in China and adversary nations. These studies are conducted by several government organizations, including the Department of Commerce, Department of Homeland Security, Federal Communications Commission, and Congress. However, each of these investigations are examining a different but related concern.

One concern is the potential cybersecurity risks posed by IoT modules produced in the People's Republic of China. For IoT modules the top 6 companies are Chinese and account for 64% of the global market.[187] More importantly, these modules are integrated into IoT devices and other IoT-enabled systems, which may be deployed into a variety of environments such as consumer, industrial, cities and critical infrastructure.

The federal government should conduct a broader and more holistic study of the impact of IoT technologies produced by companies in China and other foreign adversarial nations. The study should examine the IoT components, modules, devices and other "smart systems", as well as the software and firmware and supply chain. The objectives of the study are to identify

[183] Fast Track Action Subcommittee on Critical and Emerging Technologies, "Critical and Emerging Technologies List Update" from the National Science and Technology Council (February 2024) available at https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf

[184] S. Sinha, "55+ emerging IoT technologies you should have on your radar (2022 update)" from IoT Analytics (April 6, 2022) available at https://iot-analytics.com/iot-technologies/

[185] ibid.

[186] ibid.

[187] Steve Rogerson, "Quectel tops charts as cellular IoT module shipments soar" from IoT M2M Council (April 5, 2023) available at https://www.iotm2mcouncil.org/iot-library/news/iot-newsdesk/quectel-tops-charts-as-cellular-iot-module-shipments-soar/

and understand the true types of risks posed, how those risks are manifested, and the impact of those risks on cybersecurity, the IoT supply chain, and economic and national security. The study results should be publicly shared and should inform what actions, including policies, regulations and practices should be applied.

Enabling Recommendation ER1.1.4: Congress and the Executive Branch should establish a CEO-level ongoing advisory board to advise the federal government on matters pertaining to IoT.

Supported by Finding 2.

As IoT deploys and scales into the economy and civil society, it faces a variety of new opportunities and challenges. These opportunities and challenges may arise due to the evolution of IoT, the maturity of the supporting technologies, the enactment of new policies and regulations, and market and societal needs.

To stay current, make informed decisions and take relevant actions, the federal government should establish a group of experts and leaders with a broad and interdisciplinary background representing industry, academia, and civil society to advise the Secretary of Commerce and President on matters pertaining to IoT.

These advisory board will advise the Secretary on a variety of topics, including but not limited to the state of IoT in the United States, its impact on the economy and society, science and technology research, commercial innovation and development, standards, workforce development, governance, technology transfer, commercial applications, cybersecurity, privacy, analytics and AI, economic competitiveness, equity, international trade and coordination, policies and regulations, and other topics related to IoT.

The example organization used for the design of this advisory board recommendation is the National Artificial Intelligence Advisory Committee (NAIAC).

An IoT Advisory Board will ensure the federal government stays informed and can make well-informed decisions regarding IoT. It will provide expert guidance on emerging trends, technological advancements, and policy implications, helping to navigate the complexities of IoT integration. This proactive approach will foster innovation, enhance economic competitiveness, ensure cybersecurity and privacy, advance U.S. leadership and promote equity and international collaboration.

Enabling Recommendation ER1.1.5: The Executive Branch should integrate IoT considerations into the development of the national AI strategy and strategic AI initiatives.

Supported by Findings 3, 13, and 15.

AI requires and incorporates the use of data from various sources to build and train models, as well as make decisions and act upon those decisions. One source of data is from IoT devices and IoT-enabled systems. As the deployment and use of IoT increasingly grow and scale, an increasing amount of data will be used by AI. Research firm IDC estimated that by 2025, there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data.[188]

While AI facilitates the analysis of IoT and leads to automation of operations across a variety of applications, the use of IoT data raises a variety of challenges. Concerns such as privacy and sharing of the data, the source of the data, and the use of the data, are important considerations.

The convergence of AI and IoT (also known as AIoT) is already underway. As more and more IoT systems incorporate AI into their operations, and these systems increasingly become autonomous, the impact of AIoT must be considered.

There are a variety of federal AI initiatives, some announced and some in planning. As AIoT becomes more prevalent, these AI initiatives should take into account the role of IoT devices and systems, as well as considerations for its use and operation. Current federal AI initiatives, and future developers of a national AI strategy (including those recommended above) should include IoT in their considerations.

Innovation Leadership

Key Recommendation KR1.2: Congress should accelerate IoT technology innovation to support an evolving IoT.

Supported by Findings 1, 2, 4, and 18.

The United States is a global innovation leader. As IoT continues to evolve, new innovative technologies and solutions are required to not only keep up, but to lead. Furthermore, IoT is not one technology, but a set of disparate technologies at various maturity levels. Innovation in IoT and related

[188] "Future of Industry Ecosystems: Shared Data and Insights" from IDC (January 6, 2021) available at https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/

technologies is a key component to overcome existing IoT challenges (e.g., cybersecurity, communications, privacy), to support the evolution of IoT (e.g., 4G → 5G → 6G), and to create new applications, solutions, and capabilities as a result of the evolution.

Global innovation leadership in IoT requires continued investment in research and development. While many large organizations produce innovative technologies and solutions, many of the innovations are driven by small innovative businesses and start-ups. In addition, the federal government supports and funds a variety of innovative research through its national labs, university and industry grants, technology transfer (Lab-to-Market) and other initiatives.

The federal government should continue to facilitate and fund new innovations, particularly those by small enterprises and startups, as well as high-risk, high reward research. In addition, the government should support research in future areas that may be significant to the area of IoT (e.g., 6G, quantum, AI, etc.).

Investing in IoT innovation ensures the U.S. remains a global leader, addresses critical challenges, supports technological evolution, fosters new applications, and leverages contributions from small businesses and startups. Government support for high-risk research and future technologies will drive further advancements and maintain the nation's competitive edge.

Enabling Recommendation ER1.2.1: Congress should fully fund existing IoT research, development, deployment, and demonstrations.

Supported by Findings 1 and 18.

The IoTAB recommends that 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 appropriations that fully fund 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 allow 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 Advanced Research Projects Agency (ARPA), Department of Energy (DOE), NIST, 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.

Fully funding existing IoT research, development, deployment, and pilot projects will accelerate technological advancements, ensure continued innovation, and maximize the benefits of IoT investments. It will support the development of essential infrastructure, enhance connectivity and interoperability, and promote automation at scale. It will further strengthen the U.S.'s position as a global leader in IoT, driving economic growth, improving public services, and enhancing national security.

Enabling Recommendation ER1.2.2: Congress should facilitate and accelerate adoption of IoT technologies by small businesses.

Supported by Findings 4, 16, and 17.

The federal government should consider actions that accelerate the adoption and use of IoT technologies by small business organizations. Small businesses are the heart of the American economy and can reap significant benefits from the adoption and use of IoT in their operations, allowing them to become more efficient, productive, competitive, and profitable with the limited resources and capabilities that they have.

Spurring small businesses to adopt IoT can promote broader IoT adoption across the market. As more and more small businesses adopt this technology, they serve as good implementation examples for those other same size organizations who might also be considering this technology.

However, small businesses face many barriers to adopting IoT. This ranges from a lack of awareness and understanding, to knowing where to start or having the right resources and capital to deploy and maintain these solutions.

The federal government should consider a variety of new and existing programs and initiatives to help small businesses adopt IoT technologies into their operations. Some examples include:

- Utilizing existing Small Business Administration (SBA) resources, capabilities, and channels to communicate and promote awareness of IoT solutions and benefits.
- Utilizing SBA and associated funding mechanisms, such as loans and grants, to support the procurement and deployment of IoT solutions.
- Leveraging the current Manufacturing Extension Partnerships (MEP) to promote and support the use of IoT for small manufacturers and factories.

- Leveraging the agriculture extension offices to promote and support the use of IoT for small agricultural producers.
- The Federal Government could set aside easily and readily tappable funding pools year-round for innovation and next-generation technologies that these small companies can utilize. Grants could be set aside specifically for these types of companies.
- The Federal Government could set aside fast-track programs for startups and small companies to adopt this technology in pilots.
- A network of startups and small businesses can be formed to encourage and facilitate adoption. Similar small businesses can be identified and work together. Leading startups and small businesses can be referred to others for best practice and learning.
- The Federal Government could set up a system to make it easier for startups and small companies to find relevant funding sources to adopt this technology like grants.

The Federal Government could set aside readily available year-round funding pools for innovation and next-generation technologies. Grants could 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 Small Business Innovative Research (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)[189]
- Department of Energy (DOE) Office of Small and Disadvantaged Business[190]
- National Science Foundation Program for Small Business[191]

Enabling Recommendation ER1.2.3: The Executive Branch should accelerate the adoption of IoT technologies developed and manufactured by small business and startup organizations.

Supported by Findings 16, 17 and 18.

Many of the innovative and disruptive solutions come from early-stage start-ups and small businesses. Many of these companies offer unique and compelling solutions to challenging problems.

However, these businesses face a variety of unique challenges in developing and bringing innovative offerings to market. These challenges include access to funding and investment, incompatible procurement practices and processes, legacy standards and regulations, market incumbents and low market awareness. As a result, many promising innovations never reach commercialization, or companies stay in business long enough for commercialization.

For example, many of these early-stage companies offering solutions to government customers (including federal, local, and state) have to provide their upfront capital, access, and know-how, before hopefully being selected as a result of a request for proposal (RFP). The process for these projects can also take many years to bring them from proof-of-concept to proposal to commercial operation. Due to the lengthy cycle, many companies may go out of business, pivot to another area of focus, or lose interest in that time frame. As a result, an innovative company goes away, or the government loses out on a potentially innovative solution that could have addressed its needs.

In another example, small businesses lack access and relationships with state and local governments, while large and established companies have a history and know-how to access these customers, procurement processes and markets. As a result, many innovation developers may not know of an opportunity where their solution would be a good fit, nor will they know how to access it.

For those programs and initiatives under its control or influence, the federal government should accelerate the adoption of IoT technologies manufactured by small business and startup organizations through development of thoughtful policies, procedures, and targeted funding methods that take into

[189] "Promoting the growth of Minority Business Enterprises in every sector" from Minority Business Development Agency available at https://www.mbda.gov/who-we-are/overview

[190] "Doing Business with the Department of Energy" from Office of Small Disadvantaged Business Utilization available at https://www.energy.gov/osdbu/office-small-and-disadvantaged-business-utilization

[191] "Industry: Engaging with The National Science Foundation" from U.S. National Science Foundation available at https://www.nsf.gov/funding/smallbusiness.jsp

consideration the unique challenges faced by small innovation developers. This may be for solutions that the federal adopts for its own use, or for IoT technology adopted by other organizations funded through the use of federal grants and loans. For example,

- The Federal Government could set aside fast-track programs for startups and small companies to deploy this technology in pilots. One method to do so may be to establish 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 government can also foster more local support, such as by encouraging local governments to leverage its local startup accelerator network to develop technology and fast-track it to local adoption on successes, and through work with chambers of commerce, rotary clubs, and other associations to help identify relevant IoT manufacturers to support.

Federal funding mechanisms and procurements targeted to small businesses and startup innovation developers can aid these companies so they can more effectively compete with larger organizations on RFPs relevant to their business. End-users benefit from these federal government efforts. Innovative solutions from small businesses provide end-users with more technology options to choose from. 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.

Enabling Recommendation ER1.2.4: Congress and the Executive Branch should specify and use innovative IoT technologies and applications in federally funded projects.

Supported by Findings 1, 3, 18, 20, 21, 23, and 24.

The federal government, through its procurement and funding activities, can influence and facilitate action to improve IoT adoption. For example, the General Services Administration (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. Use of IoT in federal projects also bolsters trust in the reliability and trustworthiness of the technology.

In 2021, the Administration set ambitious 2030 greenhouse gas emissions goals.[192] By requiring increased use of energy efficient technologies, the U.S. can make progress toward these and other environmental goals. IoT tools and technologies play a central role in managing energy efficiency.

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 for 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 government should also 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, 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 automated 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.

Enabling Recommendation ER1.2.5: Congress should continue to support and fund technology research, through industry, university, and national labs, to further advance and accelerate the development of IoT technologies and its enabling infrastructure.

Supported by Findings 1 and 18.

The federal government should continue to support and fund technology research, through industry, university, and national labs, to further advance and accelerate the development of IoT technologies and its enabling infrastructure. Doing so will enable the United States to build the technical infrastructure that will support the full realization of the outcomes provided by IoT.

[192] "President Biden Sets 2030 Greenhouse Gas Pollution Reduction Target Aimed at Creating Good-Paying Union Jobs and Securing U.S. Leadership on Clean Energy Technologies" from the White House (April 22, 2021) available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/22/fact-sheet-president-biden-sets-2030-greenhouse-gas-pollution-reduction-target-aimed-at-creating-good-paying-union-jobs-and-securing-u-s-leadership-on-clean-energy-technologies/

Some example research areas important to the further IoT development include:

- **Enabling more capable and intelligent devices.** IoT workloads are increasingly processed at the edge to meet low latency, high reliability, and autonomous operation requirements. Advancements are needed in device processing capabilities to support AI workloads, reduce processor energy consumption, and develop low-cost sensors and processors.
- **Enabling network infrastructure to support IoT at scale.** Network infrastructure must support billions of diverse IoT devices across cloud, edge, and mobile environments. Advancements are needed in managing distributed networks, spectrum sharing and management, infrastructure for AI and complex IoT application workload, fault tolerance, resilience, and context-aware computing.
- **Enabling usable AI for IoT.** The convergence of AI and IoT promises to unlock the value of the data and the autonomous capabilities enabled by the Internet of Things. Advancements such as development of AI algorithms that can operate on resource constrained devices, ethical AI, explainable AI tools, collective intelligence (including swarms) and ambient IoT systems.
- **Enabling human-centric usable IoT**. IoT's full value is achieved when it is seamlessly integrated into all aspects of our economy and lives. To realize its benefits, IoT must be human-centric and user-friendly. This requires advancements in designing IoT systems for human-AI interaction, building trust in AI, and improving user experience and interactions.
- **Enabling trustworthy IoT.** In a future with billions of IoT devices integrated into the economy, trust in IoT is crucial. Ongoing research in cybersecurity and privacy must continue, with additional efforts to develop trustworthy IoT systems. Key areas include confidential computing, lightweight quantum-safe cryptographic algorithms, and adaptive, self-defending networks.
- **Enabling interoperability.** The ability for devices and systems to freely exchange data and communicate is a key enabler in fully integrating and scaling IoT into the economy. Continued research and development of various standards, frameworks, and protocols is essential

IoT is constantly evolving to meet diverse adopter needs, requiring continuous research and development to overcome adoption barriers and create technological advancements. Shifting data processing from the cloud to the edge supports low latency and autonomous operations but adds complexity to system design and management. Developing new technologies is essential to drive these innovations.

Investing in ongoing IoT research and development will accelerate groundbreaking innovations that drive economic growth and enhance technological leadership. Federal research investments catalyze advancements with broad impacts, including high-risk projects that industry might not pursue. These efforts lead to productizing cutting-edge technologies to the market, fostering efficiency, reliability, and competitiveness across sectors.

International Leadership

Key Recommendation KR1.3: The Executive Branch should promote international collaboration in IoT adoption to share knowledge, best practices, and resources; harmonize standards, policies, and regulations; and facilitate trade.

Supported by Findings 2, 3, 5, 6, 7, 11, 14, and 25.

The global nature of data, interconnected systems, supply chains and economies, requires international collaboration to facilitate the adoption of IoT. The fourth industrial revolution offers a unique opportunity to foster the sharing of IoT knowledge, best practices, and resources; harmonize standards, policies, and regulations; and facilitate trade among countries and regions. The goal is to spur innovation and accelerate the widespread adoption of IoT technologies, distribute benefits and connected outcomes, while minimizing risks and adverse impacts. For example, stakeholders from the United States Federal Government, European Union Commission, and Asian Development Bank can form a global ecosystem that supports the development, deployment, and use of IoT solutions.

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 to tackle technical, economic, social, regulatory and trade challenges. 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 outcomes of these collaborations include the development of harmonized regulations, standards, and guidelines that enable seamless and secure integration of IoT systems across borders. This harmonization can foster efficient and resilient global supply chain networks, and more equitable distribution of value and benefits.

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 areas of common interest, such as in supply chain management, environmental protection and sustainability, and global resilience. 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 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.

Trade is an area of opportunity for international collaboration for IoT. The integration of IoT technologies creates new innovative "smart and connected products" and services. These "smart products" may be offered and delivered in new ways ("product as a service", etc.), through new channels. These "smart and connected products" create new challenges, from market access, data ownership, cybersecurity, infrastructure, and regulations. Matters related to the trade of "smart and connected products" should be included for consideration in existing, planned, and future trade treaties and agreements.

Enabling Recommendation ER1.3.1: The Executive Branch should create internationally compatible data minimization guidance related to IoT devices, aligning with the NIST Privacy Framework and NIST Cybersecurity Framework principles.

Supported by Findings 1, 3, 7, and 8.

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 (PbD). 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.

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.

Key Recommendation KR1.4: The Executive Branch should lead by example by specifying, procuring, and adopting IoT by federal agencies for its internal use.

Supported by Findings 1 and 18.

The federal government can increase market adoption of innovative technologies through "leading by example" and procuring innovative and emerging technology solutions for internal use. "Leading by example" refers to a set of actions that the federal government can do to signal both support and interest in IoT.

The federal government operates and provides a variety of services in the United States, in its territories and in many countries around the world. It owns and uses a variety of assets and tools to operate and provide services. In 2021, the federal government spent $645 billion in contracts for products and services, up from $513 billion in 2017.[193] The federal government's substantial buying power allows it to influence and drive desired outcomes. The government can use direct procurement, implementation of contracting policies and innovation pilots to support market development of IoT and associated technologies.

The federal government should specify, adopt, and promote its use of IoT technologies, in order to drive broader visibility and awareness to the market and to other agencies. For example, the Central Intelligence Agency (CIA) awarded a $600 million contract to Amazon Web Services (AWS) for single client private cloud.[194] While providing the CIA with innovative capabilities, this contract award signaled confidence in the technology to the market. From an article discussing this event, "For many years, the pace of cloud adoption was slowed by concerns over data

[193] K. Bernal, "Federal Contract Spending in the Last 5 Years" from GovConWire (May 25, 2022) available at https://www.govconwire.com/articles/federal-contract-spending-in-the-last-5-years/

[194] K. McLaughlin, "Amazon Wins $600 Million CIA Cloud Deal As IBM Withdraws Protest," from CRN (October 30, 2013) available at https://www.crn.com/news/cloud/240163382/amazon-wins-600-million-cia-cloud-deal-as-ibm-withdraws-protest

security. But when the Central Intelligence Agency awarded a $600 million contract to Amazon Web Services Inc. in 2013 to move some of the nation's most sensitive information into the cloud, it was widely viewed as a seminal moment for the fledgling industry."[195]

Leading by example, the government can accelerate IoT adoption, fostering innovation and technological advancement. This approach increases market confidence, encourages investment in IoT technologies, and demonstrates practical applications of IoT, driving awareness and understanding. Promoting IoT within federal operations can improve efficiency, security, and service delivery, setting a standard for other organizations to emulate. By showcasing successful IoT implementations, the government can expand IoT adoption, ensuring the U.S. remains a global leader in technological innovation.

Enabling Recommendation ER1.4.1: The Executive Branch should lead the way in facilitating IoT adoption by adopting and promoting IoT technologies and systems for its own internal operations and needs.

Supported by Findings 1 and 18.

The federal government operates and provides a variety of services in the United States, in its territories and in many countries around the world. The government owns and uses a variety of assets and tools to operate and provide services.

The use of IoT will facilitate operations and in carrying out services. This will lead to increased responsiveness, higher service effectiveness and relevance, improved productivity, safety, resilience and cost savings and avoidance. For example, IoT-based asset tracking helps agencies manage their assets, equipment and supplies more effectively, reduce equipment losses, facilitates distribution of equipment, and aids in recovery of missing and stolen equipment and supplies. Another common use of IoT is for condition monitoring. This application spans a variety of uses, from the operating condition of a vehicle to critical infrastructure and allows for the remote monitoring of an asset's status and performance. The data collected enables asset owners to detect issues early, and to apply corrective measures to minimize downtime, optimize asset performance, and meet service levels.

There are many opportunities for the federal government to apply IoT technologies. Specifically,

- The federal government should develop an initial top ten or twenty list of most commonly used IoT applications (asset tracking, etc.). This can be done at the agency level, or at a higher level.
- The agencies should review this list and look for opportunities to procure and integrate this application into their operations and services.
- Each agency should continually review and update the list of applications and opportunities for future integration on a periodic basis.
- The federal government should promote its current use of IoT technologies, in order to drive broader visibility and awareness.

IoT applications and solutions should be piloted at a small scale initially to evaluate effectiveness and identify challenges. Agency funding and budget allocations for IoT may not be a high priority, so agencies should focus on those applications where the use of IoT will result in financial savings from operating an asset or service, so that the funding source can come from an existing budget allocated to that operation.

Enabling Recommendation ER1.4.2: Congress and the Executive Branch should upgrade legacy federally owned or operated IoT infrastructure that is integrated into government facilities, assets, and operations.

Supported by Findings 1 and 8.

Many government facilities have functional, operational, and safety dependencies on IoT-related systems. These systems can serve as gateways for malicious actors who might take control of critical applications (including life and safety-related services) such as those within a building (i.e., heating, air conditioning, physical access).

By upgrading these systems, agencies can set an example for private industry to follow. These upgrades 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.

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.

[195] "M. Albertson, "CIA's move to cloud a game changer for public sector," from Silicon Angle (June 16, 2017) available at https://siliconangle.com/2017/06/16/cias-move-cloud-game-changer-public-sector-awspssummit/

It is also notable that a great deal of data in an unprotected federal IoT infrastructure may contain significant amounts of confidential data including citizens' personal and private information.

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.[196] There are also parallels that could be explored such as the National Cyber Labeling Program for Consumer IoT versus Energy Star on appliances. 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. Another potential information source is NEMA's cyber hygiene best practice document for end-users.[197]

The need to retrofit many government buildings as called for in Executive Order 14057, in tandem with the Federal Sustainability Plan will provide additional opportunities. E.O. 14057 and the Federal Sustainability Plan serve to catalyze American clean energy industries and jobs while intending to achieve a net-zero emissions buildings goal by 2045. This effort requires that the Federal Government collaborate with stakeholders charged with new building construction, major renovations, and existing real property to electrify systems, decrease energy use, reduce water consumption, and cut waste. Federal agencies are being asked to set data-driven goals (by 2030), targeting energy and water reductions that leverage performance benchmarks for building type categories and the composition of the agency's building portfolio. Performance contracting is essential to facilitate these ambitious goals, particularly since the objectives are to reduce emissions, improve efficiency, and modernize facilities while delivering financial savings.

It is critical that legacy modernization and new construction projects be designed, constructed, and operated to be net-zero emissions by 2030 and, where feasible, net-zero water and waste. Appropriate prioritization and use of ongoing data analytics will help to both advance IoT implementation and support federal sustainability goals.

[196] Building Cyber Security available at https://buildingcybersecurity.org

[197] "Cyber Hygiene Best Practices Part 2" from National Electrical Manufacturers Association available at https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2

Modernizing IoT Infrastructure

Modernizing IoT infrastructure is crucial for the U.S. to fully exploit IoT technologies by ensuring robust, reliable, and widespread connectivity, communications, and interoperability. Key recommendations include the Executive Branch promoting industry collaboration to adopt existing standards and protocols, establishing methods to maximize interoperability through consistent models and interfaces, expanding programs to guarantee sufficient availability and quality of IoT connectivity nationwide, and encouraging digital infrastructure initiatives to support the digital transformation of enterprise business processes, thereby enhancing operational efficiency and innovation.

Objective 2: Congress and the Executive Branch collaborating with industry, academic, and public-sector partners to enhance and modernize the infrastructure that enables and supports IoT.

For continued and expanded adoption of IoT throughout the nation, it is vital that IoT technology be highly interoperable and connected. 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.

Such collaboration should include the provision of clear direction and support for consistent and resilient communications and exchange of data among devices, update of legacy computing and networking systems, improved connectivity and interconnection among technologies, and digitalization of processes and operations.

The IoTAB recognizes that the need for collaborative development applies to all industry sectors. The enabling recommendations below are illustrative examples and are not intended to be exclusive.

Promoting Existing Methods

Key Recommendation KR2.1: The Executive Branch should promote collaborative development across industries to adopt existing industry standards and protocols that enable IoT interoperability.

Supported by Findings 1 and 11.

Interoperability is a key enabler for connecting devices with each other, industry, and enterprise systems, and with other systems across industries. However, interoperability is a long-running challenge that hinders the ability of IoT to integrate, exchange data and interoperate.

Interoperability is achieved through a variety of ways, including through the development and implementation of standards, third-party middleware and connectors, and other emerging methods (e.g., use of AI to translate different semantic definitions, etc.).

The federal government should continue and build on its "industry leads, government supports" approach to the development of standards and enablement of interoperability for IoT. In this approach, the government believes that standards should be developed collaboratively by industry, standards development organizations, and interested partners. This results in standards that are based on consensus industry needs, are robust, scalable, and have industry support. Systems based on these standards are open and interoperable.

The government should continue and expand efforts to facilitate interoperability. These industry efforts include:

- Conducting the research and developing the frameworks that inform the standards development processes.
- Providing testbeds enabling industry to test and confirm interoperability of systems.
- Providing technical expertise to support standards development activities.
- Encouraging the adoption of existing developed standards instead of developing additional standards whenever available, possible, and feasible.
- Specifying and procuring those IoT technologies based on industry consensus standards.

- Collaborating with international governments to harmonize geographic and region-specific standards and practices.

In support of this key recommendation, the IoTAB developed a series of enabling related recommendations that are specific to a particular industry. However, not all industries are listed here. Similar recommendations, such as for smart communities and agriculture are listed elsewhere in this report.

Enabling Recommendation ER2.1.1: The Executive Branch should advocate and facilitate standards development and adoption that leads to interoperability for public safety IoT.

Supported by Findings 1, 11, and 24.

Public safety IoT applications enhance incident responses and coordination among responder teams, providing safety benefits that lead to a safer community. An example scenario is described below:[198]

In a future smart city environment, disparate systems communicate and collaborate with each other to create outcomes benefiting city residents and businesses.

For example, audio sensors detect gunshots. Once detected, the streetlights on nearby streets could increase in brightness to facilitate the ability of witnesses to identify the shooters and for police cameras to capture better quality surveillance footage. The information is then routed to the city's 911 response call center, which then informs the operator and provides situational awareness information to responding police officers.

However, the proliferation of IoT with interoperability challenges hampers this future success. In public safety, in practice, the individual IoT applications used were independently procured by different city organizations with little consideration for interaction and communication with each other. This leads to the deployment of technology systems that are:[199]

- Not extensible or cost effective because they are custom systems that cannot communicate and exchange information with each other.
- Based on a diverse set of proprietary architectures, standards and protocols that have not yet converged.
- Not sufficiently interoperable and scalable to support smart city applications and outcomes.

In many cases, the federal government should advocate for interoperability and facilitate the adoption of interoperable solutions for public safety through a variety of actions. Some possible examples of actions include, but not limited to:

- Education and awareness through the development of education/training materials to help agencies and state and local jurisdictions/agencies apply best practices for interoperability.
- Specification of interoperability requirements for agencies, and state and local jurisdictions procuring IoT applications funded by federal grants and funding.
- Compiling guidelines and best practices for entities from the current starting point (e.g., NISTIR 8255: Interoperability Real-Time Public Safety Data, Cybersecurity and Infrastructure Agency (CISA) SAFECOM Interoperability Continuum) will help improve future results.
- Prioritizing solutions which adhere to interoperability guidelines in government contracts for public safety IoT (e.g., bulk purchase pricing such as through the General Services Administration (GSA) catalog).
- Considering tax incentives that encourage companies to implement public safety IoT with interoperable data standards.
- Supporting existing and future research. For example, the U.S. Department of Homeland Security (DHS) is assessing the current state of smart cities standards for public safety applications with research, design and testing of a Smart City Interoperability Reference Architecture (SCIRA) interoperable framework that integrates commercial proprietary IoT sensors for public safety applications at the community level.[200]

[198] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[199] "A Consensus Framework for Smart City Architectures", IES-City Framework Release 1.0, IES-City Framework Public Working Group, September 30, 2018. https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFramework_Version_1_0_20180930.pdf

[200] "Smart City Interoperability Reference Architecture" from U.S. Department of Homeland Security Science and Technology Directorate (July 8, 2022) available at https://www.dhs.gov/publication/st-smart-city-interoperability-reference-architecture-fact-sheet

Enabling Recommendation ER2.1.2: The Executive Branch should advocate and facilitate standards development and adoption that leads to interoperability for medical devices.

Supported by Finding 1, 11, and 22.

The ability of medical devices to communicate and exchange information with each other and medical systems is essential to timely and responsive care, automation of manual processes and operational efficiency.[201]

However, attaining interoperability is challenging. A study examining IoT technology infrastructure challenges reported that "healthcare and medical devices come from a variety of manufacturers and employ different and proprietary data formats and communication protocols. While Health Delivery Organizations have addressed this situation through the use of middleman organizations which convert data from one proprietary protocol to another, this approach adds cost and complexity to the process of integrating medical devices.[202] Developing standards for the medical devices is complicated as device identity standards vary across device classes because of the wide range of technologies used in patient care from automated blood pressure cuffs to ventilators and the varying technical complexity used in their manufacture."[203]

The study further stated that medical device interoperability falls along "a continuum from data to communication on to semantic and workflow. Different medical devices may be at different places on this continuum, ranging from basic interoperability that covers data to plug-and-play workflow interoperability."[204] and that "While many medical devices can communicate today, they do so with "dysfunctional interoperability" as proprietary protocols make it difficult to extract the information."[205]

In a clinical practice, interoperability concerns lead to poor safety, poor prioritization, lost and missing data, inefficiency, reluctance to standardize processes, inability to measure and improve care and failure to transfer and disseminate successes.[206] A 2013 analysis by the West Health Institute found that medical device interoperability would help to mitigate waste and could lead to $35 billion in annual savings across the U.S. healthcare system.[207] There are ongoing industry efforts to develop consensus standards including:[208]

- Integrating the Healthcare Enterprise (IHE) promotes the coordinated use of established standards such as DICOM (Digital Imaging and Communications in Medicine) and HL7 to address specific clinical needs in support of optimal patient care.
- Devices Domain which seeks to enable the integration of healthcare devices, typically via translators, with other IT solutions such as Electronic Health Records (EHR).
- Service-oriented Working Groups in Health Level 7 International (HL7) looking at Fast Healthcare Interoperability Resources (FHIR).
- Several efforts around open health device interoperability standards, including the Association for the Advancement of Medical Instrumentation (AAMI) 2700 series looking at high-level architectures, AAMI/UL (Underwriters Laboratories) 2800 looking at process-oriented interoperability and ISO/IEEE 11073 which covers point of care medical device communication.

A Deloitte report suggested that "open platforms, based on open data standards is the direction of travel that needs to be followed to enable payers, providers, and technology vendors to finally come together to make data more available to one another".[209] While some efforts led to commercial adoption of standards (e.g., IHE Devices), the adoption of open interoperability standards at the device level has "fallen flat".[210] This is attributed to a lack of

[201] V. Gowda, H. Schulzrinne, and B. Miller, "The case for medical device interoperability" from JAMA Health Forum (January 14, 2022) available at https://jamanetwork.com/journals/jama-health-forum/fullarticle/2788095

[202] Ken Fuchs, IEEE 11073 Standards Committee Chair, IHE DEV Domain Co-Chair.

[203] Chan, B., Feller, G., Paramel, R., Reberger, C. Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT), Strategy of Things. Pending publication Fall 2024.

[204] "Medical device interoperability. A safer path forward." Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. https://www.aami.org/docs/default-source/reports/2012_interoperability_summit_report.pdf

[205] Ken Fuchs response comment to article available at https://jamanetwork.com/journals/jama-health-forum/fullarticle/2788095

[206] "Medical device interoperability. A safer path forward." Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. https://www.aami.org/docs/default-source/reports/2012_interoperability_summit_report.pdf

[207] "The value of medical device interoperability," West Health Institute, 2013. https://westhealth.org/wp-content/uploads/2015/02/The-Value-of-Medical-Device-Interoperability.pdf

[208] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[209] "Medtech and the Internet of Medical Things: How connected medical devices are transforming health care," Deloitte Center for Health Solutions, July 2018. Figure 9. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf

[210] Ken Fuchs response comment to article in Note 178. https://jamanetwork.com/journals/jama-health-forum/fullarticle/2788095

a business case for device manufacturers to move away from proprietary solutions and a lack of healthcare providers asking for open interoperable interfaces.

The federal government should advocate strongly for interoperability and facilitate the adoption of interoperable solutions for healthcare and medical devices through a variety of actions. Some possible examples of actions include, but not limited to:

- Support ongoing industry efforts to develop consensus and open standards.
- Facilitate efforts to address gaps targeting specific needs in existing standards. There is significant variability across clinical, health IT and organizational practices, which makes it difficult to develop "universally applicable" technical standards.[211]
- Specify and procure IoT solutions used in federal medical facilities which adhere to industry consensus standards and support interoperability.
- Specify the need for interoperability and specification of industry consensus standards for health organizations that procure medical device equipment supported by federal funds.

Enabling Recommendation ER2.1.3: The Executive Branch should promote the development and use of standards for supply chain logistics, traceability, and assurance.

Supported by Findings 1, 5, 11, and 25.

The federal government should encourage the development, adoption, and use of standards and protocols for supply chain logistics, traceability, and assurance. By collaborating with Standards Development Organizations (SDOs) and international allies, the government can promote secure and traceable products, ensuring efficient and reliable trade of goods.

Incentivizing Global Digital Identifiers: Suppliers should be incentivized to establish unique corporate, product, asset, and part IDs linked to a digital thread. This will enhance the tracking and tracing of goods, improving supply chain efficiency, transparency, resilience, and security. Encouraging the use of Global Digital Identifier Standards like GS1[212] in procurement contracts and regulatory frameworks will reduce cost and risk, speed adoption and increase economic value.

Support for Small Businesses: The government should provide financial and technical support to businesses, particularly small and medium-sized enterprises, to help them adopt and comply with these standards. Mechanisms should be established to monitor and adjust the effectiveness of these standards over time, addressing emerging challenges and opportunities.

Industry Initiatives and Education: Additionally, the government should support industry-led initiatives and education campaigns to promote IoT standards in supply chain management. This will foster the development and adoption of standards that enhance economic value.

Facilitating Interoperability: These standards should enable interoperability, reliability, and security across IoT-enhanced supply chains. This facilitates data exchange, improves decision-making, and optimizes services. By driving the adoption of IoT technology, the government can minimize supply chain security risks[213] and maximize economic value for businesses and users.

Public-Private Partnerships: The government could identify one or more federal agencies to convene a public-private partnership to establish a roadmap towards interoperability. This roadmap should aim to enable collaboration tools and data models for supply chain logistics, traceability, assurance, stakeholder inclusiveness, prioritizing critical areas, and developing compliance mechanisms.

Promoting and adopting these standards will enhance the interoperability, reliability, and security of supply chains. This will lead to improved efficiency, reduced risks, and maximized economic value for businesses and consumers. Supporting small businesses and fostering industry initiatives will ensure widespread adoption and continuous improvement, keeping U.S. trade competitive and resilient.

Enabling Recommendation ER2.1.4: The Executive Branch should promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across IoT systems and devices.

Supported by Findings 1, 8, 11, and 25.

Despite the potential to track freight with IoT technologies, end-to-end supply chain visibility, a basic capability for a resilient supply chain, is still not possible today. There remains a critical need for

[211] "Medical device interoperability. A safer path forward." Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. https://www.aami.org/docs/default-source/reports/2012_interoperability_summit_report.pdf

[212] April 2023 IoTAB Invited Speaker: Angela Fernandez, GS1 US – Global Identifiers for IoT. Slide deck from her presentation is available at https://www.nist.gov/system/files/documents/2023/04/24/Speaker%20-%20Angela%20Fernandez%20-%204.19.23.pdf

[213] April 2023 IoTAB Invited Speaker: Don Davidson, Synopsys – Cyber Supply Chain Risk Management Perspectives. Slide deck from his presentation is available at https://www.nist.gov/system/files/documents/2023/04/24/Speaker%20-%20Don%20Davidson%20-%204-19-23.pdf

cross-domain visibility and transparency to bolster supply chain resilience. One key cause discussed in Finding 25, is the lack of interoperability among systems, technologies, and software used across the fragmented supply chain network. This results in inefficiencies, increased costs, delays, and limited real-time visibility and traceability.

To enhance interoperability, reliability, and security across IoT systems and devices in supply chains, the federal government should promote the development and adoption of standards and protocols. Common standards enable shippers and the intermediary worldwide network of logistics services providers (carriers, warehouse operators and terminal operators) to seamlessly integrate IoT solutions into their supply chain operations, facilitating data exchange and improving decision-making processes. Establishing common standards will foster innovation and competition throughout the supply chain, simplify integration and maintenance, and potentially reduce costs while ensuring regulatory compliance.

Developing these standards requires collaboration between government agencies, industry stakeholders, technology providers, and researchers. Key specifications to address include data formats, communication protocols, interoperability APIs, security measures, and device compatibility. A diverse range of stakeholders, including businesses, technology providers, academia, and government agencies, should be involved. The focus should be on prioritizing critical areas such as data exchange, device interoperability, and security, building on existing standards where possible.

One example of related government action to drive data exchange between the businesses in the supply chain is the White House Freight Logistics Optimization Works (FLOW) pilot initiative. The FLOW pilot program[214] aims to boost supply chain resilience by enhancing data transparency and collaboration among supply chain stakeholders, including government agencies, private firms, and industry partners. While this program focuses on sharing freight data across supply chains (some of which may be supplied by IoT systems), and not specifically on supply chain IoT, it illustrates the need for the federal government to convene industry stakeholders and competitors together to work towards a common objective.

Some examples of actions that the government can support promote standards development and use include:

- Conducting research and developing the frameworks that informs the standards development processes for supply chain and logistics.
- Providing testbeds enabling industry to test and confirm interoperability of systems.
- Providing technical expertise to support standards development activities.
- Encouraging the adoption of existing developed standards instead of developing additional standards whenever available, possible, and feasible.
- Specifying and procuring those IoT technologies based on industry consensus standards for government use in its supply chain operations.
- Collaborating with international governments to harmonize geographic and region-specific standards and practices.
- Promote standards through education and awareness campaigns, providing resources and guidance to help businesses implement IoT solutions effectively.

Promoting IoT standards in supply chain management will drive innovation, improve efficiency, and ensure security and reliability. Supporting efforts by the federal government will facilitate seamless integration, foster competition, and reduce costs, ultimately maximizing the benefits of IoT technology for businesses and consumers.

Key Recommendation KR2.2: The Executive Branch should establish methods to foster interoperability for IoT technology to the greatest extent possible, through the use of consistent models, protocols, application interfaces, and schemas.

Supported by Findings 1 and 11.

To fully leverage the potential of IoT technology, it is crucial to establish methods that promote interoperability through consistent models, protocols, application interfaces, and schemas. This approach will ensure that IoT devices from various manufacturers can seamlessly interact, enhancing compatibility and connectivity.

Focus on Interoperability: While IoT technology has advanced significantly, much of the focus has been on individual devices rather than on interoperability. Ensuring that devices from different manufacturers can work together will boost competition, technology availability, and adoption by enterprises and consumers.

Industry-Led Models: A successful example of fostering interoperability is the 'Welcoming All Valuing Everyone (WAVE) Project'[215] in the streaming media industry. Hosted by the

[214] "Freight Logistics Optimization Works" from U.S. Department of Transportation available at https://www.bts.gov/flow
[215] "Wave Project" from the Consumer Technology Association available at https://CTA.tech/WAVE

Consumer Technology Association, it includes major streaming services and hardware manufacturers working together to ensure consistent application of existing industry standards. This collaboration has enabled different products to "speak the same language," enhancing the user experience.

Avoiding Vendor Lock-In: Concerns about being locked into proprietary technologies hinder IoT adoption. Interoperability and standardization, as seen in the Wi-Fi and cellular industries, do not stifle innovation but rather promote it, as the IEEE 802 and cellular industry standards proved. Ensuring products work together benefits both established companies and startups, preventing infrastructure obsolescence.

Surveying Standards: Before promoting specific standards, government agencies should survey available and relevant standards, protocols, and models tailored to specific application areas like smart homes or IoMT. This survey will help in setting federal recommendations or requirements for taxonomies of standards in federally funded projects, encouraging industry adoption and standardization.

Promoting IoT interoperability through consistent standards will enhance device compatibility, foster innovation, and prevent vendor lock-in. This approach will increase technology adoption, reduce obsolescence risks, and create a more competitive market, benefiting both consumers and enterprises.

Enabling Recommendation ER2.2.1: The Executive Branch should facilitate interoperability through the development of a consistent data taxonomy for the sharing and exchange of transportation, traffic and other data collected from IoT and non-IoT sources.

Supported by Findings 11, 15, and 21.

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.

The federal government should work with various organizations across the broader transportation ecosystem to facilitate interoperability through the development of a consistent data taxonomy that allows for the sharing and exchange of traffic and other data collected from IoT and non-IoT sources.

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. Projects involving multiple jurisdictions and requiring federal funding should specify the development of a data taxonomy that can be further used and developed by these jurisdictions. It's also important to engage with appropriate industry associations.

Enabling Recommendation ER2.2.2: The Executive Branch should promote and adopt industry-led standards, guidelines, and protocols for IoT technologies to the greatest extent possible.

Supported by Findings 1 and 11.

Industry standards and protocols ensure that devices from different manufacturers can communicate and work together seamlessly to deliver desired functionality and outcomes. For example, safety is a critical outcome in transportation systems. Standardization (especially for security and interoperability needs) ensures that devices can communicate basic safety information to other vehicles and to/from infrastructure. In public safety, standardization ensures that organizations from different jurisdictions can communicate with each other to support region-wide incidents. In healthcare, standardized solutions lead to timely communication of information and actions that lead to proper patient care and safety.

However, despite the development and availability of open standards developed collaboratively by industry participants, solution makers continue to use proprietary standards. This may be attributed to buyers not demanding standards-based solutions, as well as solutions makers not financially incentivized to adopt standards. In a global marketplace where open standards are increasingly adopted, the limited adoption of standards-based solutions by industry creates fragmented markets and will the global competitiveness of U.S. solution makers.

Some examples include:

- 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 onboard, 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, the U.S. 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, the U.S. rail industry could lose competitive advantage in an increasingly global market.

In some industries, 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.

The federal government should advocate and promote the adoption of industry-led and open standards. Some examples of possible actions to consider include, but not limited to:

- Acknowledge and recognize industry-led and open standards.
- Procure technologies that are interoperable and built to consensus standards for its own use.
- Specify interoperability and consensus industry standards in projects funded by federal funds and grants.
- In the case of ITxPT example, DOT should recognize it as a critical and emerging technology, similar to 5G, and incentivize compliance as a requirement within federal grant programs.
- In the case of the PTC example, the Federal Railroad Administration should consider evolving PTC regulations to allow PTC using 5G FRMCS. They could recognize it as a critical and emerging technology and even incentivize compliance as a requirement within federal grant programs.

A relevant example in the transportation sector is a standard that NEMA has published for connected vehicle infrastructure. Connected Vehicle Infrastructure focuses on communications and connectivity between vehicles and related roadside infrastructure. There was a gap related to a lack of uniformity between roadside infrastructure devices and OEM vehicles interpreting basic safety messages. The NEMA TS 10 standard addressed that gap by standardizing a minimal set of messages with a uniform interpretation for safety applications (i.e., emergency vehicle preemption, entering school zone, entering work zone, pedestrian crossing ahead). Manufacturers of roadside infrastructure are free to add additional functionality, but the minimum requirements for interoperability and safe operation are described in the NEMA TS 10 standard.[216] State DoTs can simply call out NEMA TS 10 in a procurement specification allowing for competitive bids from the relevant manufacturers.

Connectivity

Key Recommendation KR2.3: The Executive Branch should expand and improve programs that ensure sufficient availability, reliability, quality of service and connectivity to support IoT in all areas of the country.

Supported by Findings 1, 12, and 16.

IoT and other smart equipment require connectivity to communicate and send data to edge servers and remote data centers in the cloud for processing and storage. However, connectivity is still not ubiquitous nor freely available today. There are still parts of the U.S., many of them rural and tribal communities, where broadband infrastructure is not available. Furthermore, there are large areas of the country, including forests, deserts, coastal and littoral regions, and the open sea that are remote and unconnected. These unconnected areas of land and sea offer many opportunities for IoT.

[216] "Connected Vehicle Infrastructure – Roadside Equipment" from National Electrical Manufacturers Association available at https://www.nema.org/standards/view/connected-vehicle-infrastructure-roadside-equipment

Other communities, including those in underserved urban areas, may have old infrastructure that must be upgraded to provide affordable services and to support advanced IoT applications and services.

In addition to bringing broadband to underserved rural and remote areas, improving wireless coverage in the actual areas where the IoT devices and systems are operating is critical. For example, IoT in agriculture requires that the sensors in the field, or the "last acre" be connected. This is a major challenge as farms occupy vast stretches of land, with the largest farm in the United States spanning 190,000 acres. Bringing broadband to the farmhouse doesn't address the need to connect the sensors in the field. Besides agriculture, other applications where "last acre" coverage is needed include environmental monitoring, forest monitoring and management, rural emergency services, remote infrastructure monitoring (electrical, oil pipelines, water infrastructure) and wildlife conservation. Another area, although not land-based, is ocean transport and offshore oil rig operations.

Multiple approaches are needed to enable the ubiquitous connectivity needed to support IoT. as there is no "one size fits all" approach. Some IoT applications require services to support high bandwidth applications, while others require low bandwidth methods. Existing approaches have strengths but also challenges. These include:

- Fiber infrastructure provides high capacity, but can be expensive, especially for rural areas, takes relative longer to deploy and may not reach all areas.
- Service from wireless carriers and operators can be a solution but the lack of sufficient financial returns may prevent wireless operators from entering rural and tribal communities with low population densities.
- Geosynchronous satellite broadband service offers coverage over wide areas but suffers from latency and interference challenges.
- Low Earth Orbit (LEO) broadband satellites offer low latency service but require high investments to build and face complexities in managing multi-satellite fleets.
- Niche methods, such as TV White Spaces and Power Line Communications, have limited applicability in certain gap-filler applications.

As IoT evolves, as described in this report, the capabilities of the connectivity services must evolve to not only the massive number of devices, but to accommodate future applications. For example, while many use cases, including condition monitoring and asset tracking, will continue to be supported by low bandwidth connectivity services, future IoT applications will increasingly involve autonomy, robotics, computer vision and large amounts of sensor data. These applications require a stable and continuous connection, higher bandwidth, low latency, and symmetric upload and download speeds. To support future IoT needs, a number of connectivity considerations need to be addressed. These include service bandwidth, spectrum allocation, new connectivity technologies to support IoT at scale, energy efficiency, interference and advantages that may be provided by sixth generation (6G) technology.

The federal government should take a broader perspective of the various connectivity needs to enable and support the various and diverse IoT applications and across the United States now and in the future. It should expand its current programs and initiatives by considering new and innovative approaches to closing the connectivity gap. For example, California is facilitating the creation of new private sector "last mile" services in underserved areas by building a $6 billion middle mile fiber network (SB 156).[217] Satellite services, especially those from low earth orbit systems, should be taken into consideration as part of the overall IoT connectivity strategy and planning. Niche approaches should be considered as viable alternatives in geographic regions where traditional methods may not be feasible.

Enabling Recommendation ER2.3.1: The Executive Branch should promote continued U.S. leadership on spectrum policy by continuing to make licensed and unlicensed spectrum available via spectrum sharing, repurposing underutilized federal spectrum and spectrum auctions.

Supported by Finding 3.

As IoT adoption grows, spectrum concerns emerge. A 2017 U.S. Government Accountability Office report stated that "rapid increases in IoT devices that use large amounts of spectrum, called high-bandwidth devices, could quickly overwhelm networks, as happened with smart phones."[218] Similarly, potential interference issues emerge for low bandwidth devices operating in the unlicensed IoT frequency bands as additional devices come online. While not an immediate concern with the FCC, growth of high bandwidth IoT applications and low bandwidth unlicensed band devices will require the allocation of additional spectrum.[219]

[217] California All Middle Mile Broadband Initiative from California Department of Technology available at https://middle-mile-broadband-initiative.cdt.ca.gov/

[218] "Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available," Report to Congressional Requesters GAO 18-71, U.S. Government Accountability Office, November 2017. https://www.gao.gov/assets/690/689024.pdf

[219] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

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 underutilized 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.[220] The technology industry uses both licensed and unlicensed spectrum to enable this growth. Spectrum availability should not become a choke point in this growth. The FCC should continue to monitor and forecast the growth of IoT, especially the growth of autonomous IoT, video and other high bandwidth applications, and make spectrum as necessary.

A component of the government's toolkit for enhancing spectrum availability is the sharing of existing spectrum among stakeholders, "spectrum sharing". The FCC has enabled several models of dynamic spectrum sharing. This is a helpful tool when utilizing the spectrum whether existing private sector bands, or underutilized federal spectrum.

Repurposing underutilized federal spectrum is also an ongoing and important effort. However, there is an obstacle in repurposing spectrum to 6G.

Since 1993, the FCC has had authority to auction spectrum through competitive bidding, unlocking thousands of megahertz of spectrum and powering each new generation of wireless technology. In 2023, Congress allowed the FCC's auction authority to lapse. Without this authority, a major tool in the U.S. government's toolkit for enhancing IoT connectivity through spectrum access is lost: FCC authority to open up spectrum for commercial purposes via auction. By restoring the FCC's auction authority, Congress can get the agency back to making additional spectrum available for commercial use, including for IoT applications. Additional spectrum will power future generations of wireless connectivity including 6G. This capability will be important for mobile-connected IoT devices and applications such as precision agriculture.

Unlicensed spectrum is also widely used in connected devices and needs its own priority. An example list of unlicensed spectrum applications is described in a recent report.[221]

Enabling Recommendation ER2.3.2: Congress should increase funding and accelerate implementation of broadband deployment across rural America.

Supported by Findings 12, 16, 19, 20, 22, and 23.

Coverage is one of the most significant barriers to IoT adoption and operation. Rural areas are home to farms, factories and people that would benefit from precision agriculture, remote healthcare monitoring and smart manufacturing. Energy infrastructure, such as solar and wind generation plants, electrical grid infrastructure and oil pipelines and oil rigs operate in remote areas and are heavy users of IoT technologies. Mining operations, carried out in remote areas, benefit from using IoT applications to manage operations, equipment maintenance and worker safety.[222] A Michigan based economic development organization stated the lack of broadband access threatens the ability of its rural based manufacturing companies to compete with companies that employ industry 4.0 technologies.[223]

A United States Department of Agriculture (USDA) report estimated that realizing the full potential of rural broadband and next generation precision agriculture technologies, could lead to "$47–$65 billion annually in additional gross benefit for the U.S. economy."[224] Beyond economics, rural broadband can helps improve health outcomes of rural Americans. According to the Washington Post, the federal government has designated 80% of rural areas in the U.S. as "medically underserved". These "medical deserts" are home to 20% of the U.S. population, but only 10% of the doctors.[225] According to the U.S. Centers for Disease Control and Prevention (CDC), Americans living in rural areas face health disparities when compared to their urban counterparts. These residents are "more likely to die from heart disease, cancer, unintentional injury, chronic lower respiratory disease and stroke than their urban counterparts."[226]

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

[221] "Unlicensed Spectrum and the U.S. Economy: Quantifying the Market Size and Diversity of Unlicensed Devices" from the Consumer Technology Association available at https://shop.cta.tech/collections/research/products/unlicensed-spectrum-and-the-us-economy-quantifying-the-market-size-and-diversity-of-unlicensed-devices

[222] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[223] "Lack of Broadband Access Threatens Rural Manufacturers' Ability to Compete" from MiBiz (January 20, 2019) available at https://www.crainsgrandrapids.com/news/manufacturing/lack-of-broadband-access-threatens-rural-manufacturers-ability-to-compete/

[224] "A Case for Rural Broadband" from the U.S. Department of Agriculture (April 2019) available at https://www.usda.gov/sites/default/files/documents/case-for-rural-broadband.pdf

[225] E. Saslow, "'Out here, it's just me': In the medical desert of rural America, one doctor for 11,000 square miles," Washington Post (September 28, 2019) available at https://www.washingtonpost.com/national/out-here-its-just-me/2019/09/28/fa1df9b6-deef-11e9-be96-6adb81821e90_story.html

[226] "About Rural Health", Public Health Infrastructure Center, U.S. Centers for Disease Control and Prevention (May 9, 2023) available at https://www.cdc.gov/rural-health/php/about

Many rural areas lack broadband service and cellular coverage. The U.S. Federal Communications Commission (FCC) 2020 Broadband Deployment Report, estimated that 22.3% of the 50 million people who live and work in rural areas, have no coverage for 25/3 Internet service at the end of 2018.[227] The actual number of people in rural areas without broadband Internet service is likely higher than reported. Although the FCC broadband report states that 77.7% of the rural population have 25/3 coverage available, that does not imply that they have subscribed to service in their homes or businesses.

In addition, the FCC relies on self-reported data, through Form 477, provided by the telecommunications carriers and Internet service providers to build their broadband coverage maps. These data, however, have been found to overstate the actual broadband coverage. One study found that instead of 24.7 million people not having access to 25/3 Internet service, as many as 160 million people do not have access to this level of service.[228]

Mobile LTE connectivity service, from wireless telecommunications providers, is used by residents and businesses as an alternative to fixed terrestrial services. While 10/3[229] service does not meet the benchmark for "advanced telecommunications capability," the FCC broadband report in 2020 found that 16.7% of people living and working in rural areas do not even have 10/3 coverage availability.[230]

The federal government currently offers limited funding and grants (e.g., Department of Agriculture – Community Connect Grant Program) to help fund broadband deployment in rural communities. However, current federal funding operates across several programs making it difficult to identify and find the opportunities available to specific areas. In addition, these funding opportunities have not significantly advanced quickly enough to provide broadband coverage for certain areas of rural America. While the Bipartisan Infrastructure Law has set aside funding for deploying broadband to rural and underserved communities, the funding is insufficient to bring connectivity to every rural community that needs it.

The federal government should aggressively promote and advocate for accelerated broadband infrastructure buildout and deployment across all rural areas. Furthermore, the federal government should consider and integrate a variety of connectivity approaches, such as low earth orbit (LEO) and geostationary satellite, fixed wireless, and niche methods (TV White Spaces, etc.) as part its accelerated buildout planning and initiatives. Finally, these approaches should take into account "last acre" connectivity needs to support IoT applications on vast unconnected areas, such as farming, forest and environmental monitoring, and remote infrastructure monitoring.

Enabling Recommendation ER2.3.3: The Executive Branch should actively promote and support the adoption of satellite narrowband IoT systems to support "last acre" IoT in rural and remote areas.

Supported by Findings 12, 16, and 19.

In addition to bringing broadband to rural and remote areas, wireless coverage in the actual areas where the IoT devices and systems are operating is critical. For example, IoT in agriculture requires that the sensors in the field, or the "last acre" be connected.[231] This is a major challenge as farms occupy vast stretches of land, with the largest farm in the United States spanning 190,000 acres.[232] Bringing broadband to the farmhouse doesn't address the need to connect the sensors in the field. Besides agriculture, other applications where "last acre" coverage is needed include environmental monitoring, forest monitoring and management, rural emergency services, remote infrastructure monitoring (electrical, oil pipelines, water infrastructure) and wildlife conservation. Another area, although not land-based, is ocean transport and offshore oil rig operations.

Existing and emerging satellite-based IoT connectivity services provide a reliable and efficient means of connecting IoT systems in rural agricultural areas, tribal lands, and remote areas (forests, deserts, etc.) where traditional terrestrial connectivity options may be limited or unavailable.

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

[227] "2020 Broadband Deployment Report". FCC 20-50, Federal Communications Commission (April 24, 2020), Page 19 available at https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2020-broadband-deployment-report

[228] C. Mihalcik, "Microsoft: FCC's Broadband Coverage Maps Are Way Off" from CNET (April 19, 2019) available at https://www.cnet.com/tech/services-and-software/microsoft-fccs-broadband-coverage-maps-are-way-off/

[229] 10 Mbps down, 3 Mbps up

[230] "2020 Broadband Deployment Report", FCC 20-50, Federal Communications Commission (April 24, 2020), Figure 2b. https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2020-broadband-deployment-report

[231] Precision Agriculture Connectivity Task Force, "Examining Current and Future Connectivity Demand for Precision Agriculture", Interim Report of the Federal Communications Cmmission (December 2022), Page 2 available at https://www.fcc.gov/sites/default/files/connectivity-needs-anticipating-demand-interim-12022022.pdf

[232] E. O'Keefe, "Top 5 Farms with the Largest Acreage in the U.S.", from *Successful Farming* (September 28, 2019) available at https://www.agriculture.com/farm-management/farm-land/top-5-farms-with-the-largest-acreage-in-the-us

their operations through real-time data management, resulting in benefits for various stakeholders, including farmers, policymakers, agricultural companies, utility companies, medical personnel, and consumers.

The federal government should promote and advance satellite IoT connectivity approaches in order to advance IoT adoption in the United States. This includes such actions as:

- Harmonize standards for satellite narrowband IoT to ensure reliable and consistent operation to support applications such as agricultural applications and environmental monitoring needs.
- Establish a public-private-academia partnership that involves satellite service providers, IoT technology companies, agriculture data-platform providers, agricultural extension centers, research institutions, and relevant government agencies to support the development, implementation, and adoption of satellite IoT systems in agriculture and other applications.
- Define specific agricultural applications, develop financial incentives and subsidies, and provide incentives or subsidies to facilitate the adoption and integration of satellite IoT systems by farmers and agricultural businesses.
- Promote education and training by creating 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 agricultural extension centers, universities, and industry experts.

Key Recommendation KR2.4: The Executive Branch should encourage businesses and organizations to embark on initiatives to digitalize and transform their operations and processes in order to take advantage of IoT and the IoT-enabled economy.

Supported by Findings 14, 16, and 17.

IoT systems do not exist as standalone systems in an enterprise but are tightly integrated into a business's operations and technology systems. For example, a smart streetlight employs connected sensors to detect if a streetlight is functioning properly. The streetlight status data is sent directly to the utility company's back-office systems. Upon detection of a failed streetlight, the operations system opens a repair ticket and routes the ticket to the workflow system, which checks the nearest parts depot for inventory, assigns a technician and date, and moves inventory to a work staging area ahead of the repair date. In order to maximize the benefits provided by IoT, the organizations must undergo digital transformation – operations and policies are re-engineered and digitized for efficiency, and information technology systems updated and modernized to support new capabilities.

However, many organizations today still have legacy processes and systems that hinder their ability to integrate IoT their operations. This prevents the organizations from fully thriving, as well as supporting and realizing the benefits offered by IoT and other digital innovations. The digitalization of business functions (e.g., design, production, marketing, procurement, distribution) enables more efficient and responsive IoT management, greater operational visibility, and transparency over supply chains to track products, monitor quality, and fix issues or defects. Using cryptographic methods can improve IoT security, reliability, integrity, and trust of data produced in supply chains and edge applications supporting those business functions.

The federal government should consider incentives (financial and other) to encourage businesses to digitalize their operations. Examples of possible incentives may include grants, loans, tax credits, subsidies, education, and access to digital and technical resources. In providing incentives and subsidies for businesses to adopt digital tools and digitize their operations, the federal government can facilitate the development of more efficient and agile organizations, as well as facilitate the development of ecosystems and platforms to create the IoT-enabled economy as discussed in the "IoT-enabled Economy" section above. Furthermore, digitalization initiatives enable digital transformation of an organization's operations, whereby IoT device suppliers become connected to their customers to enable new business models and services revenue streams. This ultimately create opportunities for businesses and workers, which will drive economic growth. Small businesses, with their limited scale and capabilities, benefit most from digital transformation. The government should work with industry stakeholders to develop and communicate clear guidelines and criteria for eligibility of subsidies and incentives for digitalization.

Digitalizing business functions enhances IoT management and supply chain visibility, improving security and data trust. Government incentives can drive economic growth by promoting digital tools, creating new business opportunities, and enabling new revenue streams. Collaborative guidelines and proof of concept (PoC) projects will facilitate adoption and best practices.

Agencies may encourage orchestrated PPPs to work on larger scale, industrywide or cross-country type of proof of concept (PoC) projects to assess the economic value of the digitization of operations and processes before investing in solutions to deploy at scale. These PoC projects can demonstrate the return on

investment to the partners but also what the broader national economic benefits might be. As those PoC projects progress, the government could help monitor the progress of those partnerships, encourage businesses to invest in digitalization and adopt digital technologies and tools, and support knowledge sharing to promote best practices.

Enabling Recommendation ER2.4.1: The Executive Branch should facilitate the creation of IoT business ecosystems that enable new business models and revenue streams.

Supported by Finding 14.

As data produced across IoT networks become the *"new gold"*, the government should raise awareness about the value of trusted data business ecosystems and digital threads that 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 XaaS business models.

The federal government should promote programs that educate and raise awareness on Data Monetization Strategies, Data Analytics, Digital Marketplaces, Platform-based Business Ecosystems, Network Effects, and Digital Threads in connected supply chains, regulations, and tools for Monitoring and Managing Data Marketplaces. Promotion can be through convening conferences of stakeholders to share results and best practices, making available open-source tools, and development of model strategies and policies among other efforts.

These include:

- **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 while business ecosystems lead to better products, solutions, and services that enable new revenue streams.
- **Platform-based business ecosystems** of connected enterprises that can collaborate and innovate more effectively. They can also scale rapidly through network effects and can drive sustainable growth for businesses.
- **Data policies** that can provide a framework for businesses to manage and use confidential data responsibly and use tools for monitoring and managing trusted digital marketplaces that ensure transparency and accountability.
- **Awareness and Education** with development of educational programs (e.g., through public campaigns, conferences, and workshops) for businesses and individuals to raise awareness about business ecosystems.

The government should encourage IoT business ecosystems to enable new business models and revenue streams. By creating interconnected networks of businesses and technologies, these ecosystems can enhance products, enable digital twins, and drive growth through XaaS models. Educational programs on data monetization, analytics, digital marketplaces, and platform-based ecosystems will foster innovation, improve decision-making, and promote sustainable growth.

Enabling Recommendation ER2.4.2: The Executive Branch should lead collaboration with international allies to develop, promote and adopt a Global Digital Identifier that can link to Local Identifiers of businesses, products, and data, to enable cross-border trade, supply chain resilience, and ultimately trusted digital marketplaces.

Supported by Findings 5, 6, 9, 15, and 25.

The U.S. (including the Office of the United States Trade Representative (USTR)) should lead a collaboration with the EU and allied nations[233] to develop, promote and adopt a secure cross-border Global Digital Identifier to facilitate trade of goods and related data. A global standard like the Universally Unique Identifier[234] (UUID) but optimized for this purpose, can accelerate the use of IoT by providing a unique, standardized way to identify assets across wireless networks, supply chains. They can enhance cross-border trade, supply chain resilience and strengthen economic security while safeguarding data privacy and confidentiality.

Geopolitical tensions impact trade, supply chain resilience, and economic security, especially concerning imports of key commodities or technology leakage exploited by adversaries. To safeguard our economy and balance supply and demand, the government should create incentives for market preference by monitoring imports of essential goods like pharmaceuticals,

[233] The U.S.-E.U. TTC should be renewed and can lead with trade agreements to adopt industry consensus standards.

[234] "Universally Unique Identifiers (UUIDs)" from the Internet Engineering Task Force (March, 2024) available at https://datatracker.ietf.org/doc/html/rfc9562

or the use of critical components like chips, which are at the core of our critical infrastructure and IoT and AI advancements.

Market preference can be ensured through trusted traceability of businesses, products and data, and connectivity networks while preserving user privacy and enterprise confidentiality. To achieve this, allied nations must agree on a Global Digital Identifier standard capable of cryptographically linking to Local Identifiers of businesses, products, and data leveraging existing standards and infrastructure.

A technical standard will be required and should be developed by the usual voluntary industry consensus standards process. The identifier must be standardized as globally unique, electronically verifiable, cryptographically secure, traceable to a root of trust and capable of supporting varying levels of authentication. It should be retrievable in a standardized method such as a documented API. As the identifier becomes available, it may be linked to existing regional standards like the Cyber Trust Mark, the Digital Product Passport, and Business Identifiers used by Custom and Border Protection agencies. The Global Identifier may also be linked to local identifiers that may carry metadata pointing to businesses, assets, and data that can be shared at the producer's discretion or a private transaction.

Global Identifiers linked to Local Identifiers will enable supply chain visibility and product/data "traceability", ultimately providing opportunities of improved trust and confidence in businesses, their processes, IoT products and ultimately data related to them, which the IoT ecosystem will need to operate. By incentivizing producers and consumers to use Identifiers and metadata that enables information exchange (with producers determining the level of data sharing), this can foster trusted digital marketplaces and fuel the digital economies in the long run.

Establish Trust in IoT

Establishing trust in IoT is crucial for widespread adoption and public confidence. Secure, private, and reliable operation of interconnected devices is essential to achieve such trust. Key Recommendations include NIST continuing to provide specific and consistent cybersecurity guidance for IoT providers and adopters, Congress passing comprehensive federal privacy legislation to protect user data across all IoT applications, and the Executive Branch supporting trusted IoT architectures and infrastructure to ensure supply chain provenance and traceability.

Objective 3: A collaborative and continuous effort among government, industry and academia employing a multitude of approaches, from technical to policies and legislation, is necessary.

The U.S. has an opportunity to increase trust and confidence in IoT. While IoT provides powerful benefits and outcomes, trust challenges hinder the broader adoption, use and realization of those benefits. Trust is earned and kept when IoT devices and systems remain secure from unauthorized access, data is kept safe and used as intended, algorithms are accurate and explainable, and produced outcomes are safe, consistent, and reliable. Threats to trust are continuous and come from a variety of ways, some known and others yet to be discovered. This Objective calls for a collaborative and continuous effort between government, industry and academia employing a multitude of approaches, from technical to policies and legislation. This effort is necessary to ensure trust in IoT.

Cybersecurity Improvement

Key Recommendation KR3.1: NIST should continue to provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach.

Supported by Findings 1 and 8.

While not the exclusive source of cybersecurity guidance, NIST should continue to be recognized as a developer of outcome-based requirements that inform industry consensus standards, and industry should continue to be recognized 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 ER3.1.1: The Executive Branch 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.

Supported by Findings 1, 7, 8, and 25.

This recommendation to strengthen cybersecurity measures focused on IoT across supply chains, and networks for IoT products addresses the growing concerns around IoT data privacy, confidentiality, and 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 chains and networks, the government can foster trust in IoT technologies and enable businesses to fully leverage their potential benefits while minimizing risks.

Enabling Recommendation ER3.1.2: The Executive Branch should consider additional ways to highlight the vulnerabilities most likely to be applicable to IoT product developers.

Supported by Finding 8.

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,[235] use,[236] and for specific sectors.[237]

The government also maintains vulnerability lists, including the National Vulnerability Database (NVD) maintained by NIST[238] and the Known Exploited Vulnerabilities Catalog (KEV Catalog) maintained by CISA.[239]

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. A public forum that aggregates and highlights vulnerabilities for IoT developers ensures that they can effectively address known security issues, enhancing the security and reliability of IoT products. This approach helps prevent potential cyberattacks, protects user data, and builds trust in IoT technologies, ultimately fostering wider adoption and innovation in the IoT market.

Enabling Recommendation ER3.1.3: Congress should study the impacts of quantum computing and post-quantum cryptography on IoT cybersecurity.

Supported by Findings 8 and 10.

Traditional encryption methods rely on the difficulty of certain mathematical problems, like factoring large numbers or solving discrete logarithms, to remain secure and protect data. The rapid emergence of quantum computing poses significant challenges to cybersecurity. One key concern is that "quantum computers have the potential to bypass the encryption locks that currently protect the world's communications and data."[240]

[235] "Internet of Things (IoT) Acquisition Guidance Document" from the Cybersecurity and Infrastructure Security Agency available at https://www.cisa.gov/resources-tools/resources/internet-things-iot-acquisition-guidance-document

[236] "Securing the Internet of Things (IoT)" from the Cybersecurity and Infrastructure Security Agency (February 1, 2021) available at https://www.cisa.gov/news-events/news/securing-internet-things-iot

[237] "The Internet of Things: Impact on Public Safety Communications" from the Cybersecurity and Infrastructure Agency (March 2019) available at https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper_3.6.19%20-%20FINAL.pdf

[238] "National Vulnerability Database" from the National Institute of Standards and Technology available at https://nvd.nist.gov/vuln/Vulnerability-Detail-Pages

[239] "Known Exploited Vulnerabilities Catalog" from the Cybersecurity and Infrastructure Agency available at https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[240] S. Torkington, "Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding" from World Economic Forum (April 23, 2024) available at https://www.weforum.org/agenda/2024/04/quantum-computing-cybersecurity-risks/

As quantum computing matures, traditional encryption methods are rendered obsolete, leaving IoT devices and their data vulnerable to interception and manipulation. A classical computer looking to "crack" RSA-2048 encryption would on the order of 300 trillion years due to one very slow step (that of "factoring" a very large number); a sufficiently powerful quantum-enabled computing system running Shor's Algorithm is expected to do it in on the order of hours.[241]

IoT devices are particularly vulnerable to the risks posed by quantum computing. IoT devices often operate in environments with limited computational and energy resources, making them ill-equipped to handle the sophisticated encryption algorithms required to resist quantum attacks. Additionally, the sheer scale and diversity of IoT deployments make it challenging to implement security updates and patches uniformly across all devices. As a result, cybercriminals could exploit vulnerabilities in IoT devices to gain unauthorized access to sensitive data or launch large-scale attacks, potentially causing widespread disruption and damage. Current research on post-quantum cryptography (PQC) algorithms does not take into account low-power, low-complexity, low-compute-footprint devices that are common in IoT.

To prepare for the eventual post-quantum environment, the executive and legislative branches of the federal government should study the impact of quantum computing on IoT and identify appropriate actions and plans.

In addition to the study, the federal government should consider the following actions:

- Incorporate quantum computing and post-quantum cryptography considerations in the development of the national IoT strategy.
- Incorporate IoT considerations into the quantum strategy.
- Plan and prepare industries and organizations to train the workforce and achieve the transition to post-quantum cryptography.
- Promote industry awareness of post-quantum considerations to IoT developers and users.
- Develop plans to facilitate the transition to post-quantum for IoT devices and systems used by the federal government, as well as those using federal funds to procure IoT devices and IoT-enabled systems.
- Need for federal government to plan to transition and implementation of measures for its systems for a post-quantum world.
- Need to plan/prepare address post-quantum for critical infrastructure.
- Support research on development of quantum-safe cryptographic methods for resource and power-constrained environments typical of IoT devices and systems.

Studying the impacts of quantum computing and post-quantum cryptography is crucial for safeguarding IoT devices and data. As quantum computing advances, traditional encryption methods will become obsolete, making IoT systems vulnerable to cyberattacks. This research will help the federal government develop strategies to protect against these threats, ensuring the security and resilience of IoT deployments. The study will promote the integration of quantum considerations into national IoT strategies, facilitate workforce training for the transition to post-quantum cryptography, and raise industry awareness. Additionally, it will support the development of quantum-safe cryptographic methods tailored to the resource-constrained environments typical of IoT devices, ultimately protecting critical infrastructure and maintaining the integrity of sensitive data.

Enabling Recommendation ER3.1.4: The Executive Branch should accelerate the promotion and adoption of IoT technologies to enhance the electric grid's security, reliability, and resilience.

Supported by Finding 8.

The federal government should accelerate the promotion and adoption of procedures and methods that include IoT technologies that make the electric grid more reliable and resilient. Widespread, sustained power outages have become markedly more common due to severe weather as well as aging infrastructure. Grid infrastructure is also vulnerable to cyberattacks, physical incidents, and existential threats (e.g., Electronic Magnetic Pulse (EMP)).

There are areas in the country where the grid is already overloaded making it impossible to integrate energy from renewable sources. These renewable energy sources, such as solar and wind, incorporate the use of technologies enabled by IoT, such as smart inverters and energy storage systems. IoT technologies can also help make the grid more resilient.

A more reliable and resilient grid can provide the following:

- **Incorporation of technologies enabled by IoT:** These renewable energy sources, such as solar and wind, incorporate

[241] Marin Ivezic, "Q-Day Predictions: Anticipating the Arrival of Cryptanalytically Relevant Quantum Computers (CRQC)" from Post Quantum (July 27, 2023) available at https://postquantum.com/post-quantum/q-day-crqc-predictions/

the use of technologies enabled by IoT, such as smart inverters and energy storage systems. So, if we cannot get renewable energy projects integrated due to an overloaded grid, we are by default, holding back on the application and expansion of IoT in renewable energy industry.

- **Restoration:** A more reliable and resilient grid can recover quickly from threats both natural and human caused and get power back on one for families and communities. IoT Technologies can help make the grid more resilient.
- **Energy Efficiency:** There is more efficient transmission of electricity. Utilities also benefit from reduced peak loads, and the ability to increase integration of renewable energy sources.
- **Cost Reduction:** There are reduced operations and management costs for utilities. Consumers can also better track and manage their energy consumption, thereby lowering their energy costs as well.

IoT considerations could be included in existing or planned federal initiatives, such as the recently announced Department of Energy $48 million program to improve the reliability and resiliency of America's Power Grid.[242]

There are several near-term technologies that can provide solutions in the short term at a much lower expense. These include Dynamic Line Ratings, Volt/Var, Power-Flow Controllers, Energy Storage, Distributed Energy Resources, and Demand Response.

Microgrids can strengthen grid resilience and reliability with their ability to operate while the main grid is down and function as a grid resource. Promoting IoT adoption will improve its reliability and resilience, enabling better integration of renewable energy, enhancing energy efficiency, and reducing costs. This will result in a more secure and robust power infrastructure, enabling economic growth and sustainability.

Enabling Recommendation ER3.1.5: Congress and the Executive Branch should support domestic IoT cybersecurity labeling initiatives by establishing incentives for manufacturers to participate.

Supported by Finding 8.

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.

Congress can support three direct initiatives: 1) directly enact an "earned safe harbor" that includes protection for program participants from civil actions; 2) establish preemption of mismatched state laws for program participants; and 3) ensure adequate funding for a robust consumer education campaign.

Additionally, 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.

Enabling Recommendation ER3.1.6: Congress must ensure adequate and ongoing funding for the Cyber Trust Mark consumer education campaign.

Supported by Finding 8.

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 (PSA) 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 Energy Star is required. For this, Congress must step in to ensure

[242] https://www.energy.gov/articles/us-department-energy-announces-48-million-improve-reliability-and-resiliency-americas

adequate and continuing funding for a consumer education campaign.

Enabling Recommendation ER3.1.7: The Executive Branch should establish appropriate U.S. representation regarding international harmonization of IoT cybersecurity programs and requirements as such programs are established for domestic market sectors.

Supported by Finding 8.

The U.S. Department of State must prioritize supporting the FCC as the U.S. Trust Cyber Trust Mark program owner, NIST, and private sector stakeholders for the U.S. Trust Mark 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 arrangement between the U.S. and the EU. In October 2023, the two governments released a Joint Statement on a Joint Cybersafe Action Plan. 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."[243]

Subsequently, the Biden Administration announced a roadmap to that end.[244] 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 ER3.1.8: The Executive Branch should recognize and promote existing standards and conformity assessment schemes that facilitate cybersecurity in industrial IoT applications.

Supported by Finding 8.

The U.S. Cyber Trust Mark program is specific to consumer IoT. 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 such program. These standards and certification programs provide a systematic, practical, and holistic approach to addressing cybersecurity.

These existing standards and conformity assessment schemes can demonstrate cybersecurity compliance by a number of methods based on 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. National Cybersecurity Center of Excellence (NCCoE) or similar public-private agency groups should be considered for programs to highlight usage of selected standards. Further, international harmonization and alignment should be pursued to the greatest extent possible.

[243] "U.S.-E.U. Summit Joint Statement" from the White House (October 20, 2023) available at https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/20/u-s-eu-summit-joint-statement

[244] Adam Mazmanian, "EU signs on to IoT safety label plan" from NextGov/FCW (January 12, 2024) available at https://www.nextgov.com/cybersecurity/2024/01/eu-signs-iot-safety-label-plan/393328/

Data Privacy Policy and Regulation

Key Recommendation KR3.2: Congress should pass comprehensive federal privacy legislation.

Supported by Findings 3 and 7.

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 interagency cooperation. Several agencies could be pivotal in championing this recommendation, including the FTC, the Department of Commerce, and the House Committee on Energy and Commerce.

Enabling Recommendation ER3.2.1: Congress should include IoT in proposed comprehensive privacy legislation.

Supported by Findings 3 and 7.

To enhance privacy standards and foster innovation in the rapidly evolving realm of the Internet of Things (IoT), the U.S. government should include IoT considerations, including IoT data retention and transparency, in any future proposed Federal privacy regulations. 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.

Enabling Recommendation ER3.2.2: The Executive Branch should promote "Privacy by Design" in IoT device development, deployment, and implementation.

Supported by Finding 7.

In the realm of IoT, the U.S. government is encouraged 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 concerns 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. It should be noted that cybersecurity technology supports privacy policy, in the "confidentiality" element of the cybersecurity triad of confidentiality, integrity and availability. Therefore, the government should also continue to leverage the National Cybersecurity Strategy Implementation Plan to drive the development of secure-by-design technology through public-private partnerships.

Enabling Recommendation ER3.2.3: Congress and the Executive Branch should establish clear policies for third-party data sharing and IoT device data use.

Supported by Findings 3 and 7.

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.

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 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 ER3.2.4: Congress and the Executive Branch should encourage the use of plain language in IoT privacy policies.

Supported by Findings 3 and 7.

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.

For effective implementation, the U.S. Federal government should consider creating contractual requirements for IoT providers to implement simplified privacy policies in government procurement. 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 ER3.2.5: Congress and the Executive Branch should develop and implement privacy transparency mechanisms.

Supported by Finding 7.

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, will empower various stakeholders – businesses, governments, and consumers – by providing them with detailed insights into the privacy features and practices of IoT devices. It will 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.

To accelerate IoT adoption and overcome regulation and interoperability challenges, perhaps the creation of IoT Sandboxes at the Federal level across application areas where component and application manufacturers, users, and consumers, as well as regulators can co-create prototype solutions to test interoperability, ensure data privacy and security, and regulatory compliance, before releasing solutions for commercial use.

Enabling Recommendation ER3.2.6: Congress and the Executive Branch should endorse universal opt-out signals for IoT devices and companion apps.

Supported by Finding 7.

In an initiative to bolster privacy and data protection for 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. Standardized guidelines or legislation may be necessary to ensure uniform adoption of the Universal Opt-Out Signals.

Concerns 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. The Department of Commerce should encourage the FTC and FCC to promote this initiative.

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 ER3.2.7: Congress and the Executive Branch should require IoT privacy information on new car automobile "Monroney Labels".

Supported by Finding 7.

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 Labels" for new and used cars. This recommendation aims to leverage the traditional role of Monroney Labels – known for detailing fuel efficiency and safety ratings – to also disclose vital information about IoT privacy. The indicators should cover whether the vehicle collects personal data, whether the personal data is sold, and whether there is an option for universal opt-out. In addition, there should be a QR code (or equivalent) pointing to an online privacy notice.

Details regarding the availability of space, viability of including these details in Monroney Labels, and the contents of the online privacy notice should be studied, consistent with the goals of this recommendation.

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,[245] which reveals that all 25 car brands reviewed in this report have privacy policies that reserve the right to collect personal data, with most reserving the right to share or sell 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.

Implementing this recommendation 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 address concerns 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 Environmental Protection Agency (EPA) 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.

While this recommendation addresses Monroney Labels, it should also be applied to equivalent notices for used vehicles.

Enabling Recommendation ER3.2.8: Congress should add "Location Tracking Enabled" disclosure to future U.S. device labeling initiatives.

Supported by Finding 7.

The federal government has considered e-labeling programs that would collect multiple disclosure opportunities under a single structure, such as a QR code. Examples may include environmental, RF emissions, or cybersecurity topics. While that concept has not yet been implemented, the opportunity remains to include location tracking disclosure in that initiative. Such a disclosure should state, "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 future e-labeling programs. It is crucial to assess the technical feasibility of how and where this notice will be

[245] This report is available at https://foundation.mozilla.org/en/blog/privacy-nightmare-on-wheels-every-car-brand-reviewed-by-mozilla-including-ford-volkswagen-and-toyota-flunks-privacy-test/

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.

Enabling Recommendation ER3.2.9: The Executive Branch should promote the use, development, and implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.

Supported by Finding 7.

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.

One element in this endeavor is addressing concerns 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.

Enabling Recommendation ER3.2.10: The Executive Branch should follow NIST sanitization standards for government automobiles before resale and encourage NIST sanitization standards for automobiles before resale.

Supported by Finding 7.

Follow NIST sanitization guidance 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.

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. NIST Special Publication 800-88 provides a foundation that can be further expanded. 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 guidance 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.

The proposal to require sanitization for resale of government automobiles 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.

Key Recommendation KR3.3: The Executive Branch should support trusted IoT architectures and infrastructure that enable supply chain provenance, and traceability of IoT systems starting from chip design and manufacturing.

Supported by Findings 5 and 6.

To ensure the integrity and reliability of IoT systems, it is crucial to support trusted IoT architectures and infrastructure that enable supply chain provenance and traceability starting from chip design and manufacturing.[246] [247] This will build trust in the data and functionality of IoT systems across the entire ecosystem.

Importance of Traceability. Chip supply chain and lifecycle traceability are essential for trusting IoT data. Every part of IoT systems, including chips and devices, must be traceable to ensure the overall integrity and trustworthiness of IoT devices and the IoT ecosystem. IoT and Identification technologies can be used to trace and authenticate supply of IoT parts and detect intrusions upon power-up, enhancing security.

Cryptographically Strong Architectures. The government should promote the creation of cryptographically strong architectures and infrastructure that enable supply chain provenance, traceability, and lifecycle management. This involves linking hardware and software bill of materials to the design and manufacturing processes of chips and IoT devices delivering trusted assets and data. As markets are flooded by Chinese commodity chips targeting our critical infrastructure and western chips are used in adversaries' weapons against allies, chip supply traceability becomes critical.

Global Leadership and Policies. The U.S. and EU can lead allied nations in formulating policies for market preference and market pull from device makers purchasing chips that are traceable and secure. This will incentivize the electronics and IoT industry to develop trusted architectures for supply chain provenance, traceability, and product lifecycle management. By cryptographically linking SBOM[248] to trusted HBOM[249] in IoT systems, industries can help mitigate the risks associated with security, compromised components, and ensure the security and reliability of critical systems.

Global Public-Private Partnerships. Cross-border collaboration among government agencies and industry stakeholders through public-private partnerships is essential. These partnerships should develop and promote trusted architectures that support secure protocols for provisioning and market access. These can be linked to Global Digital Identifiers [ER2.4.2], ensuring widespread adoption and implementation including Customs and Border Protection.

Implementing trusted IoT architectures enhances system security, ensures data integrity, and boosts the reliability of critical systems. This investment strengthens national security, public safety, and economic stability, providing significant value for both government and society. Trusted architectures for supply chain provenance and traceability are key to mitigating risks and ensuring the trustworthiness of IoT systems and provide the ability to regulate access and field use. This will strengthen national and economic security and enable root-of-trust based services and business models.

[246] Don Davidson, speaker at the IoTAB meeting in April 2023. Slide deck available at https://www.nist.gov/system/files/documents/2023/04/24/Speaker%20-%20Don%20Davidson%20-%204-19-23.pdf

[247] Harvey Reed, speaker at the IoTAB meeting in May 2023. Slide deck available at IoTAB https://www.nist.gov/system/files/documents/2023/05/23/Speaker%20-%20FY23%20NCCoE%20Supply%20Chain%20Traceability%20-%20IoT%20AB%20brief%2C%20v4%20final%20draft.pdf

[248] Software Bill of Materials for Electronic parts and Software modules used in the assembly of a device of systems.

[249] Hardware Bill of Materials must include a Root of Trust and Entropy for security and unique ID (fingerprint).

Enabling Recommendation ER3.3.1: The Executive Branch should encourage trusted digital twins and digital threads for accelerating IoT adoption across supply chains and IoT application markets.

Supported by Findings 6 and 14.

Promote the use of digital twins[250] and digital threads[251] across IoT ecosystems, to accelerate adoption and deployment of IoT systems and infrastructure. Leverage digital threads of data across value chains to enable marketplaces of trusted data producers and data consumers. This can accelerate the adoption and growth of IoT systems across disaggregated supply chains and IoT vertical markets.

Promoting Digital Twins: Digital twins are virtual models of physical assets that use AI to improve efficiency, significantly shortening the manufacturing process. IoT platforms with sensors in manufacturing produce data for AI and analytics, optimizing operations across supply chains.[252] The government should incentivize companies to digitalize their workflows, starting from design and manufacturing, to support the development of digital twins from chip design to edge applications.

Leveraging Digital Threads: Digital threads of data across value chains enable trusted digital marketplaces of data producers and consumers. Integrating IoT Bills of Materials and data identifiers creates certified digital threads, facilitating platform-based ecosystems. This approach enhances supply chain visibility, efficiency, security, and growth, extending from components to IoT device usage.

Monetizing Supply Chains: Connecting digital threads across supply chains safeguards proprietary IP and fosters new digital marketplaces, driving revenue streams and improving end-to-end visibility. This leads to reduced risks of cyberattacks, counterfeiting, and product recalls, while enhancing efficiency, cost management, vulnerability handling, differentiation, and innovation.

Encouraging the use of digital twins and digital threads will modernize supply chain IoT infrastructure, improve efficiency, security, and visibility, and foster innovation. Government encouragement could encourage use in procurement, convening stakeholders to encourage use and documenting case studies demonstrating the value of investment in this technology. This approach will drive economic growth by creating trusted digital marketplaces and enhancing overall ecosystem performance.

Enabling Recommendation ER3.3.2: Congress and the Executive Branch should incentivize trusted multi-stakeholder alliances and collaboration networks to speed development and adoption of connected end-to-end IoT solutions.

Supported by Findings 6, 12, and 14.

To advance the development and adoption of connected end-to-end IoT solutions, the federal government should implement incentives that promote collaboration among stakeholders. This approach ensures that IoT systems are secure, reliable, and capable of supporting critical infrastructure.

The federal government should implement incentives to promote collaboration for trusted end-to-end IoT solutions, with enterprise business processes and workflows cryptographically linking tasks, stakeholders, and handoffs of IoT trusted assets and data among participating stakeholders. The term "trusted" means that IoT parts, systems, applications, and supply chains operate as intended and produce data that is not tampered with or compromised.

Incentivizing Collaboration. The federal government should incentivize multi-stakeholder alliances and collaboration networks to develop trusted end-to-end IoT solutions. By promoting enterprise business processes and workflows that cryptographically link tasks, personas, and IoT assets, the government can strengthen national security, drive economic growth, and position the U.S. as a global IoT leader.

Promoting Trusted Digitalization. Encouraging industries to adopt trusted digital tools and solutions with cryptographic tracing is essential. This digitalization will allow industries to design, manufacture, and manage enterprise workflows securely.[253] The government's active role in promoting these capabilities can contribute to more resilient supply chains and valuable end-to-end solutions.

[250] A digital twin is a virtual representation of an IoT device, system or process, designed to accurately simulate the behavior of function of a physical object or infrastructure. Digital twins accelerate adoption with smaller investment.

[251] Digital flow of data connecting business processes products assets and bill of materials in a value chain. For the electronics value chain the digital threat includesof HBOM, SBOM and other Digital Bill of Materials (DBOM)

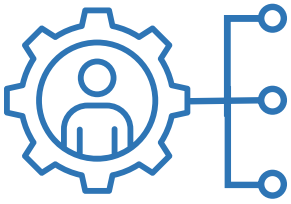
[252] Ondrej Burkacky, Mark Patel, Nicholas Sergeant, and Christopher Thomas "Reimagining fabs: Advanced analytics in semiconductor manufacturing" from McKinsey and Company (March 21, 2017) available at https://www.mckinsey.com/industries/semiconductors/our-insights/reimagining-fabs-advanced-analytics-in-semiconductor-manufacturing

[253] Global Semiconductor Alliance Trusted IoT Ecosystem Security, "Reply to NIST RFI on Evaluating and Improving Cybersecurity and the Cybersecurity Framework" available at https://www.nist.gov/system/files/documents/2022/04/25/04-25-2022-GSA_TIES.pdf

Strengthening National and Economic Security. By fostering trusted digitalization, the government can protect IoT electronics in critical infrastructure from attacks, ensuring confidentiality and integrity and preventing human and economic losses. This approach will accelerate IT/OT convergence, enhancing critical infrastructure services through trusted traceability methods. Also, it will foster innovation, enabling businesses to gain a competitive advantage with smart-connected IoT systems and. enable trusted ecosystems to accelerate the growth of IoT-enabled digital economies.

Possible Implementation Methods. To achieve these goals, the government can offer financial incentives such as tax credits and grants for companies using traceable IoT parts. It should require suppliers to adhere to specific security and traceability standards for government contracts. Establishing a certification process for IoT products linked to cybersecurity and traceability standards will also be crucial. Finally, engaging industry associations, businesses, and tech hubs to develop best practices for trusted IoT development and supply chains will ensure comprehensive and effective implementation.

Implementing this recommendation will enhance supply chain security, ensure data integrity, and boost the reliability of IoT systems. This investment will strengthen national security, promote economic stability, and position the U.S. as a global leader in IoT innovation. By fostering trusted digitalization and multi-stakeholder collaboration, the government can drive significant advancements in IoT-enabled industries and infrastructure.



Fostering an IoT-Ready Workforce

Fostering an IoT-ready workforce is crucial for the U.S. to effectively utilize and advance IoT technologies, thereby enhancing innovation, productivity, and economic growth across various industries. Congress and the Executive Branch should integrate the future IoT workforce's needs into existing initiatives and programs, collaborating with industry, academia, and state and local governments to align educational and training efforts with the evolving demands of the IoT sector, ensuring a well-prepared and adaptable workforce.

Objective 4: Material improvement in the knowledge, skills, and abilities of those who develop, implement, and operate IoT devices, applications, and systems.

Key Recommendation KR4.1: Congress and the Executive Branch should integrate the needs of the future IoT workforce into existing initiatives and programs with industry, academia, and state and local government efforts.

Supported by Findings 4 and 16.

The federal government should integrate the needs of the future IoT workforce into existing federal initiatives and programs with industry, academia and state and local government efforts. In addition, these needs should be integrated, as appropriate, into workforce development programs specified in the Inflation Reduction Act of 2022 (supporting renewable energy), the Bipartisan Infrastructure Law, the CHIPS Act, and the NSF Regional Engines. For example, Section 13007 (Workforce Development, Training, and Education) of the Bipartisan Infrastructure Law provides funding for the transportation workforce development activities, including tuition and other financial support, apprenticeships, internships, and outreach campaigns.[254]

The current workforce lacks many of the key digital, technical and data science skills and expertise required to support the IoT-enabled economy and civil society. This IoT workforce include engineers who develop the hardware and software, integrators who install, integrate, and deploy IoT and IoT-based solutions, technicians who service and maintain the products and equipment, operators and users that use the IoT-enabled systems and applications, and the analysts and data scientists who work with data and algorithms to generate insights.

The IoT workforce development areas of development should consider and include:

1. **Sourcing and recruitment of workers.** Initiatives to address the labor shortage and the need to bring more workers into the IoT and digital workforce. These include those new to the workforce (out of high school, out of college), immigrants, and people who have left the workforce - the unemployed, retired, women who left to raise kids and now coming back, etc.), people who have traditionally been underrepresented (minority groups, disabled, etc.), and those transitioning from other careers and industries.
2. **Lifelong education and development of existing and new worker bases.** This can be done at a variety of levels and means - vocational training, community college and university training, and continuing professional education. Workforce development efforts include reskilling and new skills development, upskilling, and continuing professional education.
3. **Workforce Placement.** Once the workforce is trained or retrained, they need to be placed in industries across the economy. Specific areas of need include those industries that have not traditionally been digital or have hired digital talent (e.g., mining, construction, etc.) and in geographic areas of the country with significant shortages of digital workforce (e.g., rural areas, small towns, etc.). This includes new workers, as well as those reskilled from other industries.
4. **Workforce Retention.** Initiatives to retain workers who have been trained from leaving the industry or their roles.

The federal government should also 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, which can help them to adopt, and accelerate the implementation and execution of

[254] "Highway Funding for Workforce Development" from U.S. Department of Transportation available at https://www.fhwa.dot.gov/innovativeprograms/centers/workforce_dev/OST_Workforce_Development_Fact_Sheet.aspx

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.

Enabling Recommendation ER4.1.1: The Executive Branch should review the National Cyber Workforce and Education Strategy and align and integrate any special or unique needs and considerations of the IoT workforce.

Supported by Findings 2, 4, 8, and 16.

The federal government should review its National Cyber Workforce and Education Strategy and align and integrate the special needs and considerations of the future IoT workforce. Existing federal, state, and local government, academia and industry efforts are focused on IT related workforce development. Despite its connected nature, IoT is not IT. IoT is a disparate and new set of technologies used in both IT and non-IT environments. IoT technologies integrate with other technologies, including but not limited to operations technology, medical technologies, and other industry specific systems. Further, IoT and its associated technologies represent new cybersecurity vulnerabilities that must be addressed by cybersecurity professionals in different ways.

The IoT workforce works with a different set of connectivity technologies, such as LoRaWAN and 4G/5G, integrates IoT devices into networks outside of traditional IT settings, and the edge and cloud technologies. In addition, the workforce also works with resource constrained embedded devices and firmware development, device management and integration, IoT application development and operations. The IoT data collected, transmitted, stored must be analyzed by data scientists to create insights, automate operations, and train machine learning and AI algorithms. Furthermore, the data collected may be sensitive and must be protected against unauthorized access and use.

While there is some overlap, the IoT and IT workforces are distinct. Industries such as manufacturing, energy and transportation employ operational technologies (OT), including industrial control systems, supervisory control, and data acquisition (SCADA) systems and programmable logic controllers (PLC), to monitor and control physical processes. Many of these systems are built on legacy and proprietary technology platforms and do not employ modern cybersecurity practices. In many cases, these systems operate in isolation from the IT network. In these industries, IT and OT systems operate independently of each other and are maintained by separate organizations. The OT workforce, many of whom are mechanics, electricians, technicians, and operators, have a different digital background and have very limited IT expertise.

The incorporation of IoT into industrial processes requires 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.

Enabling Recommendation ER4.1.2: The Executive Branch should collaborate with industry, academia, and state and local government to create an IoT trained workforce embedded in target high priority industry sectors.

Supported by Findings 4, 16, and 20.

While IoT creates beneficial outcomes across many sectors across the country, it offers significant transformational impacts in strategic industries and sectors like agriculture, renewable and clean energy, smart cities and communities, healthcare, manufacturing, transportation, and supply chain.

However, a shortage of IoT trained and ready workers in these industries hinders the realization of its potential. The federal government should collaborate with industry, academia, and state and local government to create and place an IoT-ready workforce around certain critical digital and non-digital skills in "priority" industries.

The collaboration should create and accelerate a wide-ranging IoT workforce at all functional levels, from field technicians, systems integrators, engineers, software developers, cybersecurity, and data scientists, proficient in the unique characteristics and needs of those industries.

As part of this recommendation, the federal government should consider:

- Identifying and agreeing on target industries where IoT has significant transformation potential, including precision agriculture, renewable and clean energy, smart cities and communities, healthcare, smart manufacturing, smart infrastructure, transportation, logistics, and others that have economic, social, and strategic importance to the United States.

- Integrating IoT development needs into new or existing industry, academia, and government (federal, state, local) initiatives.

Enabling Recommendation ER4.1.3: The Executive Branch should collaborate with industry, academia, state and local governments and private investors to create and place workforce in industries and areas of opportunity.

Supported by Findings 4, 16, and 20.

While IoT workforce development is needed across all economic sectors within the United States, some industry sectors, and parts of the country face greater challenges than others. For example, rural regions of the country struggle with building, attracting, and retaining a suitable digital workforce.

Agencies could seek out and collaborate with members of private industry, academia, state and local governments and private investors to create and expand the IoT-related workforce. Opportunities may exist in key industries that have traditionally not been digital significant digital and in geographic areas that have struggled with recruiting people (e.g., rural areas, tribal lands).

Traditional industries with limited previous digital adoption (construction, mining, manufacturing, etc.) face similar challenges. For example, 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.[255]

The federal government should create partnerships with industry, academia, and state and local governments to build, develop, place, and retain workforce in these types of industries and communities. Examples of initiatives that can be considered include:

- **Create job opportunities in small businesses:** Build upon existing SBA programs to support small businesses and start-ups that develop, install, integrate and service IoT and IoT-enabled applications. For example, the SBA partners with Small Business Investment Companies (SBIC) to make debt and equity investment in small businesses, the heart of the American economy which account for most of the jobs.
- **Development:** Offer distance learning methods to support learners and workers in rural communities, those in underserved communities, and those that are disabled. Prioritize those communities that have received funding for broadband under the Bipartisan Infrastructure Law, as well as those regions that have received workforce development funding from Bipartisan Infrastructure Law (BIL), Inflation Reduction Act (IRA), CHIPS and Science Act (CHIPS), National Science Foundation (NSF), Department of Justice, and others.
- **Placement:** Tuition forgiveness for university graduates with college loans. In exchange for loan forgiveness, graduates are deployed to communities, industries and smaller businesses that have workforce recruitment challenges for a specific period of time.

Enabling Recommendation ER4.1.4: Congress and the Executive Branch should advocate development and implementation specialized data privacy training programs to equip the IoT workforce with the necessary skills and knowledge to protect sensitive information, ensuring compliance with current privacy regulations and standards.

Supported by Findings 4 and 7.

Integration of privacy-related training into existing or planned federal initiatives will increase both awareness and capability of federal stakeholders. This training can be improved by collaborating with industry experts, academia, and privacy regulators to create a robust curriculum focused on the latest privacy laws, regulations, and best practices. To ensure full understanding and capability, the government should establish certification programs to validate IoT professionals' privacy and security expertise, ensuring they are well-equipped to handle sensitive information responsibly.

As federal agencies and their partners implement mandatory training requirements to keep employees abreast of evolving privacy standards and emerging threats, and as they include formal awareness campaigns to emphasize the importance of data privacy and promote a culture of security and compliance, the IoT workforce will be able to accomplish the necessary tasks effectively while improving trust.

The government should partner with leading technology companies and privacy advocacy groups to provide cutting-edge training resources and tools. Through this partnership, stakeholders can develop mechanisms to regularly assess the effectiveness of training programs and make necessary adjustments to address new challenges and technologies in the IoT landscape.

[255] "Digital Capabilities in U.S. Civil construction" from Dodge Construction Network SmartMarket Brief (November 2, 2021) available at https://www.construction.com/resource/going-digital-part-2/

Facilitating Industry Adoption of IoT

Facilitating industry adoption of IoT is crucial for harnessing its transformative potential across agriculture, smart communities, public safety, healthcare, environmental monitoring, and transportation. Leveraging federal grants and programs can support IoT projects that drive innovation and efficiency. Key recommendations include Congress considering new financial models for sustaining IoT programs, developing a comprehensive Agricultural IoT Strategy, implementing actions to promote IoT in smart cities and communities, enhancing public safety through IoT adoption, encouraging IoT in healthcare, promoting IoT for sustainability and environmental monitoring, and supporting IoT in smart transit and transportation to improve mobility, reduce congestion, and enhance safety.

Objective 5: The United States leads the adoption and use of IoT to benefit its economy, communities, and civil society. The U.S. Government considers and undertakes actions to facilitate and maximize adoption, realization of benefits, and mitigation of risks.

Leverage Federal Grants and Programs to Facilitate IoT Technology Adoption and Use

Key Recommendation KR5.1: Congress should consider new financial models for sustaining and supporting programs when evaluating IoT project feasibility in federal grants.

Supported by Findings 1, 16, 17, 20, 21, 23, and 24.

The integration of IoT to create "smart technologies" adds complexity to the operations and maintenance (O&M) of traditional systems. For example, these systems require periodic firmware updates, maintenance of the data stored, replacement of hardware components, and development and update of applications. These activities require additional levels of support and resources that buyers did not have traditional "dumb systems".

While grants offset the initial acquisition and build costs, many organizations lack the financial means and resources to sustain IoT operations and maintenance. For example, small municipalities and rural communities operate on tight budgets with very limited ability to raise revenue from taxes and fees from a small tax base to sustain operations. Utility companies employing IoT systems may have limited ability to pass the costs to their ratepayers. Because of this financial constraint, projects either shut down after funds run out or some entities are discouraged from applying. Smaller communities and organizations are disproportionately impacted by this constraint.

The federal government should take into consideration the financial challenges that some organizations face in adopting and sustaining IoT-based smart systems. Future initiatives and programs to facilitate IoT adoption should incorporate considerations to help grant awardees sustain the long-term operation of their smart systems.

Enabling Recommendation ER5.1.1: The Executive Branch should encourage federal grant applications to consider other financial or funding models to help adopting organizations to sustain and support IoT projects.

Supported by Findings 1, 16, 17, 20, 21, 23 and 24.

The federal government should explore financial and funding models to help organizations sustain and support IoT projects beyond initial acquisition and build phases.

Challenges with Sustaining IoT Projects. While grants can offset initial costs, many organizations lack the resources to maintain IoT operations. Smaller organizations, particularly those in rural and tribal areas, may forgo IoT projects or only operate them for a short-term due to limited funds. Current grant application criteria may also exclude those unable to sustain long-term operations. This disproportionately impacts the communities that need the IoT systems the most.

Extended Funding for Operations. Consider extending funding for operations from one to two years for applicants in areas that would benefit most from IoT, such as rural, tribal areas, and small towns. This extension would help these communities sustain their IoT projects.

Regional Models. Encourage regional partnerships where multiple adjacent communities apply together for grants. By sharing and pooling costs and resources, they can achieve economies of scale to sustain IoT applications.

Innovative Partnerships. Incorporate criteria that reward innovative approaches to sustaining operations. For example, cities could seek corporate sponsors to support the maintenance and operation of IoT networks.[256]

Implementing these models would enable broader and longer-term adoption of IoT technologies, especially in underserved areas. This would enhance the benefits of IoT projects, such as improved efficiency, enhanced public services, and economic growth, making technology more accessible and sustainable for all communities.

Enabling Recommendation ER5.1.2: Congress and the Executive Branch should develop programs and grants to help underserved and less developed communities adopt IoT.

Supported by Findings 1, 16, 17, and 20.

Small, underserved, rural and tribal communities have unique needs and face different challenges than their larger and more urban counterparts. The federal government should develop programs and grants to drive IoT adoption that is targeted to these communities. Doing so will create equitable access to IoT and smart systems and its benefits, including economic and societal outcomes.

Improving Accessibility. These initiatives would improve national accessibility to IoT benefits, making advanced technologies available to all citizens and municipalities. Targeted government grants could spur private investment and growth, amplifying economic and societal benefits.

Creating Jobs and Promoting Growth. Funding opportunities for underserved and rural communities will create jobs and promote economic growth. Adopting digital technologies will require skilled workers to develop, implement, and maintain these systems, stimulating job growth and supporting a skilled IoT workforce.

Identifying Appropriate Methods. The government should identify suitable tactics, such as ADA-compliant EV charging stations, including EV-ready language in building codes, and opportunities for small and disadvantaged businesses. Clear eligibility criteria should ensure these grants target the intended communities.

Monitoring and Evaluation. The federal government should establish a system to monitor and evaluate the effectiveness of these grants and incentives to ensure they achieve the desired impact.

These programs will enhance IoT accessibility, create jobs, promote economic growth, and ensure all communities benefit from advanced technologies, leading to a more equitable and prosperous society.

Leading the Way for IoT Adoption in Agriculture

Key Recommendation KR5.2: Congress and the Executive Branch should develop a comprehensive Agricultural IoT Strategy.

Supported by Finding 19.

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.

[256] One city outside the United States developed partnerships with local corporations to "sponsor an Air Quality sensor node". This sponsorship paid for the ongoing subscription fee for the cloud service, as well as the O&M costs.

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.

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.

Enabling Recommendation ER5.2.1: Congress should fund the deployment of a "farm of the future" setup in representative universities nationwide. This nationwide test-farm IoT network should span different forms of agriculture, including, but not limited to broadacre, horticulture, livestock, and aquaculture.

Supported by Findings 16 and 19.

The federal government should allocate funding to implement a "farm of the future" setup in a representative set of universities across the United States, providing a showcase for farmers in each region on collection and analysis of data from their farms. In seeking candidates for the "representative" universities, consideration should be given to diversity of climate, soil, and other farming conditions. Land grant universities, including the several Historically Black Colleges and Universities (HBCU) that fall under this category, are logical candidates.

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 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.

The implementation of a nationwide IoT network in representative 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.

Research will be needed to determine which IoT technologies should be used. Some concrete and specific IoT applications should be defined for inclusion in the project and funding requirements, based on project types. "Farm of the Future" efforts should look to assist in determining what IoT technologies should be acceptable for use. This may require coordination with other federal agencies in alignment with their objectives. Various universities might pose different challenges with respect to implementation, including connectivity, tech readiness, and other topics.

Development of this concept should consider, in parallel, the creation of a Forest of the Future initiative that includes ways to address connectivity issues, workforce training, data management, and other IoT adoption challenges within the forestry and timberland industry. This initiative could include ways to respond to forest fires and impacts of climate change. To further this initiative, we recommend establishing a coalition that brings together leading and mid-tier industry SMEs and organizations. This coalition's mission would be to educate Congress and policymakers about the barriers to IoT adoption and the opportunities it presents. The coalition would serve as a unified voice advocating for the necessary support and resources to overcome these challenges and promote the advancement of IoT technologies in the industry. The U.S. government should fund new grants to drive policy and new technology implementations for the industry as well as continuing to fund programs that are currently working and retire those that add little value to drive IoT and related initiative adoption.

Collaborative Development. This strategy should be created in collaboration with stakeholders, including farmers, technology providers, industry experts, and research institutions. A cohesive national strategy will prevent fragmented initiatives, improve interoperability, and provide clear direction for IoT adoption in agriculture.

Identifying Challenges. The Federal government should prioritize challenges in agriculture that IoT can address, such as water management, pest control, and labor shortages. Specific goals, timelines, and milestones should align with national objectives related to food security, environmental sustainability, and economic growth. An interagency task force involving USDA, FCC, and DOE can oversee the strategy's development and implementation.

Support Programs. Programs to help growers adopt IoT technologies should include subsidies for connectivity, sensors, and digital applications. These programs can mirror existing USDA subsidies for agricultural inputs and climate-smart practices, benefiting all stakeholders, from farmers to policymakers and consumers.

Cost and Accessibility. The upfront cost of IoT limits adoption, especially for marginalized and smallholder farmers. Federal subsidies can scale the technology, reducing costs and making it accessible to those who need it most. A public/private/

academic partnership, leveraging Agricultural Extension centers, can develop approaches to ensure these farmers can benefit from IoT technology.

A comprehensive Agricultural IoT Strategy will enhance productivity, sustainability, and economic growth in agriculture. By addressing key challenges, providing subsidies, and ensuring broad stakeholder involvement, the strategy will make advanced technologies accessible and beneficial to all farmers, improving food security and environmental outcomes.

Enabling Recommendation ER5.2.2: The Executive Branch should support and promote industry and Standards Development Organization (SDO) efforts to address interoperability of agricultural systems and machinery.

Supported by Findings 11 and 19.

Farms have a variety of equipment and machinery from different manufacturers that cannot communicate or exchange data with each other, each with its own data formats and languages. The agriculture industry model is to develop software and devices in proprietary formats. Theme 2 of this report describes numerous interoperability challenges for IoT adoption. An example of this lack of interoperability hinders agricultural 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.

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.

Possible ways the federal government can facilitate standards and interoperability include:

- Conducting the research and developing the frameworks that inform the standards development processes.
- Providing testbeds enabling industry to test and confirm interoperability of systems.
- Providing technical expertise to support standards development activities.
- Encouraging the adoption of existing developed standards instead of developing additional standards whenever available, possible, and feasible.
- Specifying requirements for those IoT technologies based on industry consensus standards in federal grants.
- Collaborate with international governments to harmonize geographic and region-specific standards and practices.

Enabling Recommendation ER5.2.3: Congress and the Executive Branch should facilitate small farm/ranch adoption of IoT technologies.

Supported by Findings 16, 17, and 19.

Small farms (< $350,000 GCFI) 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.[257] 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.

Agencies could help by offering grants and subsidies for purchase. Since small farms operate on low margins, they have limited upfront cash available for investment which 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.

The 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.

Enabling Recommendation ER5.2.4: Congress should support enactment of federal "right to repair" legislation to address the inability of agricultural producers to service their smart equipment.

Supported by Findings 2 and 19.

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 cannot afford the wait, such as during harvest season. Today, some farmers are getting around this by purchasing "hacked" software from Eastern Europe[258] or buying older non-smart equipment that they can maintain and repair themselves.[259]

[257] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[258] S. Schrader, "Farmers Are Having to Hack Their Own Tractors Just to Make Repairs" from The Drive (February 9, 2021) available at https://www.thedrive.com/news/39158/farmers-are-having-to-hack-their-own-tractors-just-to-make-repairs

[259] L. Matsakis and O. Solon, "Senate Introduces Bill to Allow Farmers to Fix Their Own Equipment" from NBC News (February 1, 2022) available at https://www.nbcnews.com/tech/new-senate-bill-farm-equipment-right-to-repair-rcna13961

As of April 2022, twenty-seven U.S. states have introduced "right to repair" legislation although not all are concerned with agriculture equipment.[260] In addition, a federal Agricultural Right to Repair Act bill was introduced in February 2022 and is undergoing consideration.[261]

To facilitate the adoption of IoT and smart farming equipment, the IoTAB recommends that Congress support the enactment of a national "right to repair" legislation for agricultural equipment.

Leading the Way for IoT Adoption Through Smart Communities

Key Recommendation KR5.3: Congress and the Executive Branch should implement specific actions to further promote IoT adoption through smart cities and communities.

Supported by Findings 16 and 20.

Enabling Recommendation ER5.3.1: The Executive Branch should facilitate and support the development and use of smart community and "IoT-related sustainable infrastructure" reference models.

Supported by Finding 20.

Today's smart cities and communities are "one-offs", designed and built using a variety of inconsistent approaches and "homegrown" practices. They have limited scalability, interoperability, cybersecurity, and resilience. 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. A reference model and framework are needed to help municipalities, solution vendors and smart community integrators build smart cities that are interoperable, secure, scalable, resilient, and relevant.

The reference models and framework capture the various components of the ecosystem and provide a blueprint for design and planning, collaboration, coordination, and communication in smart community 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 community 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.

The federal government should facilitate and support the development and use of smart cities and sustainable infrastructure reference models that provide a consistent and sound starting point and roadmap for cities and communities to build from. There have been a variety of previous federal efforts, such as the DHS Smart City Interoperability Reference Architecture (SCIRA) for public safety, and the NIST Internet of Things Enabled Smart City Framework (v1.0). The IoTAB recommends building on these and other efforts in collaboration with industry and academia to create and build out the reference models and frameworks.

Enabling Recommendation ER5.3.2: Congress and the Executive Branch should develop Smart Community and Sustainability Extension Partnerships (SCSEP) to provide technical advice to cities and communities adopting IoT.

Supported by Findings 4, 16, and 20.

IoT and smart city technologies can bring great economic and societal benefits to our cities, but most cities and agencies lack the associated technical, analytical, and operational expertise, tools, and resources internally to support smart city initiatives. Smaller cities, rural communities and agencies have even more limited resources are disproportionately impacted. While some of this digital expertise and skills are available in industry, it is limited, unevenly distributed in certain high demand industries and geographic areas, and fragmented. For example, cybersecurity skills are in-demand and resources are concentrated in those industries that pay well. Municipalities and agencies may not have the budget, the empowerment, or the ability to engage the necessary external resources. Even if they were able to, the public procurement processes to engage private sector resources are burdensome and takes a long time.

[260] N. Proctor,"Half of U.S. States Looking to Give Americans the Right to Repair" from Public Interest Research Group (April 22, 2022) available at https://pirg.org/articles/half-of-u-s-states-looking-to-give-americans-the-right-to-repair/

[261] G. Joiner, "TFB: Agricultural Right to Repair Act introduced" from Morning Ag Clips (February 1, 2022) available at https://www.morningagclips.com/tfb-agricultural-right-to-repair-act-introduced/

A different way to for cities and communities to equitably access and engage these resources is needed. The IoTAB recommends that the federal government consider a model, similar to that of existing USDA agriculture extension offices and the NIST Manufacturing Extension Partnership (MEP), to provide technical expertise and advice on smart cities and sustainability. This model, the Smart City and Sustainability Extension Partnership (SCSEP), provides an improved and more equitable access to technical expertise and resources. The SCSEP model is well suited 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.

Smart communities, 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 community" 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.

Enabling Recommendation ER5.3.3: The Executive Branch should facilitate opportunities for adoption of IoT and smart technologies for local communities.

Supported by Findings 16 and 20.

The government should facilitate opportunities for adoption and equity of benefits of IoT and smart community technologies for local governments (e.g., cities, counties), regional entities (e.g., 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 community technologies into city vision, infrastructure, and operations.
- Project grants for smart community 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).

The government can help integrate IoT and smart cities and communities' initiatives into existing federal programs and funding infrastructure, especially by leveraging existing programs that focus on socio-demographically underserved communities.

This will help provide smart community grants in underserved communities that have already received broadband grants to build on new connectivity infrastructure. The government is also well positioned to support industry and other existing partner efforts to increase the awareness of the benefits of these technologies and applications within those communities.

Enabling Recommendation ER5.3.4: The Executive Branch should facilitate smart community opportunities and IoT adoption for rural communities that have broadband infrastructure, have received broadband infrastructure funding, or have completed broadband infrastructure buildouts.

Supported by Findings 12, 16, 19, 20, 22, and 24.

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.

A number of these communities across the United States have received grants and assistance to build out broadband infrastructure. In the near future, many other communities will be receiving grant awards funded by the Bipartisan Infrastructure Law. The federal government should create initiatives to facilitate IoT and smart community adoption in those communities in order to maximize benefits and outcomes arising from the availability and deployment of broadband infrastructure.

Some examples of initiatives to consider include, but not limited to:

- Coordination with federal agencies (e.g., USDA, NTIA, EPA, DOT) to drive community awareness of IoT opportunities, and support programs that encourage community and industry participation.
- Offering project grants for community related IoT projects and deployment projects (e.g., environmental monitoring, rural healthcare, smart agriculture)
- 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).

Enabling Recommendation ER5.3.5: The Executive Branch should support and promote industry and SDO efforts to address interoperability of smart communities (including smart buildings, energy and utilities, traffic).

Supported by Findings 11, 20, 21, 23, and 24.

Cities procure and deploy a range of smart technologies, IoT devices and systems that are independently owned and operated by a variety of municipal and non-municipal organizations. While these systems work well individually, they do not integrate and work together very well.

Interoperability challenges are a major barrier to maximizing the value of IoT and smart community technologies. Disparate IoT devices and smart community systems have limited or 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.

In an ideal smart city environment, these disparate systems would communicate and collaborate with each other to create outcomes benefiting city residents and businesses. For example, audio sensors detect gunshots. Once detected, the streetlights on nearby streets could increase in brightness to facilitate the ability of witnesses to identify the shooters and for police cameras to capture better quality surveillance footage. The information is then routed to the city's 911 response call center, which then informs the operator and provides situational awareness information to responding police officers.[262]

In practice, cities do not have a reference model and individually procure and deploy technology systems that are:[263]

- Not extensible or cost effective because they are custom systems that cannot communicate and exchange information with each other.
- Based on a diverse set of proprietary architectures, standards and protocols that have not yet converged.
- Not sufficiently interoperable and scalable to support smart city applications and outcomes.

The lack of interoperability in IoT applications for smart cities remains a challenge, stopping the seamless integration and collaboration among diverse devices and systems.[264] This stops the municipality and other non-municipal organizations from realizing the full value of a smart and connected city.

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.

Possible ways the federal government can facilitate standards and interoperability include:

- Conducting the research and developing the frameworks that inform the standards development processes.
- Providing testbeds enabling industry to test and confirm interoperability of systems.
- Providing technical expertise to support standards development activities.
- Encouraging the adoption of existing developed standards instead of developing additional standards whenever available, possible, and feasible.
- Specifying requirements for those IoT technologies based on industry consensus standards in federal grants.

Enabling Recommendation ER5.3.6: The Executive Branch should facilitate small to medium city adoption of smart community technologies.

Supported by Findings 16, 17, 20, 21, 23, and 24.

Most cities in the United States are small. There are 1300 cities that have less than 250,000 people. In contrast, there are only ten American cities that have a population over a million people.

[262] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[263] "A Consensus Framework for Smart City Architectures", IES-City Framework Release 1.0, IES-City Framework Public Working Group, September 30, 2018 available at https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFramework_Version_1_0_20180930.pdf

[264] Kary Framling, "Open standards: The answer to the smart city data dilemma" from Smart Cities Dive (October 3, 2019) available at https://www.smartcitiesdive.com/news/open-standards-the-answer-to-the-smart-city-data-dilemma/564268/

Many small cities can benefit from the deployment of IoT and smart city technologies. However, compared to their larger city counterparts, these cities lack the funding, expertise, and resources to implement, operate and maintain smart community technologies. At the same time, these smaller cities have needs that are different from their larger city counterparts. They are not large smart cities on a smaller scale, nor cheaper versions of large smart cities. and may require grants that are more aligned to their needs.

The federal government should facilitate interest in and adoption of IoT and smart city technologies for small to medium size cities. Some examples of possible actions include:

- Coordination with federal agencies (e.g., USDA, NTIA, EPA, DOT) to drive community awareness of IoT opportunities, and support programs that encourage community and industry participation.
- The government can help by developing smart community grants focused on smaller communities and rural communities.
- Agencies might also consider creating smart community 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 community technologies.
- Consideration of different funding and innovative funding models to sustain the operation of IoT and smart systems.

Enabling Recommendation ER5.3.7: The Executive Branch should facilitate equity in realization of smart community benefits.

Supported by Findings 16 and 20.

While IoT and smart city technologies offer the potential of beneficial outcomes, these benefits may not be fully realized or available to all the members of the community. For example, community-based air quality systems notify residents of poor air quality levels through a mobile phone application or a website. However, some children, senior citizens, and poor people may not receive these notifications because they do not have a smart phone or do not have access to a computer at home. Other means of notification, such as through digital signage in a building or on a street, a "red light/green light" system inside school buildings, are needed.

In other cases, the technology may be available to all members of the community, but the outcomes disproportionately impact a few. For example, facial recognition systems may be used to assist in crime prevention but the inability of these systems to accurately identify Asian and African American faces creates outcomes that harm these demographics.[265] The new jobs created by IoT, smart communities and digital transformation require skills and education that members of underserved communities do not have and 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 (e.g., due to language barriers or lack of digital literacy skills).

The federal government should take into consideration the possible barriers hindering the equitable distribution and full realization of benefits from IoT and smart city technologies. These considerations may be manifested in a variety of possible actions, including but not limited to:

- Study and understand the various forms of digital inequities hindering equitable utilization and value realization of the smart city system.
- Workforce and skills development initiatives for members of the local communities to be able to use, operate, maintain, and develop smart systems.
- Grants targeting known inequities and specific outcomes in certain neighborhoods within local communities (e.g., improving health outcomes by monitoring air quality levels in poor neighborhoods located next to freeways and oil refineries, etc.)
- Provisions for IoT projects funded by federal grants requiring that benefits be accessible by the underserved (e.g., notifications from a smart city system should not accessed only by a smart phone, but also on digital signage, etc.)
- Initiatives and programs prioritizing infrastructure access and buildout in communities that lack it.

[265] Patrick Grother, Mei Ngan, and Kayee Hanaoka. *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects*, NIST IR 8280, from National Institute of Standards and Technology (December 2019) available at https://doi.org/10.6028/NIST.IR.8280

Leading the Way for IoT Adoption for Public Safety

Key Recommendation KR5.4: The Executive Branch should promote IoT adoption that will improve public safety.

Supported by Finding 24.

Enabling Recommendation ER5.4.1: The Executive Branch should require the development and implementation of privacy and data usage policies in federally funded public safety and smart community projects that use IoT technologies.

Supported by Findings 3, 7, 20, and 24.

IoT sensors and camera systems provide high value in addressing public safety issues. This includes monitoring events and preventing incidents, spotting and informing on hazards, illegal and dangerous activities, and identifying suspects and persons of interest. However, concerns about unauthorized and inappropriate data collection, misuse and misinterpretation of the data collected, and lack of governance and accountability, have led communities to ban or limit the use of these IoT systems. This leads to a loss of beneficial outcomes that would have otherwise been realized by the community.

A lack of understanding and trust of these technologies is a major cause of these concerns. The community is often unaware of how these technologies work, their limitations and capabilities, how the data is used, and the role of policies and processes in ensuring and maintaining proper usage. Furthermore, the communities that these technologies are deployed in are often not involved nor consulted in defining how these systems are used. As a result, many of the systems operate in a way that is not always in alignment with community concerns, leading to poor outcomes and an overall distrust in the technology.

Federal funding and grants help law enforcement agencies across the country procure and deploy public safety IoT and camera systems. The IoTAB recommends that provisions be placed in these grants that require grant awardees to develop and implement privacy and usage policies as part of the system deployment. The policies should be developed collaboratively with the local community and take into account best practices and the needs of the local community.

Enabling Recommendation ER5.4.2: Congress and the Executive Branch should include IoT considerations (including IoT adoption and utilization plans) in federal procurements that support public safety applications.

Supported by Findings 20 and 24.

The federal government funds a variety of large-scale programs that support public safety IoT applications. However, one major challenge is that when the program or platform is built or made available for use, there is a lack of user adoption and utilization. One reason for this is low user awareness that this program or platform exists. Another reason is that the program (and technology) may have been designed and developed in such a way that it is too expensive for users. For example, the program may be designed for expensive proprietary applications or devices, or it may have limited interoperability to support low-cost devices based on industry or open standards. This limits what IoT devices this program can support.

In order to fully leverage and justify the investment in these programs, the IoTAB recommends that the federal government require potential bidders to develop marketing and adoption plans that discuss how they will market this program to its customers (e.g., public safety agencies, cities), and how they have designed and developed it in a way that makes economic sense for its potential users to be able to use, grow its usage, and support future applications.

Enabling Recommendation ER5.4.3: Congress and the Executive Branch should create a program that advises and enables local communities to purchase IoT systems or IoT-enabled systems for public safety applications.

Supported by Findings 20 and 24.

Despite the beneficial outcomes provided by the use of IoT in public safety, many communities and public safety organizations have very limited ability to purchase IoT equipment from their own budgets and require supplemental funding from external sources. This includes systems that support law enforcement, fire, emergency management services, and public safety access points.

The IoTAB recommends that the federal government establish a program that provides funding to enable communities and public safety organizations to procure public safety IoT systems. There may already be existing grant funding vehicles for the procurement of technologies for public safety (including law

enforcement, community resilience, disaster response, etc.). If so, these funding vehicles should be updated to support this recommendation.

However, the federal government should consider some provisions in this program that help to address some long running challenges. For example, a lack of interoperability is a major challenge. The program can specify that the IoT devices, systems and applications must be interoperable with the FirstNet network.[266] This at least drives communities toward some sort of connectivity and perhaps functional interoperability. In addition, the IoT systems procured through the program should support or integrate into, as relevant and applicable, next generation 911 systems. A second challenge is privacy concerns raised by IoT systems. Grants offered should specify the need for the development, in collaboration with the community, of some privacy and usage policy for those devices that may collect personal data.

Because each community has its own unique priorities, needs and systems, the program should allow applicants to purchase the types of IoT systems and applications that best serve their community. The appropriate federal agencies could work with communities and the FirstNet Authority to identify an initial IoT list (e.g., drones, flood gauges) and guidance of what IoT applications this grant would help procure.

Consideration should be given to prioritizing certain applications for certain communities. For example, in communities prone to wildfires, the grant should prioritize the procurement of IoT systems that detect wildfires, support emergency response and community evacuations.

Leading the Way for IoT Adoption for Health Care

Key Recommendation KR5.5: Congress and the Executive Branch should promote IoT adoption in the health care industry.

Supported by Finding 22.

Enabling Recommendation ER5.5.1: The Executive Branch should promote the Internet of Medical Things (IoMT) as an enterprise priority, including to healthcare facilities' leadership teams.

Supported by Finding 22.

The Internet of Medical Things (IoMT) should be equivalent in priority for all healthcare stakeholders as is IT infrastructure, cybersecurity posture, or applications. IoMTs monitor, detect, inform, and deliver therapies to patients, therefore, they deserve just as much attention and call out as cloud services, for example. Currently IoMTs are 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.

One area where the executive leadership priority impact is needed is medical device cybersecurity. The average medical device has 6.2 vulnerabilities. This challenge is exacerbated by the fact that more than 40% of medical devices are near end-of-life and poorly or unsupported by the device manufacturers.[267] A study of 200,000 infusion pumps, medical devices that delivers fluids and medicine to a patient's body in a controlled manner, found that 75% of the units scanned had known cybersecurity vulnerabilities. Six of the top ten vulnerabilities were considered critical and two more were considered high risk.[268] A 2023 Cybersecurity Risk analysis reported that the healthcare industry has an average loss exposure (probable likelihood and probable financial impact) of $5.5 Million per attack scenario.[269] These cyberattacks put healthcare organizations at financial risk as hospitals often have low operating margins. For example, the median operating margin was 0.4% in March 2023.[270] This suggests that fixing and recovering from a cyberattack could put smaller providers out of business.

Another high impact area is device interoperability. IoMT devices adhere to standards that allow for interoperability and exchange of data. Despite this, many healthcare delivery organizations still purchase and use medical devices built to

[266] The FirstNet network was established to operate and maintain an interoperable public safety broadband network. Details are available from https://firstnet.gov/network

[267] "Total Cost of Ownership Analysis on IoMT Cybersecurity Risk" from Asimily (August 23, 2023) available at https://asimily.com/blog/new-report-hospitals-iomt-cybersecurity-risk/

[268] A. Das, "Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization," from Palo Alto Networks (March 2, 2022) available at https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/

[269] "2023 Cybersecurity Risk Report", from RiskLens available at https://www.risklens.com/hubfs/Content/reports/RISK_RiskLens%20Annual%20Report.pdf?hsLang=en

[270] N. Schwartz, "Hospital margins crawl into black for March" from Beckers Healthcare (May 12, 2023) available at https://www.beckershospitalreview.com/finance/hospital-margins-crawl-into-black-for-march-report-finds.html

proprietary standards. Researchers have reported that "While some efforts led to commercial adoption of standards (e.g., IHE Devices), the adoption of open interoperability standards at the device level has "fallen flat". This is attributed to a lack of a business case for device manufacturers to move away from proprietary solutions and a lack of healthcare providers asking for open interoperable interfaces."[271]

Enabling Recommendation ER5.5.2: Congress and the Executive Branch should facilitate cybersecurity in IoT in smart medical devices and equipment, including wearables, in-home devices, community IoT-related healthcare systems, and a continuum of care.

Supported by Findings 7, 8, and 22.

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 are 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.

The federal government should take a number of actions to facilitate cybersecurity resilience in healthcare. Some examples of actions include:

- The government should help to 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.
- As part of this facilitation, the government should consider development of programs, resources, and incentives to help healthcare providers migrate away from vulnerable legacy equipment and devices that cannot be patched or upgraded or were not subject to compliance with section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act).
- Agencies can assist by developing 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.

Enabling Recommendation ER5.5.3: Congress and the Executive Branch should facilitate and support the use and adoption of healthcare IoT in rural communities.

Supported by Finding 22.

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 a 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.[272] In addition, many have limited transit options to go see a doctor on a regular basis.

[271] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[272] "About Rural Health", from Public Health Infrastructure Center, U.S. Centers for Disease Control and Prevention (May 9, 2023). https://www.cdc.gov/rural-health/php/about/?CDC_AAref_Val=https://www.cdc.gov/ruralhealth/about.html

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.

The government could help support increased IoT adoption by facilitating grants to healthcare providers in those communities that have received broadband grants to build on new connectivity infrastructure. Agencies could coordinate to drive physician and patient awareness of IoT in healthcare for treatment and could research ways to promote broader IoT adoption (e.g., coding IoT-enabled services in Medicare to support senior population in rural areas, facilitate support from private payers (insurance companies), or focusing on IoT support for chronic disease management).

Adopting healthcare IoT in rural communities offers significant benefits, including improved access to medical services and better health outcomes. IoT-enabled services like telehealth and home healthcare monitoring can address healthcare access inequities, especially in areas with limited healthcare resources. By supporting grants for healthcare providers and promoting awareness of IoT in healthcare, the government can enhance healthcare accessibility and quality in rural areas. This approach leads to reduced disparities, better management of chronic conditions, and overall improved health for rural residents.

Enabling Recommendation ER5.5.4: Congress should facilitate the adoption of AI in IoT in healthcare through improved AI research, development, and workforce improvement.

Supported by Findings 4, 13, and 22.

AI is well suited for analyzing massive amounts of health and patient data to support patient diagnoses, make recommendations, and in some cases, take autonomous actions. Facilitating the adoption of AI in IoT for healthcare is crucial for improving health outcomes through advanced data analysis and personalized treatments.

However, using AI to diagnose people and identifying personalized treatments for people is challenging. 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.

The potential for the combination of AI with IoT to revolutionize healthcare treatment is enormous. The IoTAB recommends that the federal government facilitate the adoption of AI and IoT in healthcare. Some possible areas of action include, but not limited to:

- Research in methods that improve algorithm outcomes
- Development of explainability tools, methods, and approaches (XAI)
- Policies and frameworks for risk management, safety, ethics, and human-AI collaboration for AI and IoT in healthcare
- Development of an AI-ready workforce
- Research and development of IoT technologies for healthcare applications (edge computing, etc.)

Enabling Recommendation ER5.5.5: Congress should enact HIPAA-like protection for users' medical data in mobile applications and IoT devices.

Supported by Findings 7, 8, and 22.

The Health Insurance Portability and Accountable Act of 1996 (HIPAA) requires healthcare providers and organizations "protect the confidentiality of patient health information which is generated or maintained in the course of providing health care services". HIPAA governs how "Protected Health Information" (PHI) related to the patient's health, the services rendered and the payment for these services is used and disclosed. In addition, it governs the management of electronic protected health information (EPHI) and the prevention of access to that information by unauthorized persons.[273] Finally, HIPAA requires that PHI breaches be disclosed to the affected individuals, the Secretary, and the media if appropriate.[274] Healthcare providers who fail to protect PHI information are subject to fines.

[273] "Health Information Privacy" from U.S. Department of Health and Human Services available at https://www.hhs.gov/hipaa/index.html

[274] "Breach Notification Rule" from U.S. Department of Health and Human Services available at https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Many consumer-grade IoT devices and mobile apps collect users' sensitive medical data. For example, some smart watches collect a wearer's electrocardiogram (ECG) information.[275] Consumers tend to believe that this data is protected similarly to medical data in a healthcare facility, but it is not.

The IoTAB recommends that the federal government study the need for additional protection requirements for healthcare data collected from consumer healthcare devices. The desired goal is to extend HIPAA-like protections to these classes of devices and mobile apps or enact a similar type of protection.

It should be noted that this Recommendation represents a major change. Many manufacturers and reseller 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.

Sustainability / Environmental Monitoring

Key Recommendation KR5.6: Congress and the Executive Branch should promote IoT adoption that will improve sustainability and environmental monitoring.

Supported by Findings 20 and 23.

Enabling Recommendation ER5.6.1: Congress should study the feasibility of the concept of an open repository for environmental data generated from IoT sensors.

Supported by Finding 23.

A great deal of environmental data (e.g., air quality, or AQ, measurements, water levels) is collected separately by a variety of federal, state, and local agencies. However, the emergence of low-cost air quality sensors has created an explosion of community level data. This data, collected by a variety of individuals, community organizations and municipalities, complements existing government sensors with highly localized data not available before.

The IoTAB recommends that the federal government consider that data from these traditional and community environmental sensor systems be aggregated into an open data repository and made available to the public. This data would be useful to a lot of organizations, communities, universities, and other public health 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. This informs communities and organizations on policies and actions that support environmental sustainability and public health.

Promoting the open availability of data would support research, improve transparency, and encourage proactive improvement by industry participants. 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. Such a resource will support and inform public policy, environmental research, and community education and action.

For maximum benefit, a number of barriers need to be overcome, including normalizing the data. Different sensors may have different formats, and so one reading in one brand may not correlate with the same reading on another brand, etc.

Some implementation considerations include:

- Environmental data that is collected by a variety of federal, state, and municipal organizations. The data repositories should support the data types collected and the needs of the various organizations in mind.
- Environmental monitoring projects funded by federal grants should include provisions supporting the sharing of the collected data to this open repository.
- Third-party organizations should manage any open repositories.
- Data repository should aim for consistency in data reporting, but also focus on direct raw measurements from IoT devices.

Creating an open repository for environmental data from IoT sensors can bring significant benefits. It would support research, improve transparency, and encourage proactive improvements by industry participants. This open model would enhance interoperability and competitiveness, benefiting all IoT adopters. Aggregating data from federal, state, local agencies, and community-level sensors would provide valuable insights for organizations, researchers, and policymakers. This data can inform public policies, environmental research, and community actions, promoting sustainability and public health. Overcoming barriers like data normalization and ensuring consistent reporting are essential for maximizing these benefits.

[275] "Record an electrocardiogram with the ECG app on Apple Watch" from Apple Watch User Guide available at https://support.apple.com/guide/watch/ecg-apdea4c50a57/watchos

Enabling Recommendation ER5.6.2: Congress should facilitate and support the research, development, and deployment of low-cost Air Quality sensors.

Supported by Finding 23.

Air quality (AQ) levels are dynamic and vary by location. The air quality in a neighborhood adjacent to a freeway or a factory is significantly worse than one in a quiet neighborhood just a few miles away. Traditional AQ systems are expensive and only a few can be deployed to cover a region. For example, the air quality in the nine county, 7000 square mile San Francisco Bay Area, is monitored only by a network of 35 sensors. These sensors provide a high-level regional indication of the air quality but cannot provide a local or community perspective of the actual conditions.

The emergence of low-cost air quality sensors integrated with IoT technologies offers the potential to democratize air quality monitoring. Hundreds of low-cost sensors can be deployed into a community to support a variety of use cases that were not possible or feasible before, 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.
- Rapid or emergency air quality monitoring for particular circumstances.

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.

The IoTAB observed that there is a need to shift from expensive (i.e., highly sensitive regulatory grade) monitors that limit deployment by organizations and municipalities. The IoTAB recommends that the federal government facilitate and support the continued use and deployment of low-cost air quality sensors by communities and organizations. Some examples of possible actions to be considered include:

- Support research and development to advance the state of the sensing technology and address gaps, including measurement accuracy, monitoring of critical regulated air pollutants and other emerging chemical of concern.
- Facilitate the development of sensing and measurement standards for low cost AQ sensors.
- Promote and support deployment of community air quality monitoring use cases through grants.
- Promote and facilitate access to data collected from community air quality networks to researchers, public health agencies, and others.

Enabling Recommendation ER5.6.3: Congress should implement a nationwide IoT-based Water Monitoring Infrastructure) to expand the nationwide water monitoring system, including water treatment facilities.

Supported by Finding 23.

Efficient water management is crucial for consumption, agriculture, and industry, ultimately contributing to environmental and economic sustainability. 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. For example, integration with NOAA water models could enhance forecasting and management capabilities, leading to more effective water resource planning and allocation.[276]

The IoTAB recommends that the federal government 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.

Development of a standardized, nationwide framework for water monitoring, including protocols for data collection, transmission, storage, and analysis would help improve water management, perhaps to include open data standards and APIs to ensure interoperability among different IoT devices, platforms, and NOAA water models.

[276] The NOAA national water model is described at https://water.noaa.gov/about/nwm

The government should 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. This might include support for 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.

Implementing an IoT-based water monitoring infrastructure will provide real-time, accurate data, enhancing forecasting and management capabilities. It will ensure efficient water management, support environmental sustainability, and promote economic growth. By integrating with NOAA models, the system will offer standardized protocols and improved decision-making, addressing water scarcity, contamination, and climate change challenges.

Enabling Recommendation ER5.6.4: The Executive Branch should use IoT Technologies to facilitate carbon transparency across economic sectors.

Supported by Finding 23.

Greenhouse gas reporting is becoming increasingly important as environmental and sustainability concerns become top of mind with government, business, and communities. Today, much of the greenhouse gas reporting focuses on those emitted at the company's site (scope 1) and emissions associated with the generation electricity that the company consumes (scope 2). However, there are increasing calls to report scope 3 emissions, those that are created indirectly, beyond what is generated and reported in scope 1 and 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).[277]

IoT-enabled environmental sensors, such as air quality monitors, allow these gases to be measured. In support of emerging reporting needs, the federal government and agencies should 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 emissions will enable the implementation of effective mitigation strategies and contribute to national and global efforts to reduce carbon emissions.

The government could 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. Efforts might encourage research and development of advanced IoT sensors and data analytics tools specifically designed for estimating greenhouse gas emissions across supply chains.

Agencies could also provide training and technical assistance to stakeholders in the implementation and maintenance of IoT-based carbon emissions monitoring systems. This would facilitate collaboration and data sharing among stakeholders, researchers, and policymakers to promote informed decision-making and the development of best practices for emissions reduction.

Implementing IoT-based solutions can accurately estimate and manage indirect carbon emissions associated with goods and services. This transparency will enable effective mitigation strategies and support national and global efforts to reduce carbon emissions. By leveraging IoT technologies, greenhouse gas emissions in manufacturing, transportation, maritime, agriculture, and end-of-life practices can be measured and managed. Metrics for greenhouse gas reporting protocols will drive informed decisions, and encourage collaboration among stakeholders, ultimately contributing to significant emissions reductions and environmental sustainability.

Enabling Recommendation ER5.6.5: The Executive Branch should facilitate and promote the use and integration of IoT technologies to monitor environmental conditions and hazards.

Supported by Findings 23 and 24.

Environmental situational awareness monitoring is crucial for ecological health, public safety, and disaster recovery. However, 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. One example is 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.

[277] EPA Emissions guidance is available from: https://www.epa.gov/climateleadership/scopes-1-2-and-3-emissions-inventorying-and-guidance

The IoTAB recommends that the federal government 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 and remote areas. Examples of opportunities where IoT technologies should be incorporated include forest monitoring, wildfire monitoring, earthquake detection, flood, air quality, etc.

For instance, a network of low-cost IoT-enabled gas sensors and cameras can detect and pinpoint wildfires early, allowing firefighters to respond quickly and effectively. Integrating IoT sensors for air quality, earthquakes, and other hazards enables state and regional agencies to build real-time situational awareness, supporting the preservation of sensitive areas and improving response to natural and human made hazards.

Applying IoT technologies into environmental monitoring systems can significantly enhance situational awareness, allowing for real-time monitoring and response to hazards like wildfires, floods, and air quality issues. IoT-enabled sensors can complement existing proprietary systems, providing more comprehensive and accessible data. This improved data integration supports better ecological health, public safety, and disaster recovery efforts, enabling timely analysis and responsive actions to protect environmentally sensitive areas.

Some possible actions to consider include:

- Grants for environmental monitoring using IoT technologies to communities and other organizations.
- Procurement of IoT technologies for existing environmental monitoring systems programs owned by federal agencies.
- Migration of existing data collected by traditional systems into cloud storage (e.g., the U.S. Geological Survey's river stream gauge information).
- Specification of policies and standards for the use of IoT for environmental monitoring.

Smart Transportation

Key Recommendation KR5.7: Congress and the Executive Branch should promote IoT adoption in Smart Transit and Transportation.

Supported by Findings 20 and 21.

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 ER5.7.1: The Executive Branch should promote development and application of policies, procedures and funding methods that can accelerate the adoption of smart, connected, and electrified transportation technologies.

Supported by Findings 3, 12, 20, and 21.

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, and 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 is a viable option for transportation. Also smart, connected transportation can improve traffic flow and reduce congestion which is also better for the environment.

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.[278] Under the IRA tax credits are available for EVs that are primarily assembled in North America. It is 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.

Additionally, 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 government could also leverage innovative procurement technologies like outcomes-based contracting in surface transportation.[279]

ITS America recently 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.[280]

The U.S. Department of Transportation (DOT) also announced the Saving Lives with Connectivity: A Plan to Accelerate V2X Deployment. This plan will guide the implementation of vehicle-to-everything technologies across the nation and support DOT's commitment to pursue a comprehensive approach to reduce the number of roadway fatalities to zero.[281]

[278] "National Electric Vehicle Infrastructure (NEVI) Formula Program" from the U.S. Department of Energy available at https://afdc.energy.gov/laws/12744

[279] NEMA Transportation Management Section, "Issue Paper on Outcomes-Based Contracting" from the National Electrical Manufacturers Association (March 5, 2021) available at https://www.nema.org/docs/default-source/nema-documents-libraries/whitepaper-on-outcomes-based-contracting.pdf?sfvrsn=f3ad2716_2

[280] "ITS America National V2X Deployment Plan" from Intelligent Transportation Society of America (April 28, 2023) available at https://itsa.org/advocacy-material/its-america-national-v2x-deployment-plan

[281] "USDOT Releases National Deployment Plan for Vehicle-to-Everything (V2X) Technologies to Reduce Death and Serious Injuries on America's Roadways" from U.S. Department of Transportation (August 16, 2024) available at https://highways.dot.gov/newsroom/usdot-releases-national-deployment-plan-vehicle-everything-v2x-technologies-reduce-death

Promoting an IoT-enabled Economy

The evolution of an IoT-enabled economy involves three critical phases, each building on the others to scale effectively.

Building Block 1: Platforms enabled by Modernizing IoT Infrastructure. The first foundational phase is to modernize IoT infrastructure, ensuring robust, reliable, and widespread connectivity and interoperability. As described above key recommendations include, promoting industry collaboration to adopt existing standards and protocols, maximizing interoperability through consistent models and interfaces, expanding programs to ensure high-quality IoT connectivity nationwide, and encouraging digital infrastructure initiatives to support enterprise digital transformation.

Building Block 2: Business Ecosystems enabled by Establishing Trust in IoT. The next phase is to establish trust in IoT systems, crucial for secure, private, and reliable operation of interconnected devices, fostering widespread adoption and public confidence. As described above, recommendations focus on NIST providing consistent cybersecurity guidance, Congress passing comprehensive federal privacy legislation, and the Executive Branch supporting trusted IoT architectures to ensure supply chain provenance and traceability, enhancing device security and integrity.

Building Block 3: Partnerships and collaboration to promote an IoT-Enabled Economy enabled by workforce development and industry adoption. The final phase is to promote an IoT-enabled economy. This phase is crucial for driving innovation, enhancing productivity, and optimizing resource utilization across sectors, thereby creating a more efficient, competitive, and scalable economy. Key recommendations below include monitoring IoT adoption progress in supply chain logistics, facilitating public-private partnerships for comprehensive IoT solutions, supporting AI integration in IoT applications for improved decision-making and productivity, providing regulatory guidance for the drone industry, and promoting equitable access to IoT benefits for all societal segments. This comprehensive approach will ensure that the U.S. fully leverages advanced IoT technologies to maintain its global leadership.

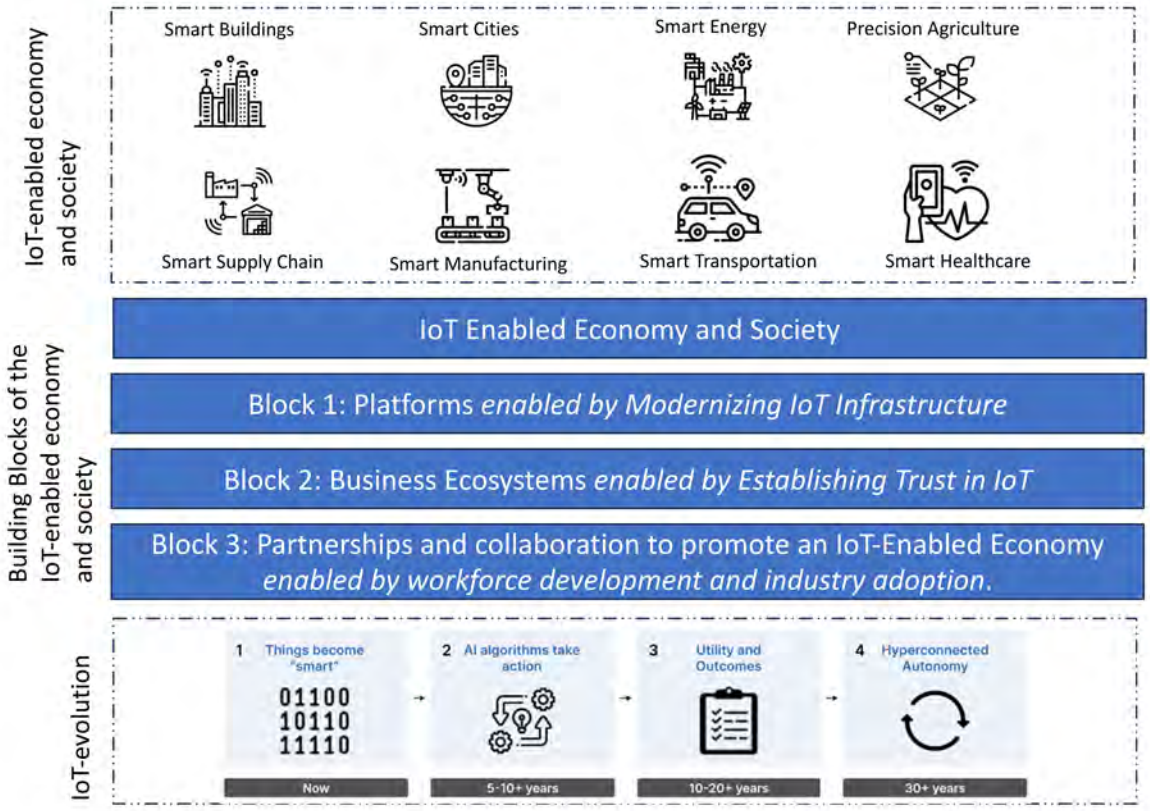


Figure 21. Building blocks for the IoT-enabled Economy[282]

[282] Figure credit: Benson Chan and Tom Katsioulas, used with permission.

Objective 6: Scaling of benefits and value provided by IoT broadly across the economy and civil society.

Key Recommendation KR6.1: The Executive Branch should monitor and evaluate progress of IoT adoption for supply chain logistics.

Supported by Findings 1 and 26.

A resilient and agile supply chain is critical to the economic health of the United States. Executive Order 14017 (America's Supply Chains) highlighted the need for a resilient supply chain.[283] IoT technologies increase end-to-end visibility across the supply chain and are a foundational contributor and enabler of the resilient and agile supply chain. Periodic monitoring and evaluating the progress of IoT adoption in supply chain logistics is essential to ensure federal strategies and initiatives are effective, inform on development and modification of programs and initiatives, challenges are addressed, and desired outcomes are achieved. This process enables the government to make informed decisions, optimize investments, and enhance the overall impact of IoT initiatives. Some of the implementation considerations include:

Establish Clear Goals and Objectives. Define specific, measurable, and time-bound goals for IoT adoption in supply chain management. These goals will provide a clear framework for monitoring progress and evaluating success.

Develop Relevant Performance Indicators. Identify key performance indicators (KPIs) that reflect the desired outcomes of IoT adoption, such as efficiency gains, cost reductions, improvements in transparency and traceability, and advancements in cybersecurity.

Implement Data Collection and Reporting Mechanisms. Set up robust systems and processes for collecting, storing, and analyzing data related to IoT adoption and supply chain performance. This will facilitate regular and accurate assessments.

Conduct Periodic Assessments. Schedule regular evaluations using the collected data and KPIs to assess the effectiveness of IoT initiatives. These assessments will help identify gaps, challenges, and areas for improvement.

Foster a Culture of Continuous Improvement. Encourage feedback and learning from monitoring and evaluation results. Use insights to refine policies and initiatives, promoting a culture of continuous improvement within the industry.

Collaborate with Stakeholders. Engage with industry, academia, and other stakeholders to gather diverse insights and perspectives. This collaboration ensures a comprehensive understanding of progress and challenges in IoT adoption.

Assign Responsibility. Designate a lead federal agency or interagency group responsible for overseeing the monitoring and evaluation process. This group will ensure accountability and coordinated efforts.

Develop a Monitoring and Evaluation Plan. Create a detailed plan outlining goals, objectives, KPIs, data collection methods, and evaluation schedules. This plan will guide the systematic monitoring and evaluation efforts.

Allocate Appropriate Resources. Ensure adequate financial, human, and technical resources are allocated to support monitoring and evaluation activities. Proper resourcing is crucial for the effectiveness and sustainability of the process.

Implementing a structured approach to monitor and evaluate IoT adoption in supply chain logistics will optimize resource allocation, enhance policy effectiveness, and ensure continuous improvement. This process will ultimately contribute to the long-term success and competitiveness of the industry, driving economic growth and innovation.

Enabling Recommendation ER6.1.1: The Executive Branch should encourage businesses to adopt IoT technologies in their supply chain operations by reducing the initial investment costs and perceived risks associated with the implementation of IoT solutions.

Supported by Findings 16, 17, and 26

While IoT provides sustainable and far-reaching benefits to supply chain logistics and management, financial considerations may hinder its adoption. IoT projects may be complex and costly as it involves not only procurement of the IoT solution, but other associated costs, including upgrade of supporting and legacy systems, and integration to back-office and operational systems.

[283] "Executive Order on America's Supply Chains" from The White House (February 24, 2021) available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

For smaller business organizations, financial factors may prevent adoption, while larger businesses may prioritize their limited budgets and delay adoption.

The federal government should consider ways to stimulate IoT adoption by offsetting the financial burden of planning, procuring, and deploying IoT technologies. Examples of potential things to be considered include grants for specific businesses, tax credits, and tax deductions. For small businesses, the federal government through the SBA and its partners may consider the development of loan programs to assist businesses with the procurement of IoT technologies.

Financial incentives will help, but funds are limited so the government should study which organization types will best benefit from assistance and establish eligibility criteria. Agencies can then focus on appropriate incentives for those entities, monitor and evaluate results, and expand the programs, as needed. In addition to financial assistance, the government can also help to raise awareness of the benefits of IoT supply chain logistics and operations and can also provide technical assistance.

Enabling Recommendation ER6.1.2: Congress and the Executive Branch should apply an appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic IoT manufacturing supply chain.

Supported by Findings 3, 25, and 26.

American manufacturers share the goal of fostering and strengthening domestic manufacturing and supply chain capabilities. With the recent influx of federal funding and executive orders in this sector, there is an increasing trend to support the "Build America Buy America" concept Ensuring the Future Is Made in All of America by All of America's Workers.

The U.S. needs to strengthen domestic manufacturing capacity, develop resilient supply chains, and train workers to improve domestic preference requirements, avoid supply constraints, and help meet deployment goals. IoT support for manufacturing supply chains will help manufacturers meet increasing demands, especially where domestic alternatives for components and subcomponents are limited.

Government policies that can foster and strengthen domestic IoT manufacturing and supply chain capabilities include: phasing in domestic content requirements, providing clear rules and guidelines how domestic content requirements apply across all funding and procurement programs, avoiding any rules thar require determining the country of origin of components and subcomponents into larger domestically manufactured components, and allowing manufacturer value add (MVA) or substantial transformation to be classified as domestic content.

Key Recommendation KR6.2: The Executive Branch should facilitate public-private partnerships (PPPs) focused on IoT adoption to advance collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia developing end-to-end IoT solutions in supply chain logistics.

Supported by Findings 5, 14, 15, 25, and 26.

The federal government should facilitate 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. This will foster collaboration and knowledge exchange, driving adoption of IoT technologies for end-to-end solutions.

Addressing Common Barriers: PPPs can effectively address common barriers to IoT adoption, such as infrastructure gaps, limited technical knowledge, and financial constraints. By pooling resources and aligning efforts, these partnerships can drive innovation in IoT solutions, initiate pilot projects, and roll out proof-of-concept initiatives that demonstrate the value and benefits of IoT end-to-end solutions.

Supporting Workforce Development: In addition to fostering innovation, PPPs can contribute to workforce development by creating and supporting training programs, potentially in collaboration with technical colleges and universities. This will help build the necessary skills for effective IoT implementation.

Establishing Standards and Regulatory Frameworks: PPPs also play a critical role in establishing industry standards and regulatory frameworks conducive to IoT adoption across diverse supply chains and industries. Close collaboration with regulatory bodies like the Federal Communications Commission (FCC) and standards setting institutions like the National Institute of Standards and Technology (NIST) is essential for this process.

Implementation considerations include:

- **Identifying Key Stakeholders.** The federal government should identify relevant private sector stakeholders, including businesses, industry associations, research institutions, and

technology providers, to help develop and implement end-to-end IoT solutions in supply chain management.

- **Establishing a Collaborative Framework.** Create a formal framework for collaboration between the public and private sectors, including joint working groups, industry forums, or tech innovation hubs sharing ideas and resources.
- **Defining Clear Goals and Objectives.** Set well-defined goals for public-private partnerships that align with the overall strategy for IoT adoption in supply chain management, ensuring a common vision and measurable progress.
- **Developing Joint Projects and Initiatives.** Collaborate on joint projects to address specific supply chain challenges, including pilot projects, research programs, and the creation of new IoT standards and protocols.
- **Ensuring Effective Communication and Coordination.** Maintain open and transparent communication with regular meetings, progress reports, and information-sharing mechanisms to ensure coordination and momentum.
- **Monitoring and Evaluation.** Establish systems to monitor and evaluate the effectiveness of PPPs, tracking key performance indicators like joint projects, private investment, and impacts on supply chain efficiency.

Facilitating PPPs for IoT adoption in supply chain logistics will drive innovation, enhance collaboration, and accelerate the deployment of end-to-end IoT solutions. These partnerships can effectively address common barriers such as infrastructure gaps and limited technical knowledge, while pooling resources to initiate pilot projects and proof-of-concept initiatives. Furthermore, PPPs will support workforce development through training programs, establish industry standards and regulatory frameworks, and promote consistent communication and evaluation, ultimately improving supply chain efficiency, resilience, and competitiveness.

Enabling Recommendation ER6.2.1: The Executive Branch should promote collaborative IoT platforms that align stakeholder business incentives and encourage businesses to work together, fostering innovation, efficiency, and competitiveness.

Supported by Findings 1, 14, 16, and 18.

Promoting collaborative IoT platforms that align business incentives among stakeholders can drive innovation, efficiency, and competitiveness. These platforms act as hubs where device manufacturers, service providers, developers, and end-users can collaborate to share data, insights, and resources, fostering collective growth and benefits. These benefits include:

- **Fostering Innovation.** Collaborative IoT platforms encourage industry-wide innovation, leading to the development of advanced technologies and solutions. By bringing together various stakeholders, these platforms facilitate streamlined device management, data exchange, and interoperability, reducing operational complexities and driving technological advancements.
- **Aligning Business Incentives.** Aligning business incentives through these platforms motivates stakeholders to prioritize shared goals and establish mutual interests. This alignment helps reduce conflicts of interest, fosters trust, and improves collaboration, ensuring that all parties work towards collective success.
- **Accelerating Economic Growth.** IoT-driven industries will experience substantial growth, creating jobs and contributing to economic prosperity. By supporting collaborative IoT platforms, the government can help harness the power of network effects to enhance security, user experience, and drive economic growth.

To effectively promote collaborative IoT platforms, the government should focus on standardization to ensure compatibility and interoperability across platforms, and foster public-private partnerships to drive innovation. Establishing robust data confidentiality will build trust and protect data, while enabling incentive mechanisms like tax benefits and grants that will motivate businesses to align with IoT platform goals. Implementing a monitoring system to track progress on security, and economic impact will ensure ongoing benefits.

Promoting collaborative IoT platforms will drive innovation, streamline operations, and foster economic growth. By aligning business incentives and encouraging collaboration among stakeholders, these platforms will enhance security, improve user experience, and create job opportunities, contributing to the overall prosperity of IoT-driven industries.

Enabling Recommendation ER6.2.2: The Executive Branch should promote the enablement and use of IoT trusted digital marketplaces and platform-based business ecosystems.

Supported by Findings 6 and 14.

As digital threads and platforms emerge, the government should promote their use to drive economic growth through trusted data exchange and licensing while protecting proprietary IP. These tools connect business processes, products, and assets across supply chains, enhancing security, integrity, and availability.

Digital Threads in Supply Chains. Digital threads link data from components like chips, software, and devices create a value chain. This flow of information—from raw materials to installed systems—can inform security and product integrity. Each stage in the value chain benefits from cryptographic protection, ensuring that data remains secure and valuable.

Trusted Digital Marketplaces. A trusted digital thread can be monetized in digital marketplaces. The government should incentivize these marketplaces, where producers and consumers share information about assets, enhancing visibility, traceability, and efficiency. The use of platforms can streamline processes, improve governance, reduce costs, and eliminate redundancies in complex supply chains.

Innovation and New Business Models. Promoting trusted digital marketplaces can lead to new business models and revenue streams. By maximizing network effects, these platforms will fuel the growth of ecosystems and future digital economies. Pilot programs, best practices, and guidelines can facilitate this adoption.

Implementation Considerations. To implement these initiatives, the government should identify standards, taxonomies, and best practices for supply chain digital threads and marketplaces. Suitable marketplaces, such as those for EV charging, should be incentivized. Promoting the benefits of data marketplaces to potential participants and providing tax credits and subsidies will encourage participation. Ensuring data security and confidentiality is crucial, and the effectiveness of these marketplaces should be continuously monitored and improved.

Promoting digital threads and marketplaces will drive economic growth by enhancing supply chain efficiency, reducing costs, and enabling new business models. These initiatives will improve visibility, traceability, and security while protecting proprietary information, ultimately contributing to a more robust and innovative digital economy.

Key Recommendation KR6.3: The Executive Branch should actively facilitate and support the adoption of AI in IoT applications to improve decision-making, optimize resource utilization, and enhance productivity.

Supported by Findings 13 and 15.

The convergence of AI with IoT offers the potential to enhance and accelerate outcomes delivered by the Internet of Things. From machine learning to generative AI, the application of artificial intelligence complements human efforts to make sense of the large volumes of data collected. By leveraging advanced algorithms, machine learning and other AI techniques help make better informed decisions in a timelier manner, automate operations, and rapidly scale beneficial outcomes. The use of AI with IoT will extend the benefits of IoT to consumers, users, communities, and businesses.

The federal government should consider actions that facilitate the use of AI with IoT. Some examples of possible actions to be considered include, but not limited to:

- Develop policies and guidelines that enable the safe, equitable, and responsible use of AI. This may include governance frameworks, models, and people.
- Support research that advances the state of AI, including algorithms and techniques, explainability tools, frameworks, and other initiatives.
- Facilitate public-private-academia partnerships to support AI and IoT. Federal stakeholders could establish a public-private-academia partnership that would define specific applications that would 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.)
- Support and facilitate the development of an AI trained workforce. The government could also create educational programs and resources to help professionals understand the benefits of AI technology and how to effectively implement and use these applications.

Supporting AI adoption in IoT applications enhances decision-making, optimizes resource use, and boosts productivity. AI enables better data analysis and informed decisions, benefiting businesses, policymakers, and consumers. Public-private- partnerships, financial incentives, and educational programs can drive AI integration. Workshops and online courses ensure widespread knowledge and skill development, improving operational efficiency and fostering economic growth.

Enabling Recommendation ER6.3.1: The Executive Branch should promote trusted AI-IoT platforms across supply chains and ecosystems to improve transparency and sustainability and drive economic growth.

Supported by Findings 6, 13, 15, 25, and 26.

The government should promote trusted AI-IoT (AIoT) platforms[284] within supply chain ecosystems, including circular supply chains. Circular supply chains aim to keep resources

[284] For further explanation of AIoT platforms see the discussion in Finding 15 above.

in use for as long as possible through sustainable processes like recycling and remanufacturing. These AI-IoT platforms and supply chains enhance transparency, sustainability, and economic growth. AIoT can drive innovation and efficiency, benefiting businesses, environments, and the digital economy.

Innovation Hubs. Promoting AIoT platforms will drive innovation, enabling the development of cutting-edge technologies and solutions within circular supply chains. This fosters a culture of continuous improvement and technological advancement.

Efficiency Boost. AIoT can optimize resource utilization, reducing waste and energy consumption. This efficiency enhances productivity and lowers operational costs, making supply chains more sustainable and economically viable.

Environmental Benefits. Sustainable practices fostered by AIoT platforms can help combat climate change and promote eco-friendliness. By reducing waste and promoting recycling, these platforms contribute to a healthier environment.

Economic Growth. The growth of AIoT-driven industries will create jobs and stimulate economic development. Increased employment opportunities and technological advancements will drive economic progress.

Competitive Advantage. By embracing AIoT, the nation can establish itself as a pioneer in the digital economy. This competitive edge will attract global investments and position the country as a leader in sustainable technology.

Promoting trusted AIoT platforms within circular supply chain ecosystems will foster innovation, enhance efficiency, combat climate change, stimulate economic growth, and establish a competitive advantage in the global digital economy. Initiatives on this topic within manufacturing related programs can provide a foundation for responsible and sustainable technological advancement.

Key Recommendation KR6.4: Congress and the Executive Branch should provide overarching regulatory guidance for the unmanned aerial systems (drone) industry.

Supported by Findings 3, 19, 20, 21, and 24.

Drones play an increasingly important role in our economy and society. For example, drones monitor agricultural lands to monitor growing conditions and plant health. They monitor the condition of infrastructure, such as water lines, oil pipelines, waterways, and electrical lines, in remote areas spanning hundreds of miles. They are used in construction to monitor buildings, inspect work, and detect variances from plans. Drones inspect disaster areas to aid in rescue and recovery efforts and assess damage. Future applications include the use of drones for delivery of products, and potential human transportation (air mobility).

Drones integrated with IoT technologies can leverage real-time data and automation capabilities to enhance functionality and efficiency.

IoT can accelerate the adoption of drone technology, especially for Non-Line-of-Sight (NLOS) operations. IoT enables seamless communication, real-time data collection, remote control, and task automation. NLOS drone operations can cover larger areas and perform tasks in remote locations, expanding their utility in various sectors. The government can help speed adoption factoring the following considerations:

- **Regulatory Guidance.** Establishing appropriate regulatory guidance is crucial for leveraging the potential of NLOS drone operations. Regulations should address data security, privacy, airspace usage, safety, and accountability. They foster investment in drone technology, benefiting the economy and society.
- **Conflicting Regulations.** There are conflicting regulations for recreational and commercial drone pilots. The FAA governs commercial pilots, but uncertainty remains over who regulates recreational pilots. This confusion can hinder the adoption and proper use of drones.
- **Advanced Air Mobility and Remote ID.** Commercial pilots flying large drones in sections of the airspace under Advanced Air Mobility (AAM) jurisdiction face regulatory challenges. Additionally, not all drones meet the Remote ID requirement, which broadcasts the drone's location and heading.
- **Stakeholder Involvement and Education.** Developing regulatory guidance requires stakeholders such as drone manufacturers and communications providers. Expanding access to education and training on drone safety is also essential for promoting safe and effective drone use.

Providing overarching regulatory guidance for the drone industry will enhance agricultural efficiency, improve energy sector monitoring, and support effective environmental monitoring. Clear regulations and stakeholder collaboration will accelerate IoT-enabled drone adoption, fostering innovation, economic growth, and societal benefits.

Key Recommendation KR6.5: The Executive Branch should promote, facilitate, and monitor equity in the accessibility, realization and distribution of value and benefits created from the adoption and use of IoT.

Supported by Findings 1, 4, 16, 20, and 26.

The use of Internet of Things (IoT) technology has the potential to generate significant economic and societal benefits. However, these benefits are not always accessible to all, creating disparities that hinder growth, resilience, and transformation.

Accessibility Challenges. Small businesses often lack the capital and resources to invest in IoT solutions. Rural communities face connectivity infrastructure shortages, making it difficult to deploy and operate IoT technologies. Individuals with limited digital literacy may struggle to utilize IoT solutions fully, missing out on the complete range of benefits. Moreover, new jobs and economic opportunities created by an IoT-enabled economy are not equally available to all residents within a smart community.

Government Initiatives. The federal government should implement policies and programs that promote equitable access to IoT benefits. This includes updating existing initiatives and launching new programs to ensure that IoT advantages are distributed fairly across all communities. Specific actions could include providing grants for smaller, rural, and underserved communities to adopt IoT technologies, promoting IoT adoption among small businesses, and specifying IoT requirements in federally funded infrastructure projects.

Supporting IoT Adoption Technical resources should be deployed to support IoT adoption and operation in rural, tribal, and smaller communities. Programs should be developed to facilitate innovation among small businesses and start-ups. Additionally, building supporting IoT infrastructure in areas without broadband connectivity and initiatives to develop an IoT-ready workforce in underserved, rural, and tribal communities are essential.

Promoting equity in IoT accessibility and value distribution ensures that the economic and societal benefits of IoT are realized by all communities. This approach fosters inclusive growth, enhances resilience, and supports the transformation towards a more connected and technologically advanced society. By addressing disparities, the federal government can create a more equitable and prosperous future for all.

Closing Thoughts from the IoT Advisory Board Chairs

We conclude this report with some closing thoughts.

IoT is a national and strategic imperative for the United States.

We strongly believe that IoT holds immense promise to transform our economy, improve our quality of life and enhance our society and communities in the United States. Our nation, our economy and our communities must embrace it and integrate it into their strategies, operations, and capabilities.

However, its benefits to the nation have been slow to develop. A number of factors, including leadership and coordination, the lack of a U.S. National IoT strategy, lack of trust, gaps in technology and infrastructure, regulatory and policy issues, and an insufficiently trained workforce, hinder progress.

If we do not accelerate our progress, we will miss out on the opportunities and benefits that IoT brings. We jeopardize our economic and national security. We risk falling behind other nations who make it a priority. We allow others to dictate the direction and nature of our transformation. This is unacceptable.

The Internet of Things is not an option. It is a development seen globally; our options lay in how we manage it for our own nation. Managing this transition properly is imperative for our economy, our society, our communities, and our country. We must prioritize and accelerate IoT. We must overcome the challenges and barriers hindering progress and accelerate the enablers facilitating integration and adoption of IoT into our country.

We urge a "whole of government" effort to accelerate IoT along six broad areas.

We developed a number of findings and recommendations that were informed by the IoTAB's collective experiences and expertise, thoughtful input from subject matter experts, members of industry and the general public, informal reviews from the Federal Working Group, research, and publicly available information. We organized these recommendations into six broad actions for the Federal Working Group and Congress to examine and consider:

1. Government Leadership
2. Modernizing IoT Infrastructure
3. Establishing Trust in IoT
4. Fostering a IoT-ready Workforce
5. Facilitating Industry Adoption of IoT
6. Unlocking an IoT-Enabled Economy

Like the transistor, personal computer, Internet and smart phone, the Internet of Things is disruptive and transformational. To unlock its potential for the United States, we ask the federal government and Congress to study our recommendations with a vision of the emerging interconnected future in mind. Look beyond the "status quo" constraints that may hinder the implementation of our recommendations and instead bring an open mind, imagination and American ingenuity and resourcefulness to consider how our recommendations can be implemented. Bring the "whole of government" together with industry, academia, and communities to partner in new and meaningful ways.

We offer a number of strategic and tactical recommendations. Some recommendations are strategic, such as the need for a national IoT strategy, the need to understand and mitigate the impact of IoT modules produced in adversarial nations and protecting access to the semiconductor and electronic supply chain, are strategic and establish long term success. Other recommendations, such as a number of privacy and cybersecurity recommendations, facilitate the removal of barriers that hinder near-term and long-term adoption. Finally, other recommendations such as the procurement of IoT for government use and the specification of IoT into federal grants, are relatively easy to implement and demonstrate government "lead by example". We urge the federal government and Congress to develop a framework for considering our recommendations that balance between the strategic and tactical, the "easy to do" and the "difficult to implement", and the "quick win" with the "long-term".

We further urge the federal government and Congress to act with urgency and speed while "the iron is hot". The COVID pandemic has shifted perspectives and priorities. The Bipartisan Infrastructure Law of 2021, the Inflation Reduction Act of 2022, and the CHIPS and Science Act of 2022 have provided a "once in a lifetime" source of federal funding that can bring some of these recommendations to life in years, not decades. The emergence of artificial intelligence can potentially address long running challenges in cybersecurity, privacy, and interoperability.

We urge the Federal Working Group and others to examine and consider additional important topics in this space.

Our findings and recommendations represent a small set of actions to accelerate IoT in the United States. Our recommendations represent those based on our charter, our collective expertise and contributions from industry members and the interested public and the limited amount of time we had. We balanced strategic and visionary recommendations that are broad across markets with tactical and specific to certain markets and applications.

We urge the federal government and Congress to consider additional topics beyond our report. Some relevant and important topics for further analysis and action, include:

- **Critical Infrastructure.** We expect IoT will make a substantial and positive contribution to the management and operation of critical infrastructure. For example, the integration of IoT-enabled devices facilitates the operation of the smart grid and its ability to dynamically balance supply and demand. However, IoT cybersecurity emerges as a paramount concern, as formerly air-gapped systems and interconnected devices become potential entry points for cyberattacks that disrupt operations and services and steal vital operational data. Limited standards and a lack of interoperability facilitate the seamless communications of a wide spectrum of heterogeneous devices across platforms and legacy systems. The provenance of the IoT devices, components and software used in critical infrastructure is essential to prevent the integration of compromised and counterfeit systems and equipment.
- **Artificial Intelligence.** We expect the increasing integration and use of AI with IoT (AIoT), corresponding with the rise in edge computing and in AI-capable chips. However, the convergence of AI with IoT presents a number of considerations to be studied. These include the ownership and authorized use of data to train AI models, privacy infringement of people captured by AIoT systems, the reliability and safety of critical IoT systems (autonomous vehicles, medical devices, etc.) operating autonomously, the transparency and explainability of the outcomes generated by AIoT systems, and ethical considerations, including biases in AI algorithms trained on IoT data reflecting societal inequalities. As AIoT systems become more prevalent, the area of human-AI collaboration, such as collaborative robots ("cobots") in manufacturing, should be studied to understand the new roles of humans. Finally, the emerging potential of AI to address long running challenges in cybersecurity protection and interoperability of systems should be studied and considered.
- **IoT architecture, data, and communications infrastructure.** As the IoT continues to grow and expand, the definition of "at scale" becomes a moving target. The network must support heterogeneous devices of all types, brands and models and variations of those models. The traffic from these IoT devices ranges from small bits of data on a periodic basis to continuous streams of high bandwidth video traffic. Some data is processed in servers integrated into the network near the point of use (edge) and in vehicles (mobile edge), while other data is sent to remote data centers (cloud). The "traditional" device to cloud architecture is quickly evolving to a multi-layer distributed architecture of cloud data centers, local edge servers, processors in routers and gateways and fixed and mobile (e.g., cars and drones) devices. The IoT infrastructures faces a variety of challenges to be addressed, including:[285]
  - Management of the distributed and hyperconnected IoT network at scale.
  - Performance and quality of service optimization under continuously varying conditions.
  - Improving communications network system fault tolerance and resilience.
  - High performance computing and network infrastructure to support AI and complex autonomous IoT applications.
  - AI-based cyberattacks.
  - Data infrastructure and ecosystem to facilitate sharing and exchange of data within and across industry sectors.
- **Data management and governance.** Research firm IDC estimated that by 2025, there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data.[286] [287] A research report states that "As IoT scales, so does data management complexity. The IoT data collected comes in a variety of types, structured and unstructured formats, and sizes. It resides and operates in a distributed environment, with data processed on the device, in moving vehicles, split among edge servers, and the cloud. Some data are time-sensitive and must be processed immediately while others are stored for future actions. Data may be required to comply with industry, state, and national regulations."[288]

[285] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[286] D. Reinsel, "How You Contribute to Today's Growing Datasphere and its Enterprise Impact" from IDC Blog (November 4, 2019) available at https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact/

[287] One Zettabyte is roughly the equivalent of 500 billion movies.

[288] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

Data management is critical for the organization, utilization and optimization of the information collected from IoT and AIoT devices. To address these needs, "beyond big data" innovations and governance approaches are needed. For example, the development and deployment of data fabrics offers the potential of connecting data sources scattered and decentralized across organizations, data centers, edge servers and businesses. Equally important, issues of data ownership, intellectual property rights, and appropriate usage will emerge and must be addressed.

- Legacy systems and technologies: Unlike consumer IoT applications, IoT systems used in enterprise, medical and industrial seldom operate in a standalone manner. These devices often integrate into operational processes and Enterprise Resource Planning (ERP), industrial control (SCADA) and operations systems, and other legacy systems. In addition, these IoT devices must co-exist with a variety of non-IoT legacy devices and systems. These older systems often lack the necessary compatibility with IoT devices and platforms, hindering seamless integration and data exchange. They were not designed with modern cybersecurity practices in mind, nor the level of scalability possible with IoT. These legacy systems hinder the ability of organizations to adopt and integrate IoT, as well as maximize the full potential that IoT can bring. Modernizing or replacing legacy systems can be complex, costly, and time-consuming, requiring significant investment in new technologies and disrupting current operations. Innovative approaches should be considered to help organizations modernize these systems and devices.
- **Smart cities and communities.** The development and adoption of smart cities in the United States is relatively modest and behind those of other countries. "Smart cities" today are "just cities with a few or several standout smart projects" that are not "networked, end-to-end."[289] There are a variety of reasons for this, including funding, and conflicts with existing governance, social justice, politics, ideology, and other considerations.[290] In other cases, smart city technologies are procured by individual organizations with no internal coordination with other agencies and no consideration for interoperability. While we proposed a number of recommendations in this report to address some "low hanging fruit" challenges, the topic of smart cities is much more complex and deserves additional consideration.

  New approaches and holistic systems thinking about smart cities are needed. As an example, privacy is a top-of-mind concern hindering adoption of smart city technologies. Researchers stated that "Today's approaches to smart city privacy are static, piecemeal and have limited effectiveness. For example, there are policies and regulations that ban or limit the use of facial recognition systems. Smart city solutions may be configured to disable certain functionality or limit data collection and storage. While this achieves the individual privacy objectives, it also keeps the city from realizing the full range of benefits from smart city technologies. In addition, "blanket" approaches may only be effective in certain settings. As IoT devices are increasingly integrated into city infrastructure and operations, managing privacy through existing "device by device" approaches may no longer be effective, sustainable, or relevant."[291] The researchers further proposed "context aware privacy" as a potential solution to this challenge.
- **Right to Repair.** We propose a right-to-repair recommendation specific to the agricultural industry in this report. Many of the same arguments in favor of the right to repair for agriculture apply to the general IoT space. However, for years there has been a broader discussion regarding right-to-repair in multiple product categories. Three states (California, New York, and Minnesota) have enacted legislation. California's right to repair law (SB244) took effect on July 1, 2024.[292] IoT devices have details that may prevent implementation of consumer-friendly repair approaches.

  Examples include security technologies that are specifically designed to block hackers from accessing internal functions, and contractual requirements to keep third-party keys secured. Consequently, IoT devices often integrate proprietary software and hardware components that are tightly controlled by manufacturers. They may also restrict access to repair manuals, diagnostic tools, and replacement parts, making it difficult for consumers and independent repair shops to effectively repair these devices. Providing access to repair information and tools makes manufacturer warranty support more difficult as consumers attempt repairs without the necessary skills to meet factory quality standards. State by state statutes add complexity for manufacturers who must comply with different laws. This is a longstanding and difficult topic that bears continued study as the IoT evolves.

[289] K. Smith, "The Inconvenient Truth About Smart Cities," from *Scientific American* (November 17, 2017) available at https://www.scientificamerican.com/blog/observations/the-inconvenient-truth-about-smart-cities/

[290] Chan, B., Feller, G., Paramel, R., Reberger, C. *Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IOT)*, Strategy of Things. Pending publication Fall 2024.

[291] Ibid.

[292] ?

We urge the federal government to lead the country and the world in IoT and to be accountable for our nation's progress.

As the IoTAB concludes its work and presents our findings and recommendations in this report on the Internet of Things (IoT), it is essential to recognize that our efforts represent a snapshot—a point in time view—of the rapidly evolving landscape. Our recommendations are grounded in the current state of IoT technology, adoption rates, and existing policies and regulations.

The recommendations we share today lay the foundation for accelerating the broader adoption of IoT and realization of its benefits across our nation now and in the future. However, this is just the beginning. IoT will continue to evolve, fueled by technological advancements, innovative business models, regulations, and policies. It is natural that new challenges will emerge. Some of these challenges, like interoperability and trust, continue in new forms. Other challenges, like ethical algorithms and decision-making, appear when IoT evolves to the next stage. Our framework, depicting the six broad areas of action, will continue to be relevant and applicable to address future challenges.

To ensure the success of our recommendations, we urge that the federal government actively monitors and tracks their implementation over the coming years. Rigorous assessment and regular progress reporting are essential. As changes occur—whether in technology, market dynamics, or societal needs—the federal government should be prepared to make course adjustments. By doing so, we ensure progress and impact of IoT to our nation.

Additional References

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

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

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

Acknowledgements

The IoT Advisory Board appreciates the extensive support provided by Katarina Megas and Alison Kahn of NIST, and the NIST Designated Federal Officer, Barbara Cuthill.

The IoTAB appreciates the work of the editors, Greg Witte and Brad Hoehn, who were supported by Wendy Szwerc and David Lemire, and graphic artists Keith Dana and Susan Broam.

The IoTAB also wishes to acknowledge and thank the many speakers at meetings of the IoT Advisory Board including:

Ishan Mehta
Legislative Assistant for U.S. Senator Brian Schatz

Erica Andeweg
Senior Policy Advisor to U.S. Senator Deb Fischer

Steven Kelly
Special Assistant to the President and
Senior Director for Cybersecurity and Emerging Technology,
National Security Council, The White House

Andrea Amico
Founder, Privacy4Cars

Chris Autry
CEO, Iothic

Jon Boulos
Wisconsin IoT Council

Hilary Cain
Senior Vice President of Policy,
Alliance for Automotive Innovation

Sven Dharmani
Global Advanced Manufacturing &
Mobility Supply Chain Leader,
Ernst and Young

David Duncan
Innovation Consultant,
Strategy of Things

Donald Davidson
Director, Cyber-SCRM Programs,
Synopsys

Paul Eisler
Vice President,
US Telecom - The Broadband Association

Dr. Amit Elazari
CEO and Co-Founder,
Open Policy Group

Angela Fernandez
Senior Vice President,
GS1 US

Manu Fontaine
Founder and CEO,
Hushmesh

Mei Lin Fung
Chair,
People Centered Internet

Syed Zaeem Hosain
Founder, CTO Emeritus and Chief Evangelist,
Aeris

Jeff Jockisch
Partner,
Avantis Privacy

Mobeen Khan
CEO,
Blue Wireless

Jim Kohlenberger
Co-Chair,
Trusted Future

Rajesh Krishnan
Head of Product Marketing,
Asimily

Dr. Joseph Kvedar
Professor of Dermatology,
Harvard Medical School and Mass General Brigham Hospital

John Marinho
Vice President Technology and Cybersecurity,
CTIA

Kathleen McTigue
Economic Specialist, Technology Partnerships Office,
NIST

Christopher Moore
President,
Mission Critical Insights, LLC

Dr. Jayne Morrow
Senior Advisor on Standards Policy,
NIST

Renil Paramel
Senior Partner,
Strategy of Things

Christopher Reberger
Partner,
Strategy of Things

Harvey Reed
Blockchain Capability Lead,
MITRE

Renee Roland
Special Counsel,
Public Safety and Homeland Security Bureau, FCC

Kathleen Scott
CTIA

Colby Scullion
CEO,
Avantis Privacy

Eric Simone
Founder and CEO,
Clearblade

Angela Smith
Technical Lead, Supply Chain Risk Management Program,
NIST

Joe Weiss
Managing Partner,
Applied Control Solutions

All meetings of the IoT Advisory Board were recorded, and the recordings are available on the IoTAB's website[293] together with the minutes and copies of any slide decks or materials provided by speakers and other commenters on the work of the IoTAB.

[293] The IoT Advisory Board website is https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/iot-advisory-board

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 third-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 return merchandise authorizations (RMAs) and bug fixes, and upgrades based on changing customer needs.

In addition, the new product line may be more attractive to buyers and allow 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 on 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 do 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 an IoT solution but require the buyer to install and set up the solution or find a third-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 and 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 third 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 socioeconomic scale from having these devices.

Table of Abbreviations

AAM	Advanced Air Mobility
ADPPA	American Data Privacy and Protection Act
AI	Artificial Intelligence
AIoT	Artificial Internet of Things
AIS	Automated Indicator Sharing
APEC	Asia-Pacific Economic Cooperation
AQ	Air Quality
AR	Augmented Reality
ARPA	Advanced Research Projects Agency
ASCE	American Society of Civil Engineers
AASHTO	American Association of State Highway and Transportation Officials
AV	Automated Vehicle
AWS	Amazon Web Services
BABA	Buy America, Build America
BIL	Bipartisan Infrastructure Law
BIM	Building Information Modeling
CAGR	Compound Annual Growth Rate
CBP	Customs and Border Protection
CCPA	California Consumer Privacy Act
CDC	Centers for Disease Control and Prevention
CET	Critical and Emerging Technologies
CIA	Confidentiality and Integrity and Assurance
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CPA	Colorado Privacy Act
CPRA	California Privacy Rights Act
CPS	Cyber-Physical System
CRQC	Cryptanalytically Relevant Quantum Computer
CSIS	Center for Strategic and International Studies
CTDPA	Connecticut Data Privacy Act
CTO	Chief Technology Officer
CV	Connected Vehicle
DBOM	Digital Bill of Materials
DDoS	Distributed Denial-of-Service
DFAR	Defense Federal Acquisition Regulation
DHS	Department of Homeland Security
DHHS	Department of Health and Human Services
DICOM	Digital Imaging and Communications in Medicine
DL	Deep Learning
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
ECG	Electrocardiogram
EHR	Electronic Health Records
EIA	U.S. Energy Information Administration
EMT	Emerging Technology
EPA	Environmental Protection Agency
EPHI	Electronic Protected Health Information
ERP	Enterprise Resource Planning
EV	Electric Vehicles
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FD&C	Food, Drug, and Cosmetic

FDOT	Florida Department of Transportation
FEDVTE	Federal Virtual Training Environment
FHIR	Fast Healthcare Interoperability Resources
FLOW	Freight Logistics Optimization Works
FRM	Future Railway Mobile Communication System
FRMCS	Future Railway Mobile Communication System
FTC	Federal Trade Commission
GCTC	Global City Teams Challenge
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GED	General Educational Development
GIST	Global Innovation through Science and Technology
GSA	General Services Administration
HBCU	Historically Black Colleges and Universities
HBOM	Hardware Bill of Materials
HIPAA	Health Insurance Portability and Accountable Act
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity and Access Management
ICS	Industrial Control Systems
ICTS	Information and Communication Technologies
ID	Identifier
IHE	Integrating the Healthcare Enterprise
IIOT	Industrial Internet of Things
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
ITS	Intelligent Transportation System
ITU	International Telecommunications Union
ITXPT	Information Technology for Public Transport
KEV	Known Exploited Vulnerabilities
KPI	Key Performance Indicators
KSE	Kyiv School of Economics
LEO	Low-Earth Orbit
LiDAR	Light Detection and Ranging
LPWAN	Low Power Wide Area Networks
LTE	Long-Term Evolution
MBDA	Minority Business Development Agency
MEP	Manufacturing Extension Partnership
ML	Machine Learning
MR	Mixed Reality
MVA	Manufacture Value Added
NAIAC	National Artificial Intelligence Advisory Committee
NCCOE	National Cybersecurity Center of Excellence
NDAA	National Defense Authorization Act
NEMA	National Electrical Manufacturers Association
NEVI	National Electric Vehicle Infrastructure
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	Networking and Information Technology Research and Development
NLOS	Non-Line-of-Sight
NOAA	National Oceanic and Atmospheric Administration
NPRM	Notice of Proposed Rulemaking
NSF	National Science Foundation

NSTAC	President's National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
NYCDOT	New York City Department of Transportation
O&M	Operations and Maintenance
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
PBD	Privacy by Design
PCAST	President's Council of Advisors on Science and Technology
PET	Privacy-Enhancing Technologies
PHI	Protected Health Information
PII	Personally Identifiable Information
PLC	Programmable Logic Controllers
PLM	Product Lifecycle Management
POC	Proof of Concept
PPDSA	Privacy-Preserving Data Sharing and Analytics
PPE	Personal Protective Equipment
PPP	Public-Private Partnerships
PQC	Post Quantum Computing
PRC	People's Republic of China
PSA	Public Service Advertising
PTC	Positive Train Control
PV	Photovoltaic
QC	Quantum Computing
QR	Quick Response
QRNG	Quantum Random Number Generation
R&D	Research and Development
RFID	Radio Frequency Identification
RFP	Request for Proposals
ROI	Return on Investment
SB	Small and Disadvantaged businesses
SBA	Small Business Administration
SBIC	Small Business Investment Companies
SBIR	Small Business Innovative Research
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SCIRA	Smart City Interoperability Reference Architecture
SCSEP	Smart Community and Sustainability Extension Partnerships
SDB	Small and Disadvantaged Businesses
SDO	Standards Development Organizations
SMB	Small and Medium sized Businesses
SME	Small and Medium Enterprises
SSDF	Secure Software Development Framework
STEM	Science, Technology, Engineering, and Mathematics
SBTT	Small Business Technology Transfer
THEA	Tampa Hillsborough Expressway Authority
TIES	Trusted IoT Ecosystem Security
TLS	Transport Layer Security
TMF	Technology Modernization Fund
TTC	Technology Trade Council
UAS	Unmanned Aircraft System
UF	University of Florida
UI	User Interfaces

USDA	U.S. Department of Agriculture
USMCA	United States-Mexico-Canada Agreement
USTR	United States Trade Representative
UUID	Universally Unique Identifier
VC	Venture Capital
VR	Virtual Reality
WAVE	Welcoming All Valuing Everyone
XAAS	Everything-As-A-Service
XR	Extended Reality
ZB	Zettabytes