



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

June 13, 2024 In-process Pre-read Draft

IoT Advisory Board Members

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

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

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

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

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

Steven E. Griffith, Executive Director, National Electrical Manufacturers Association

Tom Katsioulas, Chair, Trusted IoT Ecosystem Security (TIES) - Global Semiconductor Alliance

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

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

Ann Mehra, 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.

Working Draft IoT AB report

IoT Advisory Board Members.....	2
Executive Summary.....	6
IoT unlocks economic prosperity, innovation, and societal well-being.....	6
Key challenges are hindering IoT adoption and scaling	7
Strategic Government leadership is needed to facilitate adoption.....	9
Call to Action: Leading the Way Forward.....	9
Background.....	11
Introduction to the Internet of Things	16
What is IoT?.....	16
What can IoT do?	18
The Current State of IoT	22
The Future of IoT.....	27
The Evolution of IoT	27
A Vision for the IoT Enabled Economy	28
Promoting the IoT Enabled Economy.....	30
IoT Economy Potential to GDP.....	35
Findings of the IoT Advisory Board.....	37
General Findings – Specific Considerations.....	37
Industry findings – Specific Considerations.....	73
Finding 26: IoT technologies in the industrial sector need to be properly and responsibly governed and applied.....	92
Recommendations of the IoT Advisory Board	94
Establishing a National IoT Strategy	95
Key Recommendation KR1.1: Establish a United States national strategy for taking full advantage of the opportunity presented by the IoT.....	95
Innovation Leadership.....	101
Key Recommendation KR1.2: Congress should accelerate IoT technology innovation to support an evolving IoT.....	101
International Leadership.....	108
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.....	108
Key Recommendation KR1.4: The Executive Branch should lead by example by specifying, procuring and adopting IoT by federal agencies for its internal use.....	110
Modernizing IoT Infrastructure	115
Promoting Existing Methods	115
Key Recommendation KR2.1: The Executive Branch should promote collaborative development across industries to adopt existing industry standards and protocols.....	115

Working Draft IoT AB report

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.	121
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.	125
Key Recommendation KR2.4: The Executive Branch should encourage digital infrastructure initiatives to the digital transformation of enterprise business processes.	130
Establish Trust in IoT	135
Cybersecurity Improvement.....	135
Key Recommendation KR3.1: Congress and the Executive Branch should provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach.....	135
Data Privacy Policy and Regulation.....	141
Key Recommendation KR3.2: Congress should pass comprehensive federal privacy legislation.	141
Privacy Protections and Transparency for IoT.....	145
Key Recommendation KR3.4: 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.....	150
Fostering an IoT-Ready Workforce.....	153
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.....	153
Facilitating Industry Adoption of IoT.....	158
Leverage Federal Grants and Programs To Improve IoT Technology Use.....	158
Key Recommendation KR5.1: Congress should consider new financial models for sustaining and supporting programs when evaluating IoT project feasibility.....	158
Leading the Way for IoT Adoption in Agriculture.....	160
Key Recommendation KR5.2: Congress and the Executive Branch should develop a comprehensive Agricultural IoT Strategy.	160
Leading the Way for IoT Adoption Through Smart Communities	163
Key Recommendation KR5.3: Congress and the Executive Branch should implement specific actions to further promote IoT adoption through smart communities.	163
Leading the Way for IoT Adoption for Public Safety	167
Key Recommendation KR5.4: The Executive Branch should promote IoT adoption that will improve public safety.....	167
Leading the Way for IoT Adoption for Health Care	169
Key Recommendation KR5.5: Congress and the Executive Branch should promote IoT adoption in the health care industry.....	169
Sustainability / Environmental Monitoring	172

Working Draft IoT AB report

Key Recommendation KR5.6: Congress and the Executive Branch should promote IoT adoption that will improve sustainability and environmental monitoring.	172
Smart Transportation	177
Key Recommendation KR5.7: Congress and the Executive Branch should promote IoT adoption in Smart Transit and Transportation.	177
Promoting an IoT Enabled Economy.....	179
Key Recommendation KR6.1: The Executive Branch should monitor and evaluate progress of IoT adoption for supply chain logistics.....	179
Public and Private Partnership.....	181
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.....	181
Key Recommendation KR6.3: Actively promote and support the adoption of AI in IoT applications to improve decision-making, optimize resource utilization, and enhance productivity.....	184
Key Recommendation ER6.4: Congress and the Executive Branch should provide overarching regulatory guidance for the unmanned aerial systems (drone) industry.	186
Key Recommendation KR6.5: The Executive Branch should promote and facilitate equity in the accessibility, realization and distribution of value and benefits created from the adoption and use of IoT.....	187
Conclusion	189
References	190
Acknowledgements	191
Appendix A: IoT Stakeholders	192
Table of Abbreviations.....	197

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 accelerate economic leadership

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 will enable 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:

- **Supercharge economic growth.** IoT can unlock possibilities and efficiencies that were once deemed unimaginable to redefine industries, create new business models, increase competitiveness, and empower small businesses to innovate. Smart manufacturing keeps American factories competitive against overseas competitors. Precision agriculture innovations increase crop yields while minimizing inputs in changing climate conditions. Businesses becoming more profitable, enabled by smart supply chains that are agile and resilient.
- **Increase public safety.** IoT can enable agile and effective actions to prevent, protect, mitigate, respond and recover from man-made and natural disasters and hazards. Sensors embedded in roads 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 use of renewable energy sources. Smart buildings reduce energy consumption. Smart traffic management systems optimize traffic flow while reducing congestion and emissions. And circular supply chains enabling marketplaces while reducing waste and pollution.

- **Individualize healthcare.** IoT is a catalyst for redefining patient care, clinical practices, and the overall healthcare landscape. Wearable devices 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 vast amounts of patient data which is 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.
- **Facilitate equitable quality of life and well-being.** IoT provides innovative ways of enabling equitable outcomes. Smart medical devices 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.
- **Accelerate adoption and increase potential with AI.** While IoT devices generate massive amounts of data from the physical world, AI provides the tools to analyze and act on this data in real-time. The integration of IoT and AI is crucial as it enhances data analysis, automation, and decision-making across various sectors. This synergy leads to improved efficiency, personalized experiences, proactive maintenance, and smarter resource management, significantly advancing healthcare, manufacturing, smart cities, and more, while driving innovation and improving quality of life and our economy.

The value of an IoT-enabled economy can no longer be understated. IoT is no longer just a device connected to the internet but is evolving to integrated components within larger ecosystems (e.g., 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 also 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 fallen short. The U.S. is not alone. Over the past decade, industry analysts* have noted that global economic investment in IoT has fallen short of estimated targets due to slow adoption, with

shortcomings attributed to a variety of factors, such as change management, cost, talent, and cybersecurity. Recent estimates* show that IoT is still growing from \$56.3 billion to \$370.2 billion, and a survey of industry leaders found that 27% have deployed and 78% plan to deploy in the next two years. However, the rate of adoption is smaller, and occurs over a longer period of time.

This IoT Advisory Board (IoTAB) was chartered to assess the challenges and identify recommendations that position U.S. leadership to seize economic and societal opportunities that benefit government, organizations, communities and Americans. The board identified general findings and specific considerations that reveal ways in which the US can close existing gaps. These findings could be repositioned to allow US leadership to accelerate adoption and growth, increase capabilities and resources, bridge a future landscape, and address cross sector critical gaps as called out in the charter for this report.

Challenges	Findings
Adoption and Growth	<ul style="list-style-type: none"> • Industry has slow adoption • Lack of national coordination • Hinderance of innovation • Lack of Equity & Opportunities • Significant Barriers for Small businesses • Interoperability Challenge • Connectivity Challenges • Lack of Trust
Capabilities and Resources	<ul style="list-style-type: none"> • Startups that drive new technology • New business models and platforms to scale • AI critical to unlocking value of IoT • Insufficient people / skills
Future Landscape	<ul style="list-style-type: none"> • Business partnerships needed for solutions • Digital marketplaces to fuel economic growth • Convergence of AI /IoT can boost potential
Across Sectors (as identified in the charter)	<ul style="list-style-type: none"> • Agriculture • Communities and Infrastructure • Transportation • Healthcare • Augmented and traceable supply chains • Environmental Sustainability • Public Safety

Each of these findings is linked in the report to themes, key recommendations, and their enabling recommendations. Addressing these challenges presents tangible benefits to the larger US economy including job creation, workforce development, market access, resource optimization, and synergies between technological advancements. Such examples include:

- **Widespread IoT adoption and growth** offer a historic opportunity for US leadership, achievable by overcoming adoption hurdles and fostering a

coordinated national strategy to drive innovation, inclusive growth, and a thriving business ecosystem of all sizes.

- **Capabilities and resources** like fostering innovative startups, developing scalable business models for IoT, and integrating AI expertise are crucial to unlocking the full potential of this technology, despite current skill gaps.
- **Future landscape** Investing in capabilities like nurturing startups, fostering new business models leveraging IoT, and integrating AI with IoT will unlock their full potential, bringing economic benefits and building a skilled workforce.
- The charter calls for **critical sector** needs to be addressed that would frame new opportunities to accelerated adoption across industries including agriculture, healthcare, transportation, environment sustainability, public safety, and their communities and infrastructure.

Call to Action: Leading the Way Forward

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

The US 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 board's findings and groups actionable recommendations under overarching themes that serve to guide the US towards an IoT-empowered future. This includes experiences and perspectives from a cross-section of industry, local government, academia and other private-sector experts.

The report 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 board further urges the Federal Working Group and Congress to study these recommendations and adopt those that will best serve the needs of this nation.

We urge Congress, the Executive Branch and the IoTFWG to:

- Be visionary and bold in formulating a strategy
- Act with urgency and decisiveness on key priorities
- Bring a whole-of-government coordinated approach
- Monitor progress, measure outcomes, and report periodically

Note: The following text was marked for deletion. I'm not sure if that is an error or not, so including it here for consideration.

Next Steps: Leading the Way Forward

The US 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 board's findings and groups actionable recommendations under overarching themes that serve to guide the US towards an IoT-empowered future. This includes experiences and perspectives from a cross-section of industry, local government, academia and other private-sector experts.

The report 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 board further urges the Federal Working Group and Congress to study these recommendations and adopt those that will best serve the needs of this nation.

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

IoT Unlocks Areas of US Economic Prosperity

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. 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:

- **Supercharge economic growth.** IoT can unlock possibilities and efficiencies that were once deemed unimaginable to redefine industries, create new business models, increase competitiveness, and empower entrepreneurs to innovate. Smart manufacturing keeps American factories competitive against overseas competitors. Precision agriculture innovations increase crop yields while minimizing inputs in changing climate conditions. Businesses are supported by smart supply chains that are agile and resilient.
- **Increase public safety.** IoT can enable agile and effective actions to prevent, protect, mitigate, respond and recover from man-made and natural disasters and hazards. Sensors embedded in roads 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 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 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 vast amounts of patient data which is analyzed to deliver personalized and precision medical treatments.
- **Facilitate equitable quality of life and well-being.** IoT provides innovative ways of enabling equitable outcomes. Smart medical devices 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.

Strategic Government leadership is needed to facilitate adoption

The Approach to Action

The IoT Advisory Board (e.g., IoTAB or the board) developed initial recommendations and refined them with initial feedback in collaboration with industry participants and the IoT Federal Working Group (IoTFWG), the recipient of this report's recommendations. The Board has continued to consider the potential 'calls to action'.

The IoTAB's recommendations are organized around six major themes. These themes represent elements that are fundamental to facilitate, accelerate and sustain the adoption and integration of IoT into the American economy and society.

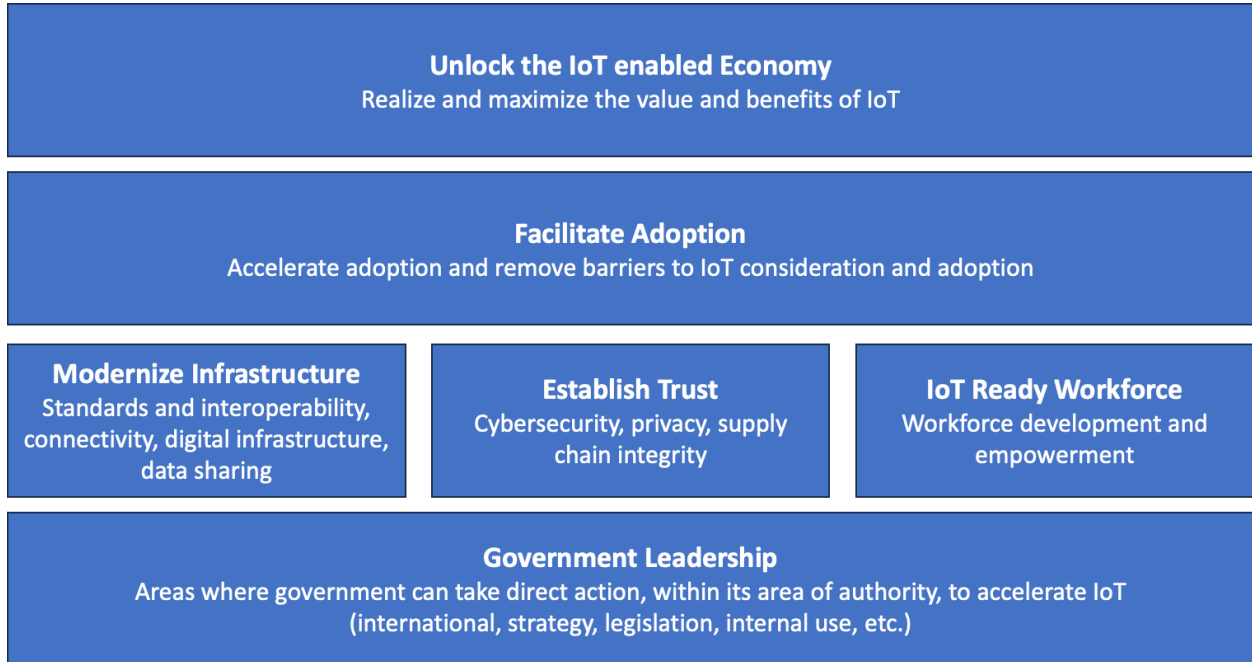


Figure 1. Caption Here

Each theme has an objective, several key recommendations, and enabling recommendations as the 'calls to action'. The enabling recommendations support the key recommendation and each enabling recommendation is associated to the IoTAB findings.

Key Recommendations

Comment: I would at this stage add a table or graphic (in landscape mode) showing all the recommendations (at least the key recommendations) before going into a breakdown of them. This gives the reader a birds-eye view of the key recommendations and themes in one easy to consume view.

Theme	Objective	Key recommendations
Leadership	create and implement a coherent comprehensive coordinated national IoT strategy,	<ul style="list-style-type: none"> Establish a strategic national approach for taking full advantage of the opportunity presented by the IoT. Accelerate IoT technology adoption as well as manufacturing for small businesses and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. Promote international collaboration in IoT adoption across global supply chains to share knowledge, best practices, and resources.
Modernize infrastructure		
Establish trust		
IoT-ready workforce		
Facilitate adoption		
Unlock IoT-enabled economy		

Figure 2. Caption Here

Priorities

The board has identified a number of high priority recommendations. These are recommendations that are strategic in nature, provides foundation and structure to enable sustained and accelerated adoption and value realization, or leverages existing initiatives and programs to drive rapid and effective action.

Need to poll the board to identify what could fit here.

- Build a national IoT strategy (Brief reason and recommendation number)
- Include IoT in the national comprehensive privacy legislation

Background

In January 2020, Congress enacted the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. That act established the Internet of Things Advisory Board (IoTAB) within the Department of Commerce.¹ In accordance with the Federal Advisory Committee Act, as amended, the IoT Advisory Board (IoTAB) was chartered in December 2021.

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

Description of Duties. The Board shall advise the Working Group with respect to:

- a. the identification of any Federal regulations, statutes, grant practices, programs, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development of the Internet of Things;
- b. situations in which the use of the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States, including benefits from or to:
 - i. smart traffic and transit technologies;
 - ii. augmented logistics and supply chains;
 - iii. sustainable infrastructure;
 - iv. precision agriculture;
 - v. environmental monitoring;
 - vi. public safety; and
 - vii. health care;
- c. whether adequate spectrum is available to support the growing Internet of Things and what legal or regulatory barriers may exist to providing any spectrum needed in the future;
- d. policies, programs, or multi-stakeholder activities that:
 - i. promote or are related to the privacy of individuals who use or are affected by the Internet of Things;
 - ii. may enhance the security of the Internet of Things, including the security of critical infrastructure;
 - iii. may protect users of the Internet of Things; and
 - iv. may encourage coordination among Federal agencies with jurisdiction over the Internet of Things;
- e. the opportunities and challenges associated with the use of Internet of Things technology by small businesses; and
- f. any international proceeding, international negotiation, or other international matter affecting the Internet of Things to which the United States is or should be a party.

¹ The work was described in Public Law No. 116-283, Section 9204(b)(5)

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).
- **When the NIST Director will submit the IoTAB report to Congress.**
- 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.



Introduction to the Internet of Things

What is IoT?

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

From a technology perspective, IoT have sensors that collect real world data and actuators that perform actions in the physical environment based on the processing of the data collected. IoT data is either processed locally on the device, by an on-premises processor (“the edge”) or sent over the internet to be handled off-premises (“the cloud”). The “cloud” collects the data, normalizes it, stores it, analyzes it and acts on it according to algorithms or manually by users. The information is then 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, a vibration sensor 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 will disrupt manufacturing operations.

A high level IoT technical architecture is shown below in Figure 3.

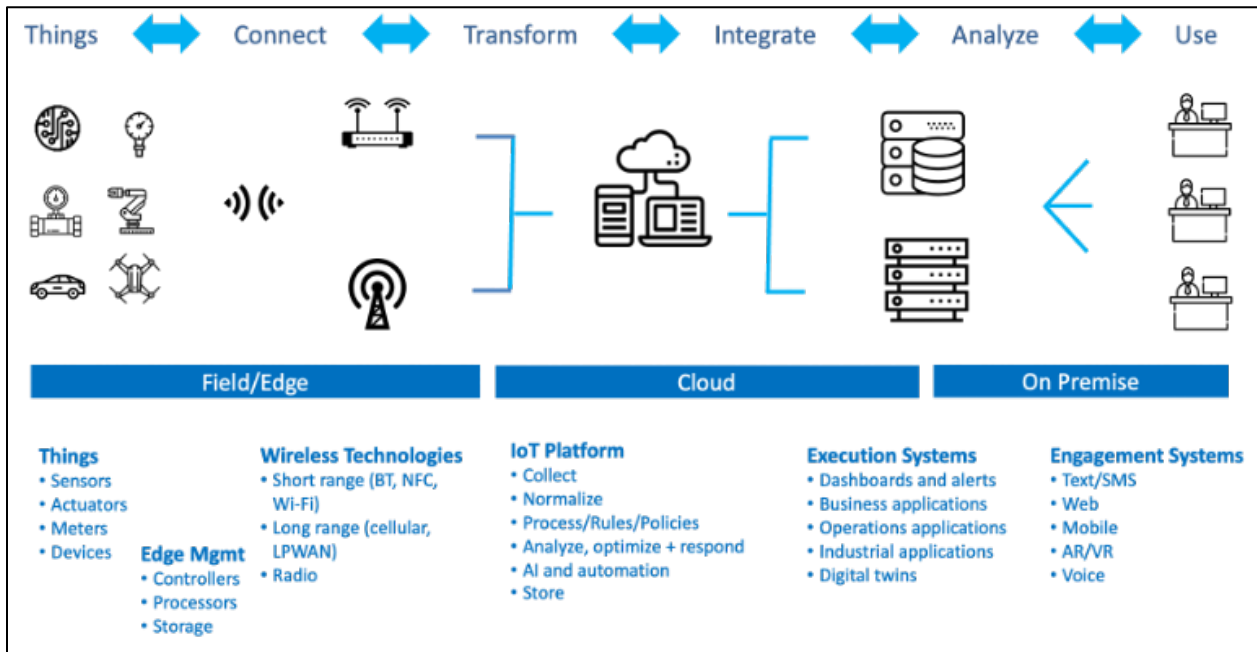


Figure 3. High-Level Internet of Things Architecture

What can IoT do?

IoT creates new value

From an economic perspective, adding sensors and actuators to the internet yields value from doing old things in new ways and seeing new things done in ways that were not possible before.

Create a graphic around 3 or 4 IoT applications (describing application, problem being addressed, benefits created. We can pull some use cases from the smart home, consumer, industrial, etc.)

1. Asset tracking
2. Machine Condition Monitoring
3. Predictive maintenance
4. Autonomous Farming

IoT Transforms Business Models

Adding connectivity and sensors to traditional products create smart connected products. These products allow suppliers to create innovative offerings based on new business and operating models, leading to new revenue streams not previously available with traditional products. In this way, suppliers transform from just selling “products” to become “smart solutions suppliers” offering products, IoT-enabled smart services, and “product as a service”. This allows suppliers to become more aligned with their customers, increasing their competitiveness and value, and ultimately, profitability.

For example, connected sensors on IoT-enabled equipment allows jet engine manufacturer Rolls Royce to take over the responsibility for engine maintenance from the airlines (TotalCare “Power by the Hour”). In return for a fixed cost per flying hour, Rolls Royce will actively manage the engine through its lifecycle to achieve maximum flying availability while the airlines will have a predictable cost of ownership.²

For buyers and users, these new offerings provide increased value and relevance with services and capabilities that may not be possible before. For example:

- Suppliers sell “outcomes” delivered by products instead of products. The Rolls Royce TotalCare “Power by the Hour” model sells “flying availability”. The money saved by buying “outcomes” can be redeployed to another part of the business that could be put to better use. For suppliers, this model enables focus on customer success, and provides them with a sustainable recurring revenue stream instead of a one-time sale.
- Product suppliers and their dealers have traditionally relied on two sources of revenues – sales of equipment and service contracts. Connected systems allow

² <https://www.rolls-royce.com/media/our-stories/discover/2017/totalcare.aspx>

dealers to offer managed services to 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, in maritime IoT a shipping company can collect fleet data and make it available to charterers, insurance companies, classification societies, and academia.
- Product suppliers become software providers by extending its IoT platform to other makers. For example, Amazon’s Alexa smart speakers allow other smart products to integrate to its platform. This extends the product ecosystem, and allows other products to interoperate and collaborate together to create an end-to-end solution to customers.

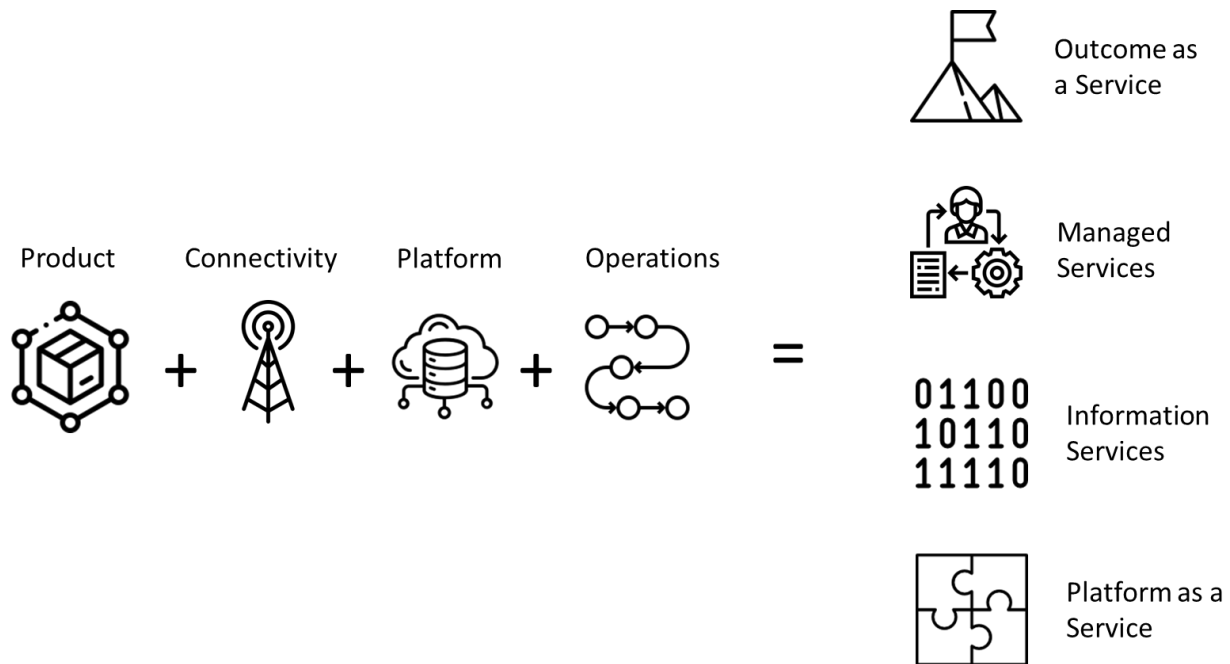


Figure 4. Caption to be added

IoT Transforms Business Ecosystems

Smart, connected products reshape value and change the way product manufacturers compete. The basis of competition shifts from selling discrete products to offering product systems to systems of systems, to platform ecosystems and marketplaces³.

A car integrating sensors, software and connectivity, adds new value beyond a traditional “dumb” car. The smart car allows the manufacturer’s dealers to monitor the

³ <https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition>

status of the car, determine its maintenance needs, and optimize gas mileage performance by studying the data collected.

Suppliers extend their value to customers by allowing complementary products from other suppliers to use software platforms. This creates a product system where different product makers partner together to share a common platform, exchange data, collaborate together. For example, a manufacturer can allow 3rd party smart speakers to be integrated to its software, allowing drivers to integrate voice commands to control some car functions. Insurance companies can develop and integrate in telematics systems to 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 experience and lower ownership costs.

In this way, a new business ecosystem is formed. The automobile maker is no longer competing against other car manufacturers, but against other mobility ecosystems with its solution platform.

As these solution platforms grow in sophistication, their basis of value (and competition) increases as they become relevant in a broader ecosystem. For example, instead of competing at the car level, they compete at the “driver experience” level. In time, as IoT evolves in other sectors, the smart car ecosystem becomes part of the smart city ecosystem (Figure xx).

In an ecosystem environment,

- **Smart-connected product businesses evolve into solutions platforms.** From manufacturing to agriculture and aviation, similar opportunities and evolution are happening. The software platform and applications may differ, but the need for collaborative ecosystem partnerships remains the same. Companies that deliver smart-connected solutions with ecosystem partners capture high value.
- **Companies whose product platforms connect to other systems will capture more value** with ecosystem partnerships by expanding industry boundaries. For example, a coordinated approach across supply chains in transportation and logistics ecosystems will speed adoption, across connected industries accelerate supply chain resilience and enable new solutions.
- **Partnerships for end-to-end solutions will accelerate adoption and growth** by combining existing products with new technologies among stakeholders. Complex system-of-systems and solutions require orchestrated ecosystem collaboration with platforms that provide incentives for businesses to participate and share the innovation burden and economic value delivered.

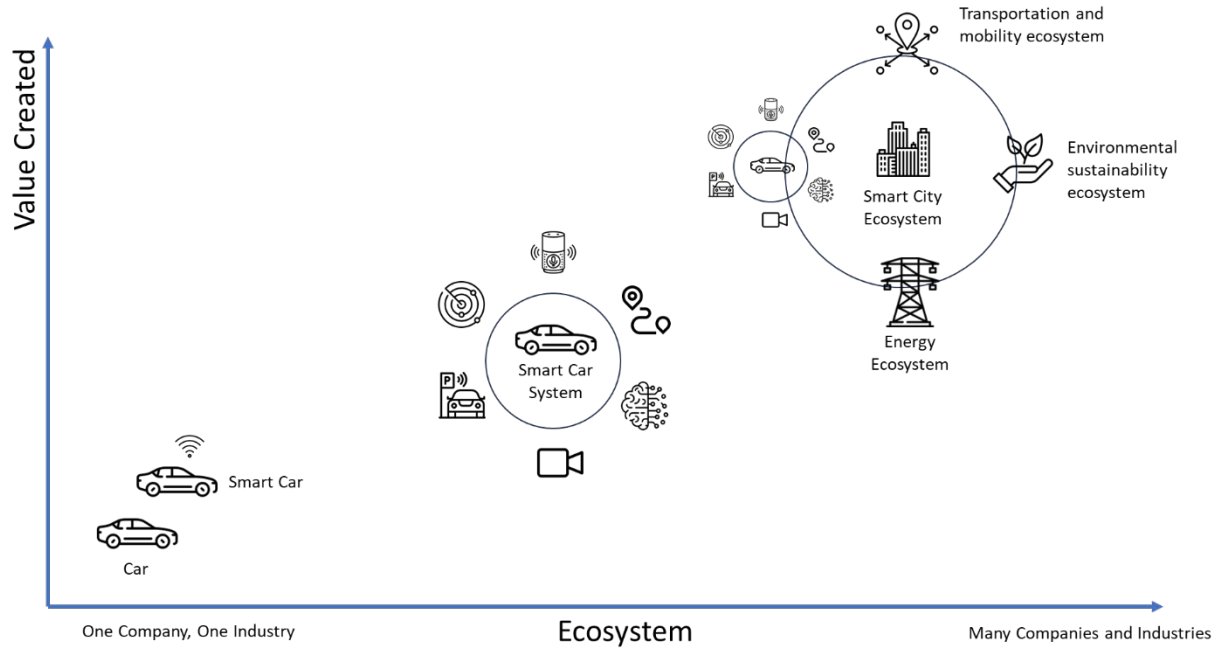


Figure 5. Caption to be added

The Current State of IoT

IoT Trends Worldwide.

In 2014 the World Economic Forum and McKinsey & Co. projected that IoT, and adjacent technologies (analytics, cloud computing, big data and ML/AL) will produce \$9.6 to \$21.6 trillion of value for the global economy by 2022⁴.

In 2021, McKinsey & Co. revised the IoT forecast drastically downward, projecting global value of only \$5.5 to \$12.6 trillion, and not reaching those targets until 2030⁵. The new projection covers the top nine categories, IoT adoption was less than anticipated. The firm clarified that the 2014 projection was off mainly due to headwinds related to change management, cost, talent, and cybersecurity. They also noted factors of slow market adoption of digitalization and cyber-resilience, particularly in large enterprises.

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

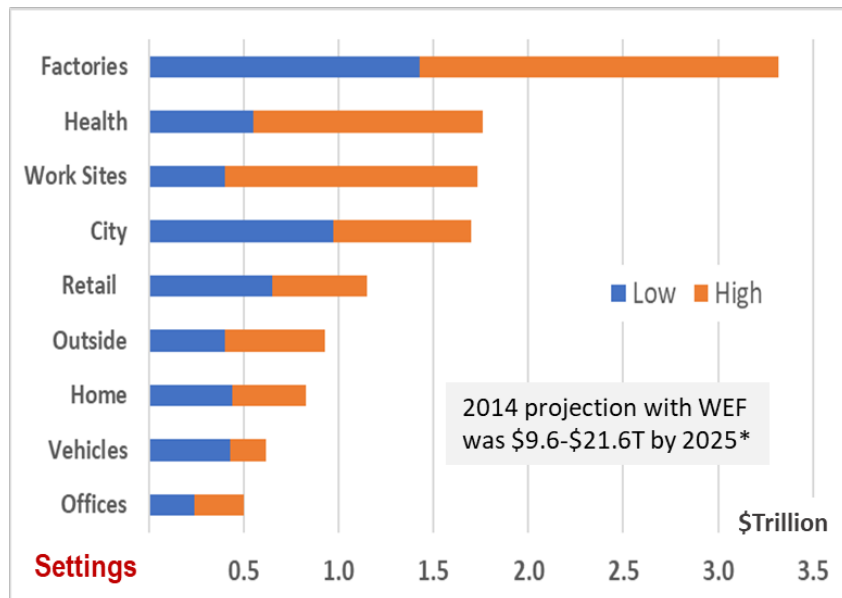


Figure 6. Caption to be updated

For each setting, the report cited a min-max range for projections factoring adoption rates, impact, and scale. It analyzed the settings for tailwinds and headwinds, opportunities and risks and ranked them based on size. *The convergence of physical and digital worlds enabled by IoT was cited as a fundamental trend underlying the digital transformation of businesses that can fuel the global economy.*

A key indicator for IoT growth projections is the number of connected devices. In 2016 Verizon noted, *“The installed base of IoT endpoints will grow from 9.7 billion in 2014 to*

⁴ www.weforum.org/press/2014/01/increased-cyber-security-can-save-global-economy-trillions/

⁵ www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

more than 25.6 billion in 2019, hitting 30 billion in 2020⁶.” This was in line with most analysts’ expectations. In 2022 Verizon revised its projections downward estimating that there will be 14.4 billion connected IoT devices worldwide, an increase of roughly 18% over last year alone, with numbers climbing to 27 billion by 2025⁷.” More recent projections by McKinsey⁸ and Frost & Sullivan⁹ cited the in early 2023 there were 42 billion connected devices. Driven by AI, 5G, and big data, some analysts project that by 2030 the number of IoT devices could exceed 100 billion fueled by trillions of chips.

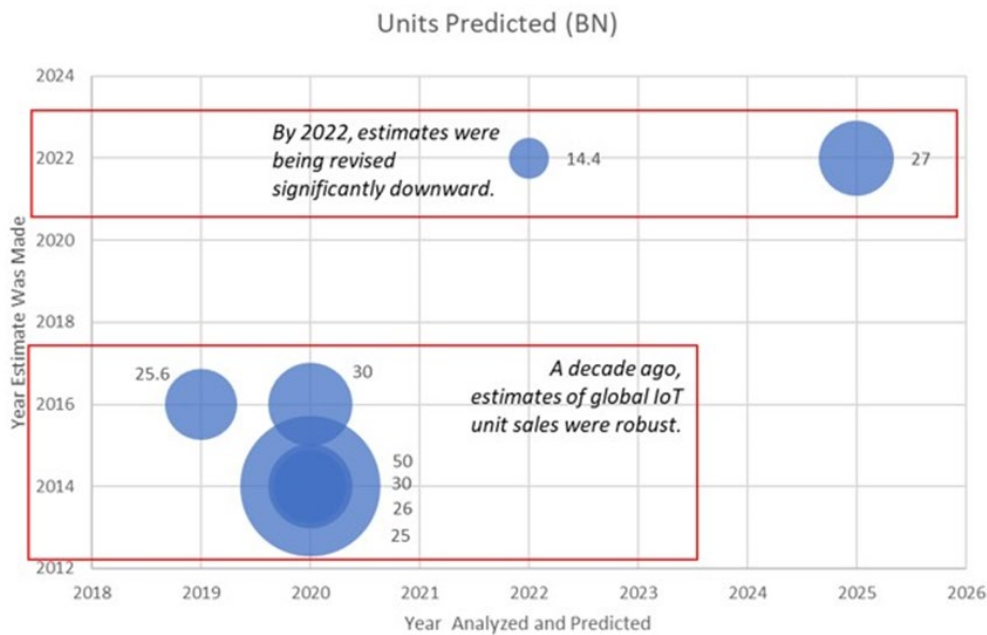


Figure 7. Caption to be updated

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

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. Some barriers to adoption cited 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.

IoT Trends in the U.S.

IoT and the US The adoption of IoT is growing in the United States, likely driven by digitalization of enterprises. Research published in the 2021 Microsoft IoT Signals

⁶ <https://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf>

⁷ <https://www.verizon.com/about/news/5g-iot-together-changing-our-world>

⁸ <https://www.mckinsey.com/industries/private-equity-and-principal-investors/our-insights/growing-opportunities-in-the-internet-of-things>

⁹ <https://www.insiderintelligence.com/insights/internet-of-things-devices-examples/>

found that 94% of business decision-makers, IT decision-makers and developers at U.S. enterprise organizations (1000+ employees) surveyed are “IoT adopters”¹¹, either learning about IoT, conducting a trial or proof of concept, or using IoT (Ibid Exhibit 2). Of this, 27% have projects in the “use” phase, while 78% reported that they are planning to use IoT more within 2 years (Ibid Exhibit 3). According to Fortune Business Insights, the value of the U.S. IoT market was \$195.48 billion, and it’s expected to quadruple by 2030¹².

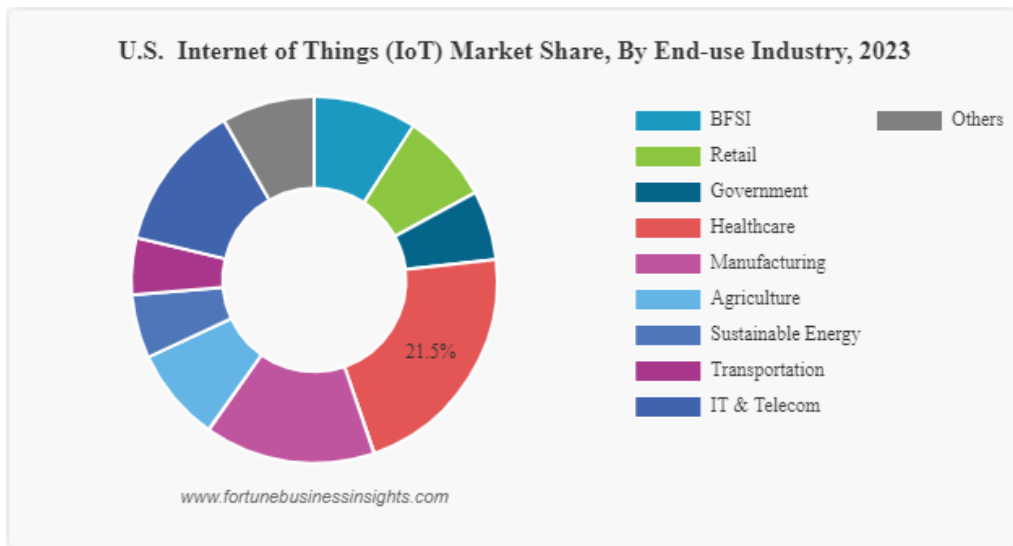


Figure 8. Caption to be updated

IoT is used across a variety of industries for different reasons. The adoption rate varies 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 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 automation, personalized customer experiences, and brand protection.

Transportation and logistics: IoT tracks real-time locations and quantities of goods, optimizing logistics and minimizing disruptions. Shipments of telematics devices are

¹¹ “IoT Signals - Edition 3|October 2021”, Microsoft, October 2021. Exhibit 3. [Link](#)

¹² <https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307>

increasing, with an estimated 160 million units by 2026. Embedded car OEM telematics units are also growing, with 375 million units projected by 2026.

Market Consolidation

The IoT market is an organically developing from a fragmented ecosystem of sensors, chips and processors, modules, devices and software platforms.¹³ The IoT platforms landscape is consolidating, as reported by IoT Analytics.¹⁴ The fragmented nature of the market and lack of ubiquitous end-to-end solutions has created confusion for IoT buyers who struggle with adopting IoT technology from many suppliers.

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

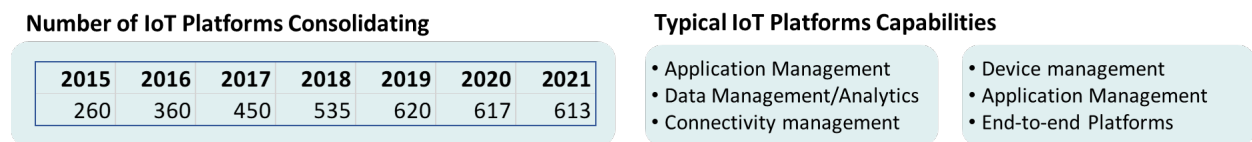


Figure 9 – Caption TBD

Telit acquires Thales’ cellular IoT products to establish Telit Cinterion
Source: [IoTNews](#), August 1, 2022

Semtech Corporation to Acquire Sierra Wireless
Source: [Semtech](#) Press Release, August 2, 2022

Google to shut down its IoT Core Services from Aug 2023; users seek options *Source: Business Standard, August 18, 2022*

Cisco Systems Pulls Back From Smart City Push *Source: Wall Street Journal, December 28, 2020*

IBM to fire Watson IoT Platform from its cloud
Source: The Register, November 15, 2022

Ericsson quits IoT – agrees sale of loss-making IoT Accelerator business to Aeris *Source: RCR Wireless News, December 7, 2022*

Figure 10 - IoT Market Consolidation – Representative News Headlines

¹³ IoT platform is a software system facilitating the development, deployment, and management of IoT applications.

¹⁴ <https://iot-analytics.com/iot-platform-companies-landscape/>

IoT market have been consolidating as evidenced by recent mergers, acquisitions and divestments including: IoT module maker Telit acquiring Thales cellular IoT division¹⁵; Semtech acquiring of Sierra Wireless¹⁶; Google exiting the IoT services business¹⁷ Ericsson selling its IoT business¹⁸ ; IBM shutting down Watson IoT¹⁹ ; SAP retiring IoT platform²⁰ ; and Cisco exiting smart city market.²¹

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

IoT Solutions Partnerships for Specific Use Cases

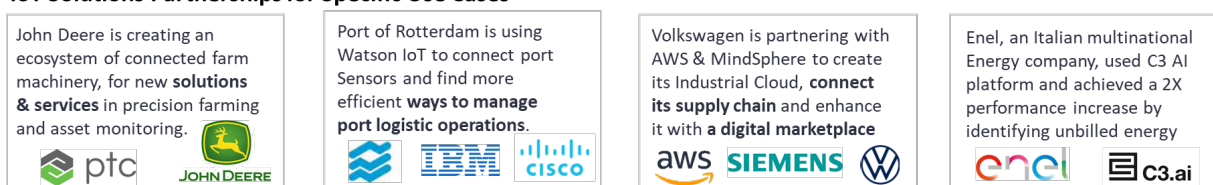


Figure 11. IoT Solutions Partnerships for Specific Use Cases

Since 2019, most of the remaining IoT Platform companies are transitioning into IoT solutions. In 2023, the top 10 companies controlled 65% of the market, compared to 58% in 2019 and 44% in 2016. Leading Hyperscalers (Microsoft, AWS, Alibaba, Google) in IoT, continued to outgrow the market with growth rates of 50%+ per year since their platforms enable business ecosystems and scalable revenue streams. Platform-based partnerships have led to successful collaborations for various market applications.

Technology Maturity

The technology enabling IoT continues to evolve. IoT is an evolving set of disparate technologies at various levels of maturity. While some are mainstream and mature, others are emerging and immature. Technologies such as cloud computing, IoT platforms, containers, supervised machine learning, IoT streaming analytics, cellular IoT and Low Power Wide Area Networks (LPWAN) have reached a certain level of maturity.²² Others are “coming up”, including edge data and app platforms, serverless/Function-as-a-Service, cloud-connected sensors, edge AI chips, and low code/no code development platforms and satellite IoT connectivity.²³ Still others like

¹⁵ “Telit acquires Thales’ cellular IoT products to establish Telit Cinterion,” R. Daws, IoT News, August 1, 2022. [Link](#)

¹⁶ “Semtech Corporation to acquire Sierra Wireless,” Semtech press release, August 2, 2022. [Link](#)

¹⁷ “Google to shut down its IoT Core Services from Aug 2023; users seek options, August 18, 2022. [Link](#)

¹⁸ “Ericsson quits IoT - agrees sale of loss-making IoT accelerator business to Aeris,” December 7, 2022. [Link](#)

¹⁹ “IBM to fire Watson IoT Platform from its cloud,” L. Clark, The Register, November 15, 2022. [Link](#)

²⁰ “SAP IoT Retirement and SAP Asset Performance Management,” S. Lee, SAP, October 5, 2022. [Link](#)

²¹ “Cisco Systems pulls back from smart city push,” A. Tilley, Wall Street Journal, December 28, 2020. [Link](#)

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

²³ *ibid.*

data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, QRNG chips, biodegradable sensors, 6G and quantum computing are only just hitting the market or are still in research labs. still “years out” and require continued research investments.²⁴

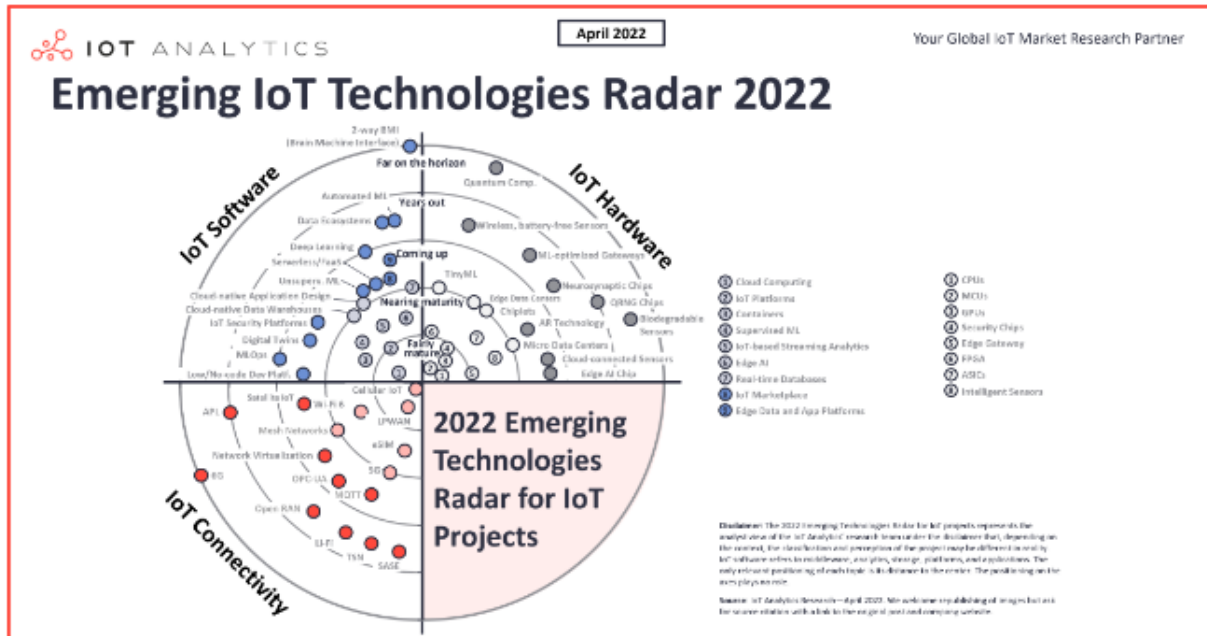


Figure 12. Caption to be updated

The Future of IoT

The Evolution of IoT

IoT will continue to evolve, driven by advancements and evolutions in the underlying technology (Figure xx). 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 economy, leading to new innovation, value creation, operational efficiency, and growth and prosperity.

²⁴ *ibid.*



The Future of IoT Solutions and Services

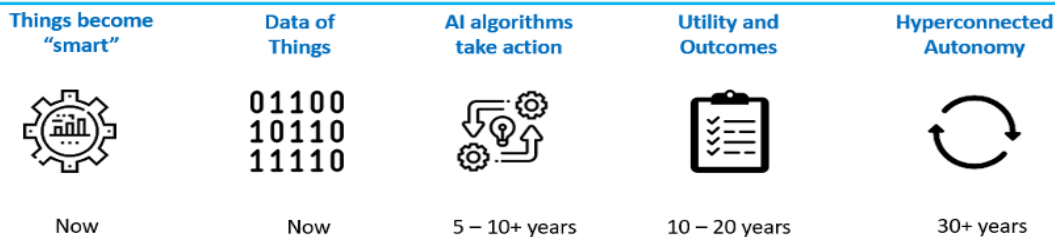


Figure 13. Evolution of IoT

The evolution of IoT is accelerated by a number of enablers, including:

- IoT devices integrate to form end-to-end solution platforms.** IoT devices, enabled by interoperability, link with other IoT devices to create connected device systems. Systems connect with other systems to create “systems of systems” and platforms offering “end-to-end” value within industries.
- IoT and AI converge.** AI unlocks the value of IoT by analyzing the vast amounts of data collected. These AI algorithms, running in cloud servers or on the devices itself, 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.
- Business ecosystems scale IoT benefits.** IoT facilitates new innovative solution offerings. Business ecosystems, built on industry platforms and business partnerships, scale these innovative offerings broadly to transform industries to smart industries.
- Strategic application of policies and regulations.** As IoT progresses in its evolution, it will be hindered by a variety of challenges, many of which are addressed by industry participants. Well-crafted government policies and regulations, created strategically in partnership with industry at the appropriate levels as needed, address challenges industry cannot resolve to continue IoT growth and evolution.

A Vision for the IoT Enabled Economy

The continuing evolution of IoT facilitates the creation of IoT platform-based industry ecosystems that develop and deliver innovative offerings and outcomes to the economy and civil society.

The internet facilitated the development of digital platform business models. A platform business model “creates value by facilitating exchanges between two or more interdependent groups, usually consumers and producers. In order to make these

exchanges happen, platforms 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.”²⁵ Examples of Internet digital platform businesses include eBay, Amazon and Facebook (now Meta).

The Internet of Things will facilitate the similar development of IoT-enabled digital platforms and models. Coupled with the ongoing digitalization of business and operations processes in enterprises across the economy, the integration of IoT device platforms into this digital infrastructure creates a platform developing, delivering and operating innovative solutions. Digital transformation initiatives for IoT²⁶ will further evolve business processes and functions. From predictive maintenance and asset tracking to personalized customer experiences and smart supply chain management, this digital transformation enables organizations to harness the power of IoT to enable new business models.

For example, an industrial supplier offers IoT-based “smart machines” to its factory customers. The smart machine is integrated with a software platform that enables the supplier to monitor real-time machine condition data and perform responsive actions. Technicians monitor machine usage and remotely service the equipment. Supplier and customers stakeholders review usage patterns and offer advice to optimize machine performance and efficiency. Operations teams predict maintenance needs and schedule downtimes to service the equipment.

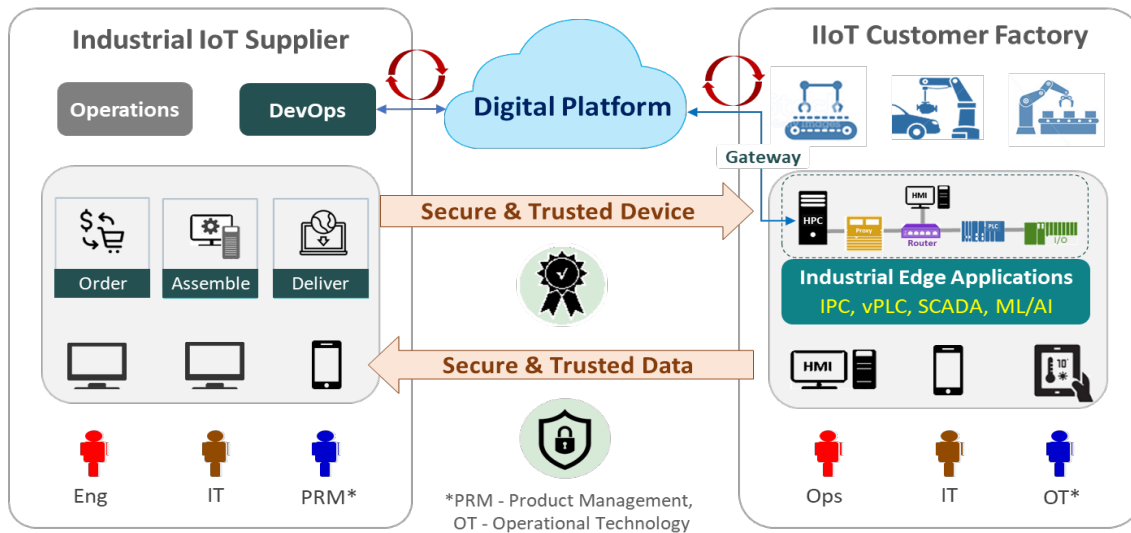


Figure 14. Caption to be updated

This example highlights how suppliers of Industrial IoT products become **Smart-connected IIoT suppliers** by digitalizing their operations, updating processes, and

²⁵ <https://www.appicoinc.com/blog/what-is-a-platform-business-model/>

²⁶ <https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/implementing-a-digital-transformation-at-industrial-companies>

leveraging digital platforms to connect with their customer using their IoT products real time. This enables IoT suppliers and customer 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 optimize workflows that lead to enhanced productivity.
- **Trusted data for digital twins**²⁷ ensure accurate simulations, timely predictive maintenance and better process optimization boosting operational efficiency.
- **Growth of XaaS**²⁸ **revenue streams** with value-added services and solutions, leading to stronger customer relationships and scalable economic value.

The extension of this platform from one supplier into the industry ecosystem, where it can be accessed by partners and customers, forms the base of the IoT-enabled economy. For example, third party service providers can be integrated into the platform to provide additional value-added services. Complementary equipment suppliers can integrate into the platform to provide a more complete solution offering.

These platforms help bring together internal and external capabilities, resources and expertise to drive efficiency and innovation in product development and IoT service delivery. From edge computing and sensor management to device provisioning and security, IoT-enabled platforms provide organizations with the means to harness the power of connected devices to drive operational efficiency, enhance customer experience, increase competitiveness and agility, and unlock new revenue streams.

Promoting the IoT Enabled Economy

The IoT enabled economy is built on a key set of building blocks (Figure xx1). These include:

- Enabling technologies provide the capabilities that allows IoT to function and create value by generating data used in analytics and AI applications.
- Digital platforms integrate devices, hardware and software technologies together to extend value and create broader end-to-end solutions
- Business ecosystems bring complementary suppliers with solutions built on digital platforms, resources and expertise to create and deliver sustainable value
- Orchestrated partnerships organize stakeholders, technologies, digital platforms and ecosystems to work together in a structured manner to create solutions

²⁷ <https://www.mckinsey.com/capabilities/operations/our-insights/digital-twins-what-could-they-do-for-your-business>

²⁸ <https://www2.deloitte.com/us/en/pages/consulting/solutions/xaas-everything-as-a-service-model.html>

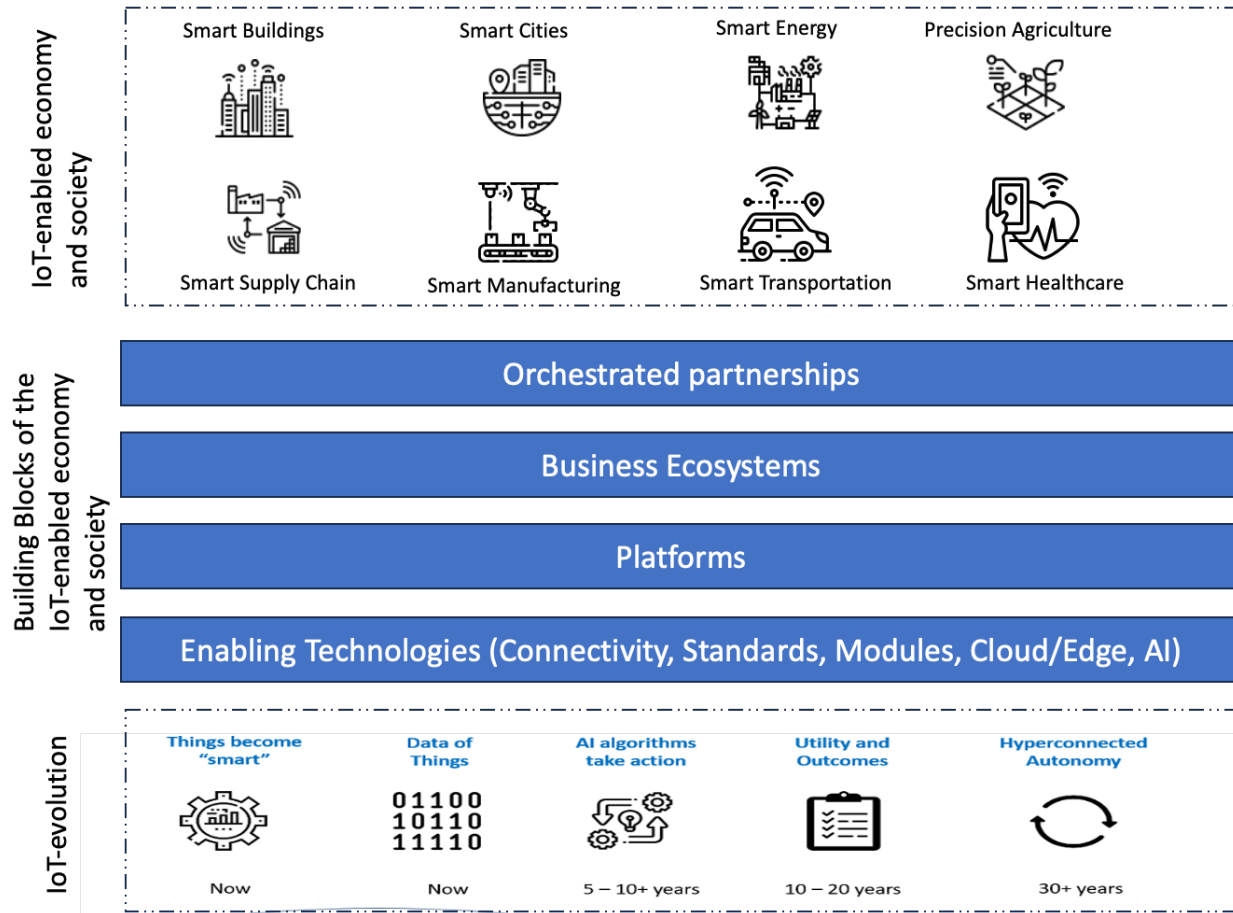
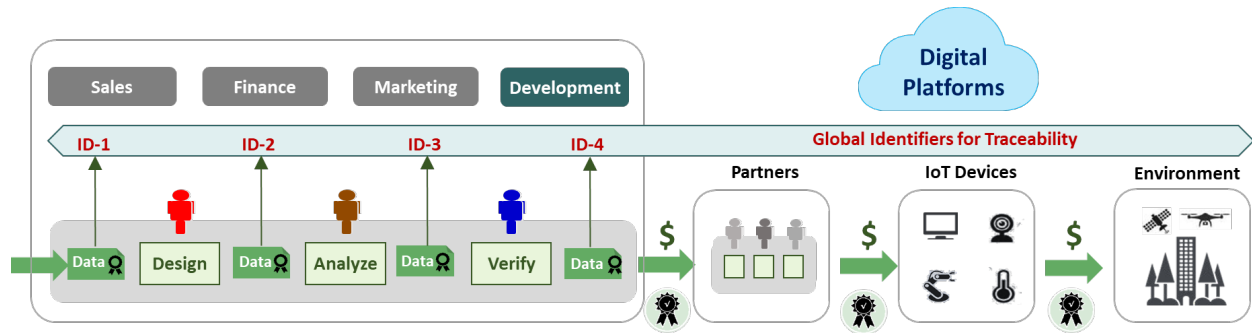


Figure 15. Caption to be updated

IoT Ecosystem Platforms

End-to-End IoT Solutions Platforms will evolve through increasing IoT connectivity. They will extend beyond device platforms to encompass the entire IoT value chain, from data acquisition and analytics to application development and deployment. These platforms offer comprehensive toolsets and services that enable organizations to design, deploy, and optimize IoT solutions tailored to their specific needs and objectives. By providing integrated workflows, data sharing capabilities coupled with analytics tools, end-to-end solutions platforms streamline the development process, accelerate time-to-market, and maximize the impact of IoT investments.



These digital platforms provide the technical foundation to foster collaboration, partnerships, and innovation within broader IoT ecosystems to drive economic growth. Extending these platforms to create an industry ecosystem platform can bring together diverse stakeholders, including technology providers, developers, enterprises, and government agencies, to co-create and exchange value.

By providing open APIs, digital tools, and mechanisms to share resources, ecosystem platforms will facilitate interoperability across diverse IoT domains, enabling new types of digital marketplaces²⁹ across IoT ecosystems. As the IoT landscape continues to evolve, these platforms will enable multi-stakeholder collaboration and innovation, unlocking new opportunities for differentiation, automation, and economic growth.

Platform-based IoT Business Ecosystems³⁰

Platform-based business ecosystems, built around a platform, comprise of complementary partners, resources, standards and tools. These have been long 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-competition among participants, platform-based business ecosystems drive innovation, monetization, agility, and scalability enabled through open architecture, governance, and network effects³¹, as proven by trillion-dollar platform companies.

Orchestrated Ecosystem Partnerships

Partnerships are critical to the development of the IoT enabled economy. End-to-end IoT solutions in the industry ecosystem are inherently complex, and involve multiple companies, technologies, and standards. By forging partnerships with complementary stakeholders, organizations can leverage each other's strengths to develop integrated solutions that seamlessly different part of the IoT ecosystem. Partnerships include:

²⁹ <https://www.mckinsey.com/industries/retail/our-insights/moving-past-friend-or-foe-how-to-win-with-digital-marketplaces>

³⁰ <https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/>

³¹ <https://www.wallstreetprep.com/knowledge/network-effects/>

- **IoT Private Public Partnerships (“PPPs”)** including government, industry stakeholders and tech hubs, enable to spread investment for end-to-end solutions among multiple stakeholders provide and share intelligence. PPPs accelerate the creation of data ecosystems³², which are vital for growth of digital businesses generating high margin recurring revenue streams. Ecosystems can share information about data, availability, and analysis to develop new business models, and an architecture³³ for services that improve customer experience, lift adoption barriers and drive economies of scale.
- **Partnerships for End-to-End IoT solutions.** Private Public Partnerships including broadline suppliers, innovative startups, and application domain experts can be a catalyst to growth. Orchestration requires re-thinking the roles of ecosystem participants³⁴, which must be clearly defined to support a collective mix can bridge the gaps between legacy infrastructure and IoT markets to accelerate IoT adoption.

Orchestrated partnerships organize and convene the proper initial mix of partners to catalyze the platform-based industry ecosystem and accelerate the IoT economy. Orchestrated partners are key because:

- They minimize market failures (e.g., fragmented supply chain) or organizational failures (e.g. silos) and with proper governance they can mitigate stakeholder self-interest driven actions that undermine the overall value structure³⁵.
- They accelerate network effects that are key to the growth of business ecosystems. A platform-based digital marketplace connects buyers and sellers. As more customers and a wider range of equipment join, the value of the platform grows with more stakeholders and applications.
- They facilitate the innovation and validation of IoT proof of concept pilot offerings by bringing the right mix of partners collaborating to show the economic value before investing to deploy at scale.

Broadline suppliers bring platform orchestration capabilities, startups push the boundaries of IoT with innovation, and domain experts provide real-world relevance optimizing for practical use. Innovative startups and SMBs, especially the ones that are domain experts in specific market applications and application environments, must be incentivized to use Hyperscalers’ platforms in was that help them attract skilled personnel, innovate, and grow business ecosystems.

Tech hubs³⁶ facilitate regional partnership orchestration for scalable solutions that drive economic growth. Innovation hubs bring together diverse stakeholders such as R&D institutions, venture capital, incubators, startups, and businesses, fostering

³² <https://www.bcg.com/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition>

³³ <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/data-ecosystems-made-simple>

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

³⁵ <https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3DiHub>

³⁶ <https://www.eda.gov/funding/programs/regional-technology-and-innovation-hubs>

innovation, attracting talent, and creating economic value. Tech hubs can lead innovation ecosystem orchestration, emphasizing priorities such as talent attraction, capital investment, strengths identification, and comprehensive support.

Below are two business use case examples that can be accelerated with orchestrated PPPs consisting of an appropriate 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.

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



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

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

risks. A 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 and improved supply chain reliability.

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

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



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

For collaboration, large companies like Shneider, ABB, Siemens, PTC and GE offer industrial IoT platforms, while innovative startups like QualitySense provide specialized solutions for quality control and process optimization. Chip suppliers like Nvidia contribute AI and IoT hardware, while domain experts in manufacturing processes collaborate on real-time data analytics

and automation. A digital twin can help analyze and simulate quality control processes and predict operating costs and benefits. The economic value proposition for all stakeholders, centers on increased efficiency, reduced downtime, improved product quality, and cost savings, benefiting both large and small enterprises that jointly offer unique solutions.

IoT Economy Potential to GDP

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

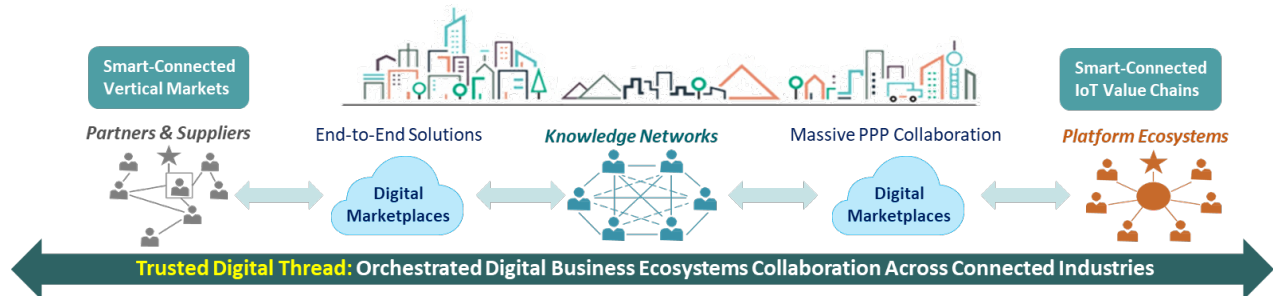


Figure 16. Caption to be updated

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

The journey from IoT partnerships to knowledge networks, to digital ecosystems.

Digital ecosystems are not limited to the exchange of goods and services. They encompass a broader spectrum, starting with partnerships where entities collaborate to achieve shared goals. Over time, IoT partnerships 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 IQ across value chains to drive new XaaS revenue streams and amplified growth from network effects.

Strategy for giants to empower SMBs to scale with massive collaboration.

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

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

Leveraging circular value chain ecosystems for sustainability. Platform-based business ecosystems in circular value chains play a pivotal role in driving sustainability and accelerating the convergence of physical and digital worlds with digital twins. Digital twins being replicas of physical systems integrated into circular ecosystems, will contribute to collective ecosystem IQ amplified by network effects evolving new layers of digital twins. The convergence of physical and digital words, fueled by digital twins within circular business ecosystems, will foster efficiency, innovation, and environmentally responsible practices that will take economies to the next level.

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



Findings of the IoT Advisory Board

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

General Findings – Specific Considerations

Finding 1: Industry adoption is slower and lower than expected and hindered by a variety of challenges.

The adoption of IoT, in the United States and globally, has been slower and at lower rates, than expected. In 2014, the World Economic Forum and McKinsey & Co. predicted that IoT and adjacent technologies (e.g., analytics, cloud computing, big data, and ML/AL) will produce \$9.6 to \$21.6 trillion of value for the global economy by 2022³⁷.

However, in 2021, McKinsey & Co. revised the forecast downward to between \$5.5 trillion and \$12.6 trillion by 2030.³⁸ 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. As a result, several major technology companies have moved away from IoT. Despite its potential, several challenges³⁹ and

³⁷ www.weforum.org/press/2014/01/increased-cyber-security-can-save-global-economy-trillions/

³⁸ www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

³⁹ [IoT Analytics - Challenges with IoT product launches: Why time-to-market has increased 80% in 4 years](#)

barriers have contributed to the slow pace of adoption across businesses and society. Some of these challenges include:

- **Complexity and Integration.** IoT consists of set of disparate technologies offered by a fragmented ecosystem of hardware suppliers, software platforms, and connectivity service providers. It is not a “one size fits all” 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 related to 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 markets are more sensitive to privacy issues (e.g. smart communities, retail, insurance, and healthcare) and other markets are more sensitive to confidentiality issues (Industrial IoT, smart cities, manufacturing, and financial services).
- **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%.

- **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.
- **Uncertain ROI and Business Value.** Some industries are more hesitant to adopt IoT technologies due to uncertainty about the return on investment (ROI) and the overall business value. This 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. 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” 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 2: A lack of coordination at the national level is hindering IoT adoption and operation across the economy and industry sectors.

Technological advancement brings both opportunities and risks, requiring a strategic approach to mitigate potential negative consequences. By carefully balancing the pace of innovation with risk mitigation measures, organizations can maximize the

benefits of technology adoption while minimizing potential risks. The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) will fundamentally enable our nation's most critical infrastructure sectors to become increasingly reliable, resilient, sustainable, and scalable.

However, to balance the promise of transformational capabilities with the risk of cyber-physical security threats, it is imperative that the Federal Government institute an overarching entity within the Executive Office of the President responsible for IoT and IIoT adoption. The Office of Science and Technology could fill this role.

The recent Office of Management and Budget Memorandum (OMB) 24-10 underscored that "federal agencies must clearly understand the devices connected within their information systems to gauge cybersecurity risk to their missions and operations." Moreover, the memorandum goes on to say, "maturing Federal cybersecurity practices for IoT devices are critical in today's increasingly automated world."

Examples of IoT and IIoT adoption barriers include:

- **Technical Challenges** including infrastructure limitations and compatibility issues. IoT is, by definition, connected, so interoperability issues limit usefulness. Additionally, technical challenges securing data and protecting individual privacy represent barriers to adoption. As IoT implementation grows, the ability to quickly and effectively scale operations are technical challenges. Lastly, IoT has particular challenges in that many devices have limited battery life and/or connectivity capabilities.
- **Regulatory Framework:** The regulatory framework for IoT faces significant challenges due to the lack of clear regulations and standards, making compliance complex and daunting. Companies must navigate intricate data privacy laws and cybersecurity regulations, often with limited understanding of the potential risks and benefits involved. This complexity can hinder the adoption and effective implementation of IoT technologies.
- **Business Model Challenges:** Monetizing IoT data remains a significant challenge for businesses, compounded by the high initial investment costs required to deploy IoT solutions. Integrating these new technologies with existing business processes and workflows is another hurdle, often exacerbated by a lack of understanding of the value proposition IoT offers.
- **Infrastructure and Connectivity:** IoT deployment is hindered by limited connectivity infrastructure, especially in rural and underserved areas, and the high costs of connectivity and data plans. Additionally, the infrastructure is vulnerable to outages and security threats, which can disrupt IoT operations and compromise data integrity.
- **Security and Privacy Concerns:** IoT technology is plagued by security vulnerabilities and data breaches, raising significant privacy concerns related

to data collection and use. There are also broader societal concerns about the potential for job displacement as IoT technologies automate various tasks.

- **Organizational Challenges:** Organizations often struggle with a lack of awareness and understanding of IoT technology, facing resistance to change and adaptation within the organization. Limited IT resources and expertise further complicate the implementation of IoT solutions, along with a lack of clear governance and accountability structures.
- **Social and Cultural Factors:** Public skepticism and privacy concerns pose significant barriers to the adoption of IoT technologies. Cultural and societal resistance to technological change, coupled with a lack of understanding of the potential benefits, can slow down or halt IoT initiatives.
- **Economic Factors:** The high initial investment costs and ongoing maintenance and operational expenses associated with IoT technology are major economic barriers. Additionally, there is uncertainty about the return on investment (ROI), which can deter businesses from committing to large-scale IoT deployments.
- **Lack of Collaboration:** Effective IoT implementation is often stymied by limited collaboration between stakeholders and difficulties in coordinating efforts across different organizations. The lack of open-source software and hardware also hampers innovation and the widespread adoption of IoT technologies.
- **Ethical Considerations:** The use of IoT technology in sensitive industries raises ethical concerns, including the potential for job displacement and broader societal disruption. The implications of data collection and surveillance by IoT devices also pose significant ethical dilemmas that need to be addressed.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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.

While IoT offers the potential for disruptive transformation and value, there are instances where policies and regulations at various levels of government hamper the benefits it provides. Competing and even contradictory regulation at state/local level

vs federal may add increased complexity to IoT adoption. Policies and regulations are generally well-intentioned and crafted to protect users and the community from harm, or to comply with standards and norms. Conflicts arise because the development and use of technology moves and changes rapidly and is often used in ways that have never been well studied. Well intended policies may conflict with one another, resulting in barriers to adoption, use, compliance and commerce of IoT. Government policies and regulations play a critical role in advancing or stifling the use, the beneficial outcomes and the scaling and evolution of IoT.

Examples of policies affecting the use of IoT include:

- Facial recognition algorithms running on a city's network of video cameras help deter and solve crimes but may lead to privacy violations when it is used outside of its intended purpose or provide inaccurate results. Many cities have enacted laws restricting the use of video cameras and facial in smart 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 4: There is an insufficient number of people in the current workforce with the technical, digital and analytic skills required to develop, integrate and deploy, operate and maintain IoT devices and IoT-enabled systems and applications.

A significant challenge in scaling IoT into the national infrastructure and economy is the development of 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 a workforce with interdisciplinary knowledge who can understand the complexities of both hardware and software components. Integrating these diverse skill sets within a single workforce is a considerable challenge.

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

- **IoT requires different skills.** Despite its connected nature, IoT is not IT. IoT is a disparate set of technologies requiring an interdisciplinary combination of existing and new technical, digital and analytical skills. The workforce must develop expertise in working with new connectivity technologies, such as LoRaWAN and 4G/5G, integration of IoT devices into internal and external networks, and the cloud. In addition, the workforce must develop skills in working with the cloud, and application development. Finally, the amount of data collected required data professionals to manage the data and analyze it to create optimal outcomes.
- **Non-digital industries and systems go digital.** Many 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 of IT, OT and IoT systems.** Industries such as manufacturing, energy and transportation employ operations technologies (OT), including supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLC), to monitor and control physical processes. On the other hand, business operations are supported by Information Technologies (IT) systems that process data and communications. In these industries, IT and OT systems operate independently of each other and are maintained by separate organizations. The incorporation of IoT into industrial processes 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.
- **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.

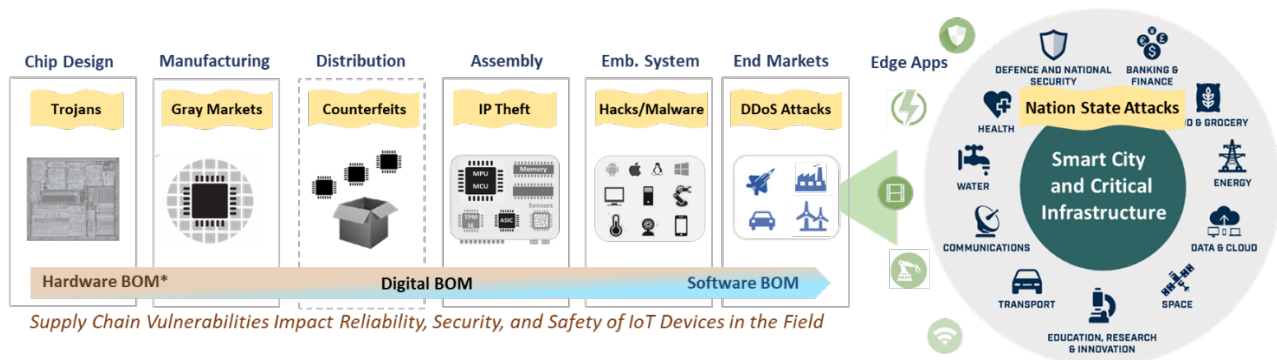
- Harnessing the full potential of IoT and AI.** Just as Excel transformed bookkeepers into accountants by automating calculations, IoT and AI will transform industries, necessitating new skills. Along with the skills described above, Co-pilots, AI-powered tools designed to assist humans, can significantly aid this transition. They enable workers to automate routine tasks, analyze complex data, and make informed decisions at a higher-level. By embracing and integrating these co-pilots, the workforce can not only adapt to but thrive in the rapidly evolving landscape of IoT and AI, driving innovation and efficiency.

TomKat – Propose to lead with Finding #9 (IoT modules) and then #5 (chips inside)

Finding 5: Legacy chips from China targeting our critical infrastructure and weaponization of AI chips require coordination of U.S.-EU CHIPS Acts.

Chip supply chains are vulnerable.

Supply chain traceability is even more critical for chips due to their foundational role in IoT devices, Geopolitical tensions and global supply chain vulnerabilities highlight the need for visibility and traceability of goods across industries. Supply chain traceability is even more critical for chips due to their foundational role in IoT devices, systems, and critical infrastructure. Multi-nation collaboration on chip supply traceability is essential since complex supply chains involve multiple countries and regions across the globe.



- Increasing IoT Supply Chain Security Risks.** Supply chain security and trust pose major concerns due to fragmentation and vast attack surface from chip design to IoT edge applications. Attacks experienced during field use of IoT devices such as DDoS attacks⁴⁰ can be traced back to supply chain vulnerabilities due to bugs or intrusions in chips and electronics. The risks to national and economic security are growing.
- Security and Economic Risks Related to Chips Trade.** Trade restrictions on chips are ineffective. Despite bans, western chips⁴¹ end up in Russian⁴² and

⁴⁰ Cybersecurity News - [Why DDoS Attacks Use IoT Devices as Weapons?](#)

⁴¹ Reuters - [Chip challenge keeping western semiconductors out of Russian Weapons](#)

⁴² Bloomberg - [Chips from Texas Instruments and other US makers flow into Russia despite bans](#)

Chinese drones⁴³ 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 bans⁴⁴. Imports of Chinese legacy chips on track to flood U.S. and EU markets which prompted the Select Committee on the CCP to urge Secretary Gina Raimondo and U.S. Trade Representative Katherine Tai to act⁴⁵.

- **Investments in CHIPS Acts can be at Risk Without Allied Coordination.** In December 2022, the U.S.-EU Technology Trade Council (TTC) officials agreed to strengthen chip supply chains⁴⁶ by coordinating semiconductor subsidies. Since then, allied nations committed \$450 billion in government funds to build fabs worldwide surpassing China's \$150 billion investment⁴⁷. However, China will produce much higher volume of chips at lower prices compared to allied nations and will continue to flood allied nations' markets. This puts at risk the \$450 billion CHIPS investment, that which exceed \$1.5 trillion with PPPs.

Limited Allied Nation Initiatives on Cross-border Traceability need to be expanded.

- **Lagging U.S.-EU Transatlantic Cooperation Agenda:** In early 2024, the U.S.-EU Trade Technology Council convened to discuss transatlantic cooperation⁴⁸ on trade and technology, covering export controls, AI governance, secure 5G connectivity, and semiconductor strategies related to U.S.-EU CHIPS Acts. Later discussions as part of the Transatlantic Economic Security Agenda covered digitizing supply chains⁴⁹ and chip traceability⁵⁰ to establish market preference for chips produced by the U.S. and allied nations. However, legacy chips imports used in our critical infrastructure and advanced chips leakage⁵¹ being weaponized in by adversaries⁵² are still ongoing.

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



- **Urgency for cross-border chip traceability solutions.** A study by KSE Institute⁵³ 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-

⁴³ Politico - [A \\$2M missile vs. a \\$2,000 drone: Pentagon worried over cost of Houthi attacks](#)

⁴⁴ Reuters - [China's military and government acquire Nvidia chips despite US ban](#)

⁴⁵ The Select Committee on the CCP - [Letter to Secretary Raimondo on Foundational Semiconductors](#)

⁴⁶ WSJ - [U.S., EU Agree to Coordinate Semiconductor Subsidy Programs](#)

⁴⁷ Sources: DARPA, EY.com GlobalFoundries, various business journals (estimated)

⁴⁸ CSIS.org - [The Fifth Ministerial of the U.S.-EU Trade and Technology Council](#)

⁴⁹ Atlantic Council - [Gina Raimondo and Margrethe Vestager on future of US-EU economic ties](#)

⁵⁰ CSIS.org - [The Transatlantic Economic Security Agenda \(Promote, Protect, and Partner\)](#)

⁵¹ The Economist - [Why America's controls on sales of AI tech to China are so leaky.](#)

⁵² Asia Financial - [China provides 90% of chips used in Russia despite bans.](#)

⁵³ KSE Institute - [Challenges in export control enforcement](#)

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

Opportunity IoT to mitigate vulnerabilities and drive economic growth

- **Leveraging IoT to mitigate supply chain risks and enable growth.** Enforcing export controls on chips is challenging as they can be programmed remotely. Intel's [pay-as-you-go chip licensing](#) and Samsung's [chip rental service](#) based on a Root of Trust signify the start of the "*Internet of Chips*" era. A trusted traceability infrastructure linked to customs controls that incentivize chip suppliers to securely trace, monitor and update chips can be more effective. It can unlock opportunities for trusted IoT services, digital marketplaces, and ecosystems to strengthen economic security.
- **Leveraging CHIPS Acts investments for collaboration on traceability.** With 80% of global fab capacity controlled by allies, the U.S. and EU are well-positioned to pursue proven ecosystem strategies⁵⁴ and pilot programs for global supply chain traceability like the National Defense Authorization Act (NDAA) applicable to US government purchases⁵⁵. These include, establishing provenance during chip design and manufacturing [KR3.4]; instituting global chip identifiers linking to local identifiers and chip fingerprints [ER2.4.2]; using IoT technology and identifiers to track chips; creating digital twins starting from manufacturing⁵⁶ [ER2.4.3]; managing chip supply chains by using AI to improve efficiency⁵⁷ [KR2.4]; using IoT platforms with sensors deployed in manufacturing produce data used for AI and analytics across supply chains⁵⁸ [ER2.4]; and creating digital threads⁵⁹ of data that enable XaaS⁶⁰ to create value [ER2.4.1] (see figure XX below).

⁵⁴ GSA TIES – [Cybersecurity strategy to create a Digital Supply Chain Business Ecosystem](#)

⁵⁵ NDAA Sec. 5949 - [Microelectronics traceability and diversification initiative](#)

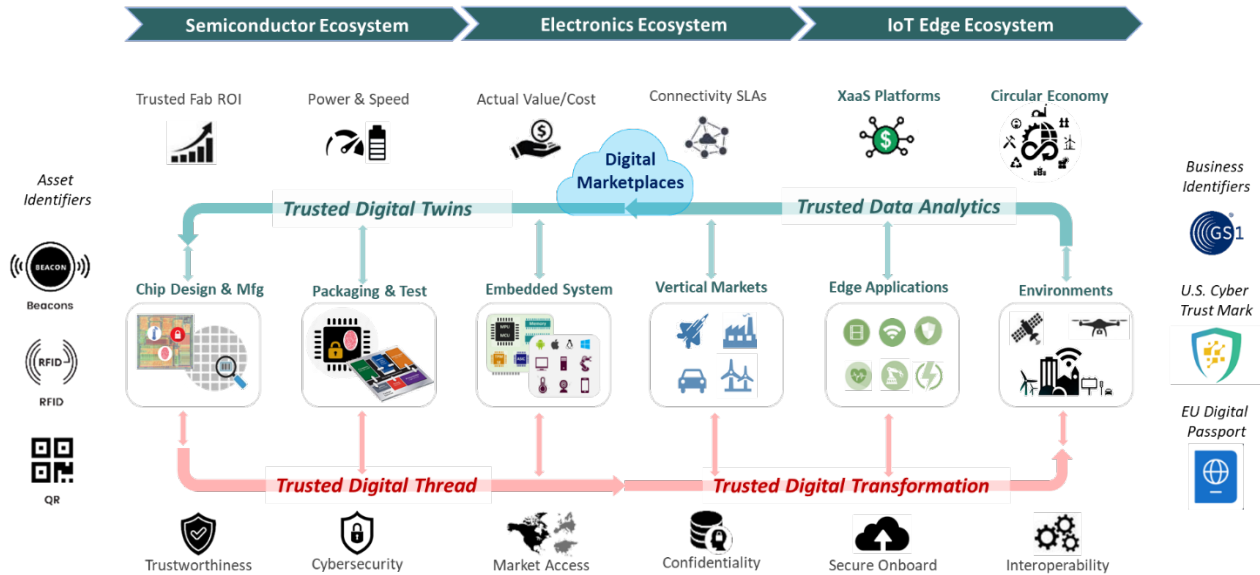
⁵⁶ Executive Gov - [NIST's CHIPS R&D Office Intends to Create Digital Twin Manufacturing USA Institute](#)

⁵⁷ CNBC - [How using analytics and AI can help companies manage the semiconductor supply chain](#)

⁵⁸ McKinsey & Company - [Reimagining fabs: Advanced analytics in semiconductor manufacturing](#)

⁵⁹ NIST - [Circular Economy Product Design and Digital Thread](#)

⁶⁰ Rochak Sethi, Deloitte - [How Semiconductor Companies can leverage XaaS to drive value creation](#)



A holistic strategy for a coordinated response is needed.

The U.S. and EU can leverage CHIPS investments to create a traceability infrastructure linked to a Root of Trust embedded in chips during manufacturing. The investment is small, compared to the volume of chips produced by fabs over their lifecycle. Lack of action could result in dire consequences if adversaries control the Root of Trust.

Initiatives for coordinating CHIPS Acts investments with the U.S.-EU TTC, the Executive Branch should include: (a) utilizing NIST’s global reach with Standards Development Organizations (SDOs) to create taxonomy of standards [ER2.1.3], (b) orchestrating PPPs in the chip ecosystem from design and manufacturing [KR6.2], (c) Investing in pilot projects to prove the value of traceability [ER6.2.1] and (d) promoting cross-border Digital Trust with programs like the U.S. Cyber Trust Mark⁶¹, the EU Digital Product Passport ⁶²and CBP Global Business Identifiers⁶³ with an goal to achieve a global ‘digital paper trail’ of chips [ER2.4.1].

⁶¹ whitehouse.gov - [Biden-Harris Administration Announces Cybersecurity Labeling Program](#)
⁶² World Business Council for Sustainable Development - [The EU Digital Product Passport](#)
⁶³ cbp.gov - [CBP Launches Global Business Identifier Pilot to Increase Supply Chain Visibility](#)

Finding 6. Establishing Trust in IoT requires a multi-dimensional and 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 breaches, and reliability.

Trust in IoT extends beyond cybersecurity and privacy. The World Economic Forum, in collaboration with technology companies, government, and consumer advocates, have created a holistic framework for digital trust (Figure xx).⁶⁴ The framework considers a variety of dimensions, including cybersecurity, confidentiality, privacy, safety, transparency, and fairness.

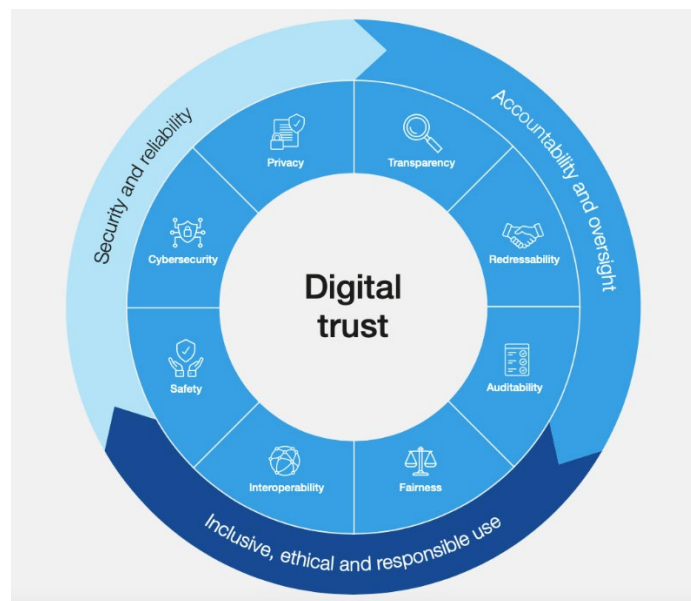


Figure xx.

Similarly, trust in IoT is multi-dimensional. Loss of trust in IoT is manifested in many forms. It may occur when the IoT device is insecure and allows cybercriminals to access the device and the network it is connected to. This may be due to a design that is insecure, insecure components from a compromised supply chain, or from insecure network connection. Similarly, loss of trust may result if the IoT devices produce incorrect responses or insights due to the poor accuracy of the data collected or compromised data (“poisoned data”) from a deliberate attack.

This creates adverse impacts to business and operational systems, as well as digital twin systems, that rely on the IoT data. Finally, trusted business ecosystems and partnerships are vital to creating trusted solutions and outcomes. Partners that deliver poor quality or security hardware and software, or those that are unreliable and lack

⁶⁴ <https://initiatives.weforum.org/digital-trust/about>

the necessary capabilities, compromise the integration, delivery and operation of IoT systems and solutions. This results in solutions and outcomes that don't meet requirements, lack consistency and performance, and have limited utility.

Actions and initiatives that address trust in IoT today focus mostly on cybersecurity and privacy. However, a more holistic perspective is needed to consider technology, data, operations and ecosystems.

Technology

- **Trusted IoT Devices:** Trust in IoT starts with awareness about trustworthiness of IoT devices. Device makers prioritize security, data protection, standards, and conformity assessment programs across the IoT ecosystem. An example for consumer IoT devices is the U.S. Cyber Trust Mark Program. Recognition of the trust mark enhances consumer confidence and conveys that consumer IoT devices are secure and trusted.
- **Trusted IoT Networks⁶⁶:** Securing Telco infrastructure and wireless networks, reinforced by encryption, authentication, and monitoring, are vital for trusting connected IoT devices and applications. Trust in network integrity is key to preventing breaches, ensuring smooth operations, and driving IoT adoption.
- **Trusted cloud platforms:** These are essential for IoT deployments, offering security, scalability, reliability, data analytics, interoperability, and cost efficiency. By leveraging trusted cloud platforms, organizations can accelerate their IoT initiatives, unlock new business opportunities, and drive innovation.

Data and analytics

- **Trusted IoT Data for Privacy⁶⁷:** Emphasizing the protection of personal user data and privacy rights is key for trusting IoT. It involves compliance with stringent data privacy regulations like GDPR and CCPA⁶⁸ and transparent data handling practices. Users have the right to control their data and its usage.
- **Trusted Data for Confidentiality:** Safeguarding enterprise data for IoT is critical to operations and competitiveness, including securing data transport, storage, access for devices and edge applications, etc. Confidentiality measures include encryption, access controls, secure communication, and identity management.

⁶⁶ <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value>

⁶⁷ <https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/securing-the-future/consumer-privacy.html>

⁶⁸ Deloitte - [A quick reference guide for CCPA compliance. Comparing CCPA compliance and the GDPR](#)

- **Trusted IoT Digital Twins⁶⁹:** Digital twins serve as virtual replicas of physical objects, used in simulations, predictive maintenance, and more. Trust in the data used in digital twins is key for reliability and integrity. Users rely on real IoT data to model real-world objects, ensuring their effectiveness in applications.
- **Trusted Analytics and AI:** Analytics and AI drive insights and decision-making in IoT applications. Trust in the data used for analytics and training models that drive AI algorithms and the algorithms themselves is paramount. Users need assurance that AI systems provide accurate, unbiased, and ethical insights.

Operations

- **Trusted IoT Supply Chains⁷⁰:** Ensuring the integrity of the supply chain is essential. Adopting traceability best practices, from component sourcing to device assembly can minimize the risk of tampering or vulnerabilities. Digitalization, Blockchain and distributed ledgers are key enablers trusted supply chains.
- **Trusted IoT Digital Transformation⁷¹:** Digital trust in operations and business is a key enabler for IoT adoption. The role of trust in data privacy, cybersecurity, and ethical AI, emphasizing that trust-building is essential for successful digital transformations among users, teams and organizations.
- **Trusted Digital Threads:** Digital Thread refers to a continuous flow of data throughout a lifecycle of a product. Digital threads are the backbone of IoT ecosystems, enabling traceability and transparency in data flows. Trust in digital thread provenance⁷² is crucial to ensure data integrity, accuracy, and reliability across value chains supporting trusted IoT applications.

Ecosystems

- **Trusted IoT Digital Marketplaces:** A digital marketplace is an online platform or ecosystem where buyers and sellers can engage in transactions for goods or services electronically. Trustworthy marketplaces offer transparent product information, user reviews, and metadata links to proprietary data for secure transactions. Users need to trust that the products and services they find in digital marketplaces are of high quality and safe to use.

⁶⁹ <https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/digital-twins-the-key-to-smart-product-development>

⁷⁰ <https://hbr.org/2020/05/building-a-transparent-supply-chain>

⁷¹ <https://www2.deloitte.com/xe/en/insights/topics/digital-transformation/digital-trust-for-future.html>

⁷² <https://www.semi.org/en/blogs/technology-trends/Enabling-End-End-Digital-Thread>

- **Trusted IoT Business Ecosystems:** Trust in business ecosystems requires organizations to invest in platforms that foster trust⁷³ through collaboration, innovation and trust-based decision-making. Industry stakeholders, regulatory bodies, and end-users should prioritize methods for trusted ecosystem.
- **Trusted IoT Partnerships:** Building trust within IoT involves establishing trusted PPPs. Collaborative relationships among stakeholders prioritize data security, privacy, and adherence to ethical standards. Trustworthy partnerships contribute to the overall reliability of IoT solutions.

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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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 article titled "IoT Cybersecurity: How Trust Can Unlock Value"⁸³ 61 percent 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 hinders 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

⁷³ <https://www.bcg.com/publications/2021/building-trust-in-business-ecosystems>

⁸³ <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/cybersecurity-for-the-iot-how-trust-can-unlock-value>

practices, ultimately slowing down the growth and potential benefits of IoT innovations.

[insert graphic of 16 states with disparate privacy regs]

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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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 compute provide the technical infrastructure for IoT to scale, a trust 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 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 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 9: IoT modules built by Chinese companies are a significant part of the market.

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. In modules, the top 2 Chinese companies combined for an estimated 48% of the market and is projected to be in 75% of devices by 2025.

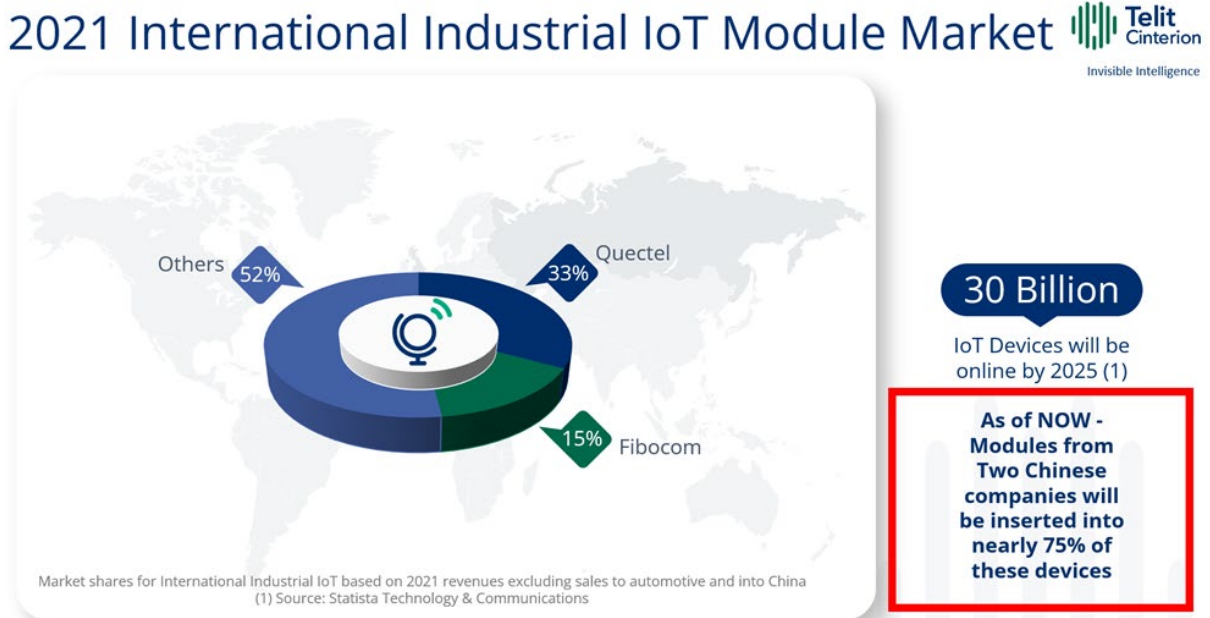


Figure 17 - Caption TBD

The majority market share by two companies raises cybersecurity and trade concerns. For example, analysts have raised concerns that IoT modules produced by companies in China pose potential cybersecurity risks.⁸⁴

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.

These concerns were highlighted in a letter⁸⁵ 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 FCC Chair Jessica Rosenworcel. The letter raised a series of questions regarding the FCC's 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; and
- 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 ICTS Integral to Connected Vehicles⁸⁶
- Lawmakers urge Biden administration to investigate Chinese LiDAR companies to determine whether they should be on government-restricted entities list.⁸⁷

⁸⁴ "China's cornered the IoT market. That could be a cybersecurity nightmare.", G. Noone, TechMonitor30, January 27, 2023. [Link](#).

⁸⁵ <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2023-08-07-cellular-iot-modules.pdf>

⁸⁶ "Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles." Press Release, U.S. Department of Commerce, February 29, 2024. [Link](#).

⁸⁷ "Lawmakers raise concerns over Chinese-made LiDAR tech." E. Graham, Netgov/FCW, November 29, 2023. [Link](#).

- 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.⁸⁸

While general competition is a healthy condition, 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.”⁹⁰

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 it.”

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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 10: Quantum computing poses a major threats to cybersecurity.

The encryption methods that protect our data and communications is based on mathematics. Quantum computers are well suited for solving mathematics problems. In a 2019 experiment, Google performed and completed a target computation in 200 seconds that would take the world’s fastest supercomputer 10,000 years to complete.⁹¹

Quantum computers have the potential to bypass the encryption locks that currently protect the world’s communications and data.”[3] 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

⁸⁸ As defined by section 8(c) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1607(c))

⁹⁰ “China’s overcapacity results from state interference in markets, say analysts.” L. Ya, Voice of America, April 5, 2024. [Link](#).

⁹¹ “Quantum Supremacy Using a Programmable Superconducting Processor,” J. Martinis, and S. Boixo. Google AI Quantum, October 23, 2019. [Link](#).

infrastructure, and defeat security protocols for most Internet- based financial transactions.”⁹²

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

- All 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.
- In addition, 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.
- Against IoT’s very 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 for the use of quantum computing to conduct cyberattacks is high (either for access to their data or to spoof/corrupt the data).
- Quantum computing poses major implications for the security-by-design of IoT devices with long lifecycles. It has the potential to break older cryptographic methods, rendering current security measures obsolete. This necessitates the integration of quantum-resistant algorithms in IoT devices from the outset to ensure long-term data protection, to avoid vulnerabilities and breaches.

However, much of 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.

⁹² “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. [Link](#).

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.⁹³ The response to post-quantum cybersecurity is in its early stages. For example, NIST is in the process of standardizing a set of post quantum cryptographic algorithms. Four algorithms are going through the standardization process (completion sometime in 2024) with three additional ones being considered for standardization.

However, the 2030s are not that far away, but there are no 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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 different brands may communicate and work together in a system. While interoperability is enabled by standards, it is challenging to achieve for a variety of reasons. In some areas, IoT technology is still new and rapidly evolving.

Many areas of IoT technology still need standardization, and reaching consensus on standards takes time. While open standards could enable seamless interoperability, the market is currently dominated by products with proprietary standards, "walled garden"⁹⁴ ecosystems and varying standards and protocols. Some vendors believe their proprietary standards are superior, others entered the market before standards emerged, and some fear commoditization. For IoT to progress, interoperability and standards across devices, industries and countries are critical (source: NIST IoT report draft). The lack of interoperability slows IoT functionality, adoption, scaling, value realization and delivery, and evolution in a number of ways including:

- Integrating devices and systems is challenging due to interoperability issues. Devices from different vendors often can't communicate because of incompatible protocols, and data may be in different formats. Even older and newer systems from the same vendor don't work together. These issues create "siloes" 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.

⁹³ "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret," E. Parker, RAND, September 13, 2023. [Link](#).

⁹⁴ 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.

- The inability to integrate IoT with existing legacy and modern systems hinders innovation and the full benefits of interconnected, automated systems. 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. 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.
- 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%.
- 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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

Connectivity service coverage is essential for IoT adoption and operation. The COVID-19 pandemic highlighted the digital divide and the need for connected communities. 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. The FCC is exploring the use of TV white space for rural IoT connectivity, and satellite operators are launching Low Earth Orbit (LEO) broadband services. Private enterprises are also establishing LTE and 5G private 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.** While urban areas have the infrastructure to offer different connectivity service options, rural areas and remote regions lack the same. This may be manifested in the lack of fiber infrastructure, as well as a lack of sufficient wireless infrastructure. Limited infrastructure, low population and population densities, terrain challenges and poor economic returns limit industry connectivity investments in these areas.
- **Future use cases require higher bandwidth symmetric services.** Future IoT use cases, such as drone and remote machinery operation applications in agriculture, require higher bandwidth symmetric connectivity services. The FCC's current 25/3 broadband service level definition is insufficient to support those applications.
- **Insufficient spectrum to support future needs of IoT at scale.** As the number of devices and IoT-enabled services continue to grow, additional 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 a large number of building structures, high wireless device density, are most susceptible to disruptions and issues.

The sunset 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.

Enabling “last acre” wireless service availability is also a major challenge. Not all areas can be covered due to geography and topographic constraints. For example, signal attenuation and interference from hills and tree foliage is a common challenge.[3] According to one technology solution provider, soil moisture sensors placed underneath leafy vegetables in a farm had experienced difficulties communicating with a nearby gateway.

Finally, many wireless operators face unfavorable economics, construction challenges and inability to secure suitable “right of ways.”[4] Privately owned wireless networks

are financially infeasible to all but the largest farms who have the capital and resources to operate this network.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 13: Artificial Intelligence (AI) is critical to unlocking and accelerating the value of IoT.

IoT and Artificial Intelligence (AI) are two distinct technologies that complement each other to create value. IoT devices collect data and report about its physical environment. 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. Digital twins, simulations of physical environments, use IoT and AI to model and predict system responses and impacts.

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 thought-focused tasks (clerical work, order taking, food service), freeing up human resources to focus on higher value, human-exclusive skills (creative thinking, problem solving, interpersonal skills, emotional intelligence, reasoning, negotiation, and decision-making).

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.

Artificial intelligence (AI) is a collection of technologies and approaches. 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 learnings to make predictions, classify data, recognize objects or images, and understand speech or text.

Generative AI (GenAI) offers new exciting 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 patterns to create content with 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 in September. GenAI can recommend specific signal timings by analyzing IoT data, road types, historical traffic patterns, and projected weather. This integration of GenAI with IoT technologies allows small communities to achieve results similar to those of larger cities with more resources.

Challenges

Despite the value offered by AI in IoT, a number of 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, 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 contain information on the farmer’s proprietary processes, which may inadvertently help their competitors, if not properly secured.
- **Data Management.** Proper data management is foundational to successful AI implementation, as highlighted by IoT Analytics⁹⁵. 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 data strategy, without which AI initiatives risk failure. Investing in 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 FTC from using facial recognition video systems for five years because

⁹⁵ <https://iot-analytics.com/how-global-ai-interest-is-boosting-data-management-market/>

its algorithms generated false positives, leading to false detentions and unfair treatment of some of its customers.⁹⁶

- **Explainability of outcomes.** AI algorithms for IoT may generate outcomes that are neither transparent nor explainable. For example, a IoMT device operating autonomously may create a recommendation that may lead to the death of 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.⁹⁷ Protestors have immobilized self-driving vehicles by placing traffic cones on its hood.⁹⁸
- **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 LLMs and AI algorithms.** These offer benefits such as increased accessibility, transparency, and the potential for collaborative innovation, enabling a wide range of applications and advancements. However, they also present 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

⁹⁶ <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>

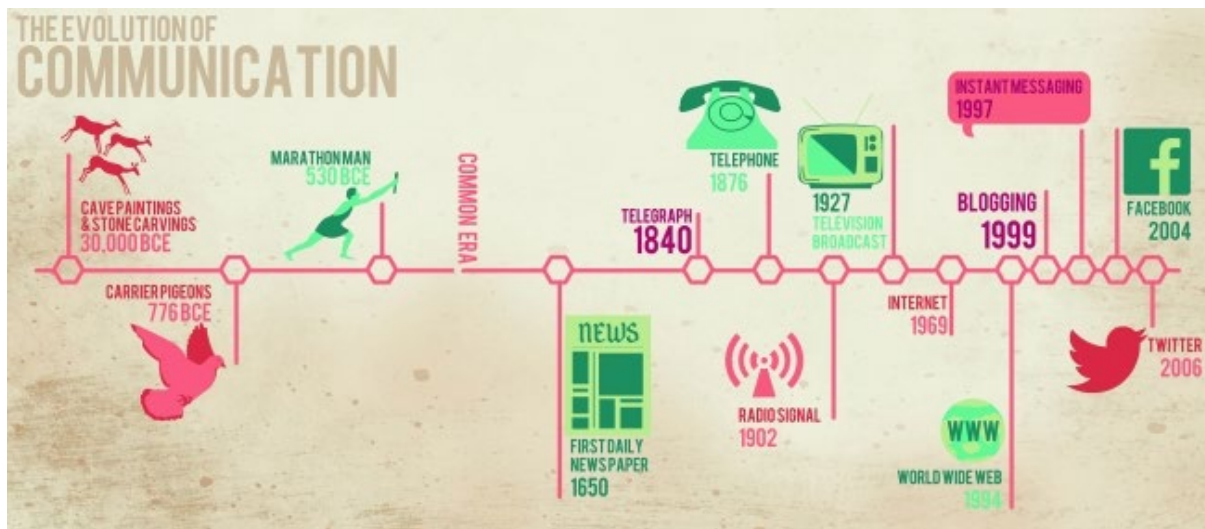
⁹⁷ https://globalnews.ca/news/3654164/alterred-stop-signs-fool-self-driving_cars/

⁹⁸ <https://www.npr.org/2023/08/26/1195695051/driverless-cars-san-francisco-waymo-cruise>

Finding 14: Barriers to IoT adoption due to legacy infrastructure require multi-stakeholder business ecosystem partnerships that align stakeholder incentives on end-to-end IoT solutions.

The potential of the IoT future economy driven by connectivity can be illustrated through the evolution of communication which has been a catalyst for market transformations. From carrier pigeons, to newspaper, to telegraph, to telephone, to radio, to television, communication was transformative driving major market shifts⁹⁹.

In today's digital age, the evolution of the IoT digital economy will be driven by the foundation of connectivity and IoT digital platforms that will drive interoperability, digital transformation collaboration and business ecosystems¹⁰⁰.



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

Foundational platforms accelerate evolution of ecosystems. History shows that innovative businesses can't evolve in a vacuum. They must attract resources of all sorts, drawing in capital, partners, suppliers, and customers to accelerate growth through cooperative networks and ecologies of competition¹⁰¹. Hardware and software value chains evolve from foundational platforms (e.g. *Intel Inside*) into partnerships and scalable business ecosystems.

Partnerships driven by connectivity gave rise to internet business platforms. Since the 90s disruptions, go market strategies, business platforms and revenue models

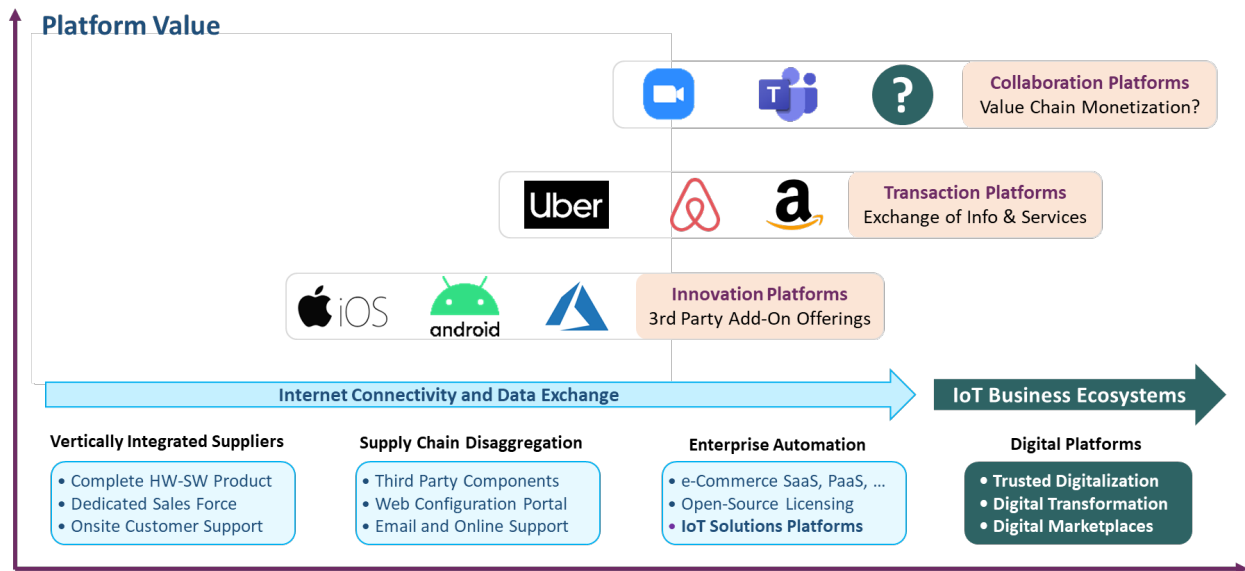
⁹⁹ <https://sci10sectionm.wordpress.com/2013/12/08/the-evolution-of-communication-effects-on-the-world-of-science/>

¹⁰⁰ <https://www.bcg.com/publications/2022/what-is-your-business-ecosystem-strategy>

¹⁰¹ <https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition>

advanced along with new generations of technologies on top of legacy infrastructure. In the new age of ecosystem partnerships¹⁰² value creation reflects a networked and dynamic collaboration and exchange among partners, which was accelerated with internet-based business platforms.

Platform-based business ecosystems created trillion-dollar valuations. Business scholars have advocated platform-based business ecosystems and their potential to fuel economic value driven by architecture, governance, and network effects¹⁰³. Architecture platforms like Apple iOS and Android enabled third parties to add apps to smart phones. Transaction Platforms like Airbnb and Uber enabled supply-demand matchmaking for the exchange of goods, or services. Hybrid Platforms¹⁰⁴ combined the advantages of both. Collaborative platforms like MS Teams and Zoom which grew during Covid-19, facilitated innovation, but not business ecosystem orchestration.



Multi-stakeholder collaborative business platforms failures lessons for strategy.

The IBM-Maersk TradeLens IoT blockchain platform was taken out of the market¹⁰⁵ because it was not open and failed to gain stakeholder support in the maritime supply chain. Collaborative platforms and ecosystems emerge as new organizational forms that provide distinct ways to cope with market failures (e.g. fragmented supply chain) or organizational failures (e.g. silos). Distributional and functional failures arise from self-interested actions by members, undermining the overall value structure¹⁰⁶. Recognizing these failures is crucial for designing effective collaborative platforms across the IoT value chain, to prevent or mitigate failures, and create value.

IoT creates opportunities for digital collaboration across business ecosystems. IoT provides the potential to transform linear supply chains and silos workflows to

¹⁰² <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ecosystem-partnering>

¹⁰³ <https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/>

¹⁰⁴ <https://sloanreview.mit.edu/article/the-future-of-platforms/>

¹⁰⁵ https://www.theregister.com/2022/11/30/ibm_and_maersk_tradelens_shutdown/

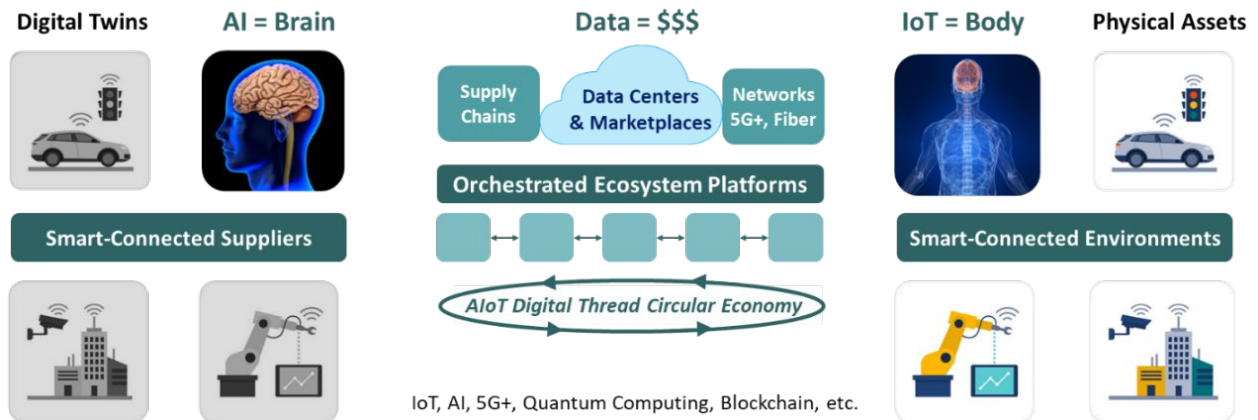
¹⁰⁶ <https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3DIthub>

dynamic value chains and connected organizations. Transformative IoT platforms enable scalable business ecosystems¹⁰⁷ where enterprises collaborate to provide coherent end-to-end solutions that benefit all stakeholders. Platform-based business ecosystems based on Group Orchestration, Governance Rules and Network Effects can fuel adoption of IoT and economic growth.

[Insert a paragraph describing how this finding relates to which recommendations.]

Finding 15: Convergence of AI, IoT and adjacent technologies used in supply chains will accelerate sustainability and drive growth fueled by massive data centers serving a hyperconnected planet.

The global economy operates linearly, extracting, producing, consuming, and disposing of materials, posing challenges due to finite resources. Transitioning to a circular economy, where resources are recovered and recycled, has been elusive but offers trillions in value. Barriers include low residual product value, material collection challenges, high processing costs, and supply chain traceability and monetization issues. AI and IoT platforms collapse these barriers¹⁰⁸.



IoT is the body and AI is the brain, supply chains & networks are the arteries where data flows. Digital AI + IoT (AIoT) platforms linking smart-connected suppliers with smart-connected environments powered by massive data centers will create digital marketplaces and sustainable ecosystems, which will surpass human intelligence. AIoT and data are intricately interconnected in a rapidly evolving landscape¹⁰⁹:

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

¹⁰⁷ <https://sloanreview.mit.edu/article/how-healthy-is-your-business-ecosystem/>

¹⁰⁸ <https://hbr.org/2023/06/how-ai-will-accelerate-the-circular-economy>

¹⁰⁹ <https://www.linkedin.com/pulse/transformative-power-data-ai-iot-shaping-worlds-future-jha/>

data for tasks such as predictive analytics, extracting valuable insights and patterns that may be too complex for manual analysis.

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

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

Data is the new raw material or the “new oil” for AI, which, in turn, can be applied to analyze and extract valuable insights from the data generated by IoT devices. This synergy between data, AI, and IoT coupled with quantum computing powered by massive data centers will drive advancements across various industries, 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.
- **Predictive Maintenance:** Use AI algorithms to analyze IoT data from industrial machinery and equipment to predict maintenance needs, reducing downtime and improving operational efficiency.
- **Healthcare Monitoring:** Combine IoT wearables with AI-powered analytics to monitor patients' health data in real-time, enabling early detection of health issues and timely medical interventions.
- **Supply Chain Optimization:** Employ IoT sensors to track goods in transit and use AI to predict potential disruptions, enhancing supply chain visibility and reducing inefficiencies.
- **Precision Agriculture:** Utilize IoT devices to gather data on soil moisture, weather conditions, and crop health. 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 occupancy patterns.
- **Connected Vehicles:** Use IoT sensors in vehicles to collect data on driving behavior and road conditions, then apply AI to improve road safety, traffic management, and vehicle diagnostics.
- **Environmental Monitoring:** Deploy IoT devices to collect environmental data (air quality, water levels, temperature, humidity, etc.), and employ AI to identify trends and potential hazards.

- **Smart Homes:** Integrate IoT devices like smart thermostats, cameras, and appliances with AI to create intelligent and automated home management systems that furnish data to utility companies contributing to energy savings.
- **Wearable Health Tech:** Combine IoT wearables with AI-driven analytics to provide personalized health recommendations based on continuous monitoring of vital signs and send a notice in the event of emergency.
- **Industrial Automation:** Use AI to analyze data from IoT sensors in manufacturing processes, to optimize production, quality control, and resource utilization.
- **Natural Disaster Management:** Combine IoT sensor networks with AI algorithms to predict and manage natural disasters, such as flood monitoring and early warnings.
- **Energy Grid Optimization:** Utilize IoT-enabled smart meters and AI algorithms to balance energy demand and supply, improving efficiency and reducing costs.
- **Waste Management:** Combine IoT sensors on waste bins with AI analytics to optimize waste collection routes and schedules, reducing fuel consumption and operational costs.
- **Smart Appliances:** Integrate AI and IoT to create appliances that can interact with users, optimize energy usage, and provide real-time feedback on performance.

Orchestrated platform ecosystems combining AI and IoT accelerate adoption and growth of digital economies. IoT produces data, AI consumes data, supply chains and networks transport data and data centers process applications to monetize data for a wide variety of use cases. Emerging trends in digital platforms include sustainability, connected manufacturing, creator economies, and new regulations¹¹⁰:

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 will support circular economies by enabling product and material exchanges, promoting reuse, repair, redesign, and recycling. Opportunities include material exchanges, reuse/resale marketplaces, sharing assets (e.g., cars, real estate), circular supplier networks, and sustainable logistics.

¹¹⁰ <https://mitsloan.mit.edu/ideas-made-to-matter/5-trends-mit-platform-report>

3. **Platform Regulations:** Platforms face new regulatory oversight that varies among geographic regions. For example, the US Section 230 offers legal immunity for content posted by third parties, while the EU Digital Services Act requires transparency and holds platforms liable for violating terms of service.
4. **Connected IoT + AI Manufacturing:** Manufacturing is adopting digital technologies with platform-based solutions leveraging data for smarter factory operations, optimized supply and demand forecasting, predictive analytics and better supply chain visibility leading to competitive advantage.
5. **Increasing Power of Influencers and the Creator Economy:** The Creator economy, estimated at \$100 billion. Influencers and creators face challenges like burnout and time management, with AI tools like ChatGPT offering assistance in saving time and managing workloads.

The circular nature of supply chains requires digital threads combining AI and IoT.

Trusted digital twins and AI need reliable data from trustworthy devices, which depend on secure hardware and software (HBOM and SBOM). Ensuring this trust involves reliable design and manufacturing of physical assets. The convergence of IoT and AI 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.

The explosive growth of AI and IoT requires monitoring and regulatory actions:

The examples above show just a fraction of the potential of combining AI and IoT platforms with supply chain data. ChatGPT quickly reached 100M users, surpassing Twitter and Facebook, and 2M developers are creating numerous APIs and apps. Since many developers and rogue actors connect remotely to AI platforms, monitoring and regulating these ecosystems is crucial to mitigate risks and drive growth.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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 greatly 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 greatly benefit these areas, especially for chronic health conditions. However, rural regions often lack the necessary connectivity infrastructure, workforce, and resources to support IoT operations. This lack of local expertise and trained personnel hinders 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 large 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, 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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 17: Small businesses can reap significant benefits from IoT, but significant barriers hinder 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.

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

- **Financial.** The initial cost associated with purchasing and implementing IoT solutions may be beyond the means of small businesses. These businesses have limited financial resources, and many have cash flow constraints, hindering their ability to invest in IoT, hire skilled resources or contracting with service providers.
- **Skills and Expertise.** Integrating IoT technologies into existing business processes can be complex. Small businesses lack personnel with the expertise to successfully deploy and manage 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.
- **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.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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 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 R&D. Investors are hesitant with emerging technologies, and customers rarely have budgets for pilot projects. Unlike larger companies, small firms can't afford to fund development projects or offer free pilots, leading many to fail in the "Valley of Death" 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 companies can offer discounts or free proof of concept to mitigate risks, but small businesses lack this ability.
- **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 new 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:** Innovative 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.

[Insert a paragraph of 2 describing how this finding relates to which recommendations.]

Industry findings – Specific Considerations

Finding 19: Precision Agriculture. 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, 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 suffers from a variety of challenges. The top barriers include:¹¹²

- **Connectivity:** Agricultural producers face three connectivity challenges: limited broadband in rural areas, inadequate 25/3 Mbps (download/upload) broadband for precision agriculture, and the need for wireless connectivity to the "last acre" on large 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 large amounts of data.
- **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.
- **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.
- **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 producers are more likely to adopt these technologies due to better education and economies of scale.

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

IoT and its adjacent technologies offer the potential to transform cities and communities to become more responsive, resilient and sustainable. For residents of these 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

¹¹² 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

navigate to the space directly, instead of driving around looking. In addition, it also helps identify parking space violations and direct parking enforcement officers to the spot directly without having to drive around.

- Community air quality networks are deployed in select areas of the community to monitor environmental conditions and inform residents and policymakers. Air quality networks may be deployed in areas with poor air quality, or where poor air quality would harm vulnerable populations 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 reasons. These include:

- **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, are very expensive. While larger cities may have the capabilities and some funding vehicles to support these projects, America’s small and medium size cities do have very limited capabilities. In some cases, federal, state and regional grants may be available, but securing these grants can be difficult.
- **Lack of skills and resources.** Many cities and communities lack the new innovation and digital skills and resources to plan, deploy, operate and support IoT applications. These resources are scarce in the market, and cities often cannot compete with the private sector for the same talent.
- **Privacy Concerns.** The extensive collection of data from IoT devices raises concerns about data security and privacy. Ensuring robust cybersecurity measures and transparent data handling practices is crucial to building and maintaining public trust.
- **Community and political resistance.** Candidates are not elected for building a smart community. Political leaders are re-elected if they are responsive to the needs of their constituents. Smart community initiatives that don’t align with

the city's strategic and near-term priorities are likely to face resistance from both citizens and policymakers.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Smart Infrastructure

Infrastructure is essential to the functioning and resilience of the United States. For example, a nationwide network of roads, waterways, rail and airports transports freight and goods to market, and connects people with places. A regional system of natural and man-made reservoirs, aqueducts, pipes, pumping stations, and treatment plants brings fresh water to cities and farms. Electricity generated from renewable and non-renewable energy power plants travels over through a network of transmission lines and substations to power cities and communities across the country. Sewage is routed from homes and buildings through a regional network of underground pipes to wastewater treatment plants for reclamation for reuse and release.

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

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

Despite the many capabilities and benefits offered by smart infrastructure, American infrastructure is old and failing. It must be repaired, replaced, and upgraded before it can be digitized and made "smart". The American Society of Civil Engineers (ASCE) have given American infrastructure an overall C- grade in its 2021 report card,¹ a slight

improvement from the previous report card (2017), which rated the state of American infrastructure as D+.² For example, the United States has over 2.2 million miles of underground pipes that deliver drinking water. There is a water main break every two minutes and an estimated 6 billion gallons of treated water are lost each day.³ Many of America's wastewater treatment plants were built in the 1970's and have an average life span of 40-50 years.⁴ This aging infrastructure and inadequate capacity leads to the discharge of 900 billion gallons of untreated sewage into U.S. waterways each year.⁵

Another concern is the vulnerability of smart infrastructure to cybersecurity threats, cybercriminals, and malicious state actors. IoT and other smart technologies create new attack surfaces and vulnerabilities to assets and infrastructure that had traditionally not been digitized or had been protected through "air-gaps". These cyberattacks may lead to disruption of operations and services, compromise of control and operational capabilities, and harm to millions of Americans who rely on this infrastructure. For example, the energy sector was the third and fourth most targeted sectors in 2020 and 2021 respectively.⁸ The utility industry averaged 736 cyberattacks per week and experienced a 46 per cent year-over-year increase in cyber-attacks in 2021.⁹ In 2019, a renewable energy generator company, the largest private owner of operating solar assets in the United States, was subjected to a denial-of-service attack. While no loss of energy generation was reported in the attack, the company lost visibility into about 500 MW of wind and PV generation in California, Utah and Wyoming.¹⁰ Similarly, U.S. water utilities are prime targets for cyberattacks. The March 2020 Cyberspace Solarium Commission report stated that the nation's 70,000 water utilities "remain largely ill-prepared to defend their networks from cyber-enabled disruption."¹¹ In 2021, an operator at a small water treatment plant in Oldsmar, Florida, thwarted an attempt by an intruder to boost the level of sodium hydroxide (lye) in the water supply to 100 times higher than normal.¹²

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 21: There's an opportunity for IoT to further transform transit systems and traffic management with real-time data analytics, intelligent traffic management, and predictive analytics to enhance efficiency, reduce congestion, increase safety, and improve overall transportation experiences.

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

roadmap includes leveraging technology to improve the safety of motor vehicles on our roadways.

Smart traffic technologies provide an organized, integrated approach to minimizing congestion and improving safety on streets through connected technology. These technologies smooth traffic flows and prioritize traffic in response to demand in real time. They enhance pedestrian, bicycle and vehicle safety and reduce accidents that cause injuries and fatalities. Connected vehicles can alert drivers of potential hazards such as pedestrians crossing the street or other cars in the vicinity. Using adaptive control, detected vehicle congestion triggers changes to traffic signal timing to optimize traffic throughput in near real-time. Traffic signal timing can be adjusted to maintain schedules of bus and rapid transit lines. A path through the city is coordinated for first responder vehicles, using congestion data and vehicle location to adapt route guidance and traffic signal timing allowing these vehicles to get to their destination sooner.

These technologies can facilitate and support multimodal transit and other innovative transportation models (including ride-share, e-scooters, drones, etc.). They also facilitate the safe testing and operation of 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 showcase the technology's ability to improve work zone and intersection safety.¹¹⁵
- 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.¹¹⁶
- A project with an auto maker and a bicycle safety platform maker to highlight the benefits of C-V2X-powered bicycle use cases.¹¹⁷
- A project with the Tampa Hillsborough Expressway Authority (THEA) to deploy and pilot Connected Vehicle (CV) applications to demonstrate safety and

¹¹⁵ Jacob Levin, "Virginia Tech Transportation Institute researchers to deploy smart work zone in Wise, Virginia," Virginia Tech Exponentially More (May 19, 2022), https://vtx.vt.edu/articles/2022/05/vtt-smart-work-zone.html?utm_source=cmpgn_news&utm_medium=email&utm_campaign=vtUnirelNewsDailyPublicCMP_052022-public; Audi, *Audi collaborates to deploy C-V2X communication technology on Virginia roadways* (Sept. 29, 2020), <https://media.audiusa.com/en-us/releases/437>.

¹¹⁶ Press Release, Audi, (Mar. 30, 2021), *Blue Bird, Fulton Co. Schools join Audi, Applied Information on connected vehicle deployment to boost school bus and school zone safety*, <https://media.audiusa.com/en-us/releases/465#>

¹¹⁷ Press Release, Audi, *Audi joins Spoke Safety, Qualcomm, Commsignia to help protect bicyclists through connected technology*, <https://media.audiusa.com/en-us/releases/514>.

mobility benefits of the technology with respect to pedestrians in and around downtown Tampa.¹¹⁸

- A project with the Florida Department of Transportation (FDOT) to test and implement connected vehicle and pedestrian/bicyclist safety applications (active or passive) at 13 signalized intersections and 8 mid-block crossings within the core of the University of Florida (UF) campus.¹¹⁹
- The New York City Department of Transportation Traffic Safety Network. a large-scale Intelligent Transportation System (ITS) upgrade, replacing their entire citywide traffic communications network with a cellular IoT system. DOT's traffic management system controls the traffic signals at 14,000 intersections, as well as a range of ITS devices including traffic cameras, variable message signs and vehicle detection devices. The new network is highly automated, secure, and achieves four 9's availability using dual concurrent cellular links.¹²⁰
- 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 phases¹²¹
- 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.¹²²

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

While there are several opportunities and benefits for 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

¹¹⁸ https://www.its.dot.gov/pilots/pilots_thea.htm

¹¹⁹ <https://teo.fdot.gov/architecture/architectures/d2/html/projects/projarch47.html>

¹²⁰ <https://www.digi.com/resources/customer-stories/new-york-city-dot-deploys-digi-solutions>

¹²¹ <https://www.digi.com/resources/customer-stories/trimet-bus-fleet-management-with-digi-connectivity>

¹²² <https://www.digi.com/resources/customer-stories/digi-helps-septa-comply-with-federal-mandate>

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 (See Carnegie Mellon Study for an example: <https://www.cmu.edu/piper/news/archives/2012/october/smart-signals.html>) as well as increased productivity (drivers spend less time stuck in traffic). Other 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 aspects of data jurisdictions can collect, retain, and subsequently use. Certain aspects of this sector still need high level policies and regulations that adequately address safety and liability concerns. The benefits of these technologies are not available in rural or underserved areas. Interoperability and fragmentation is also a challenge when dealing with different jurisdictions and it's important to address cybersecurity implications of all the connected devices that can be used as a gateways. Finally, there is a considerable amount of funding needed to drive adoption in this sector. The examples provided above reinforce that this technology is ready to go mainstream.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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.

IoMT devices fall into four categories:

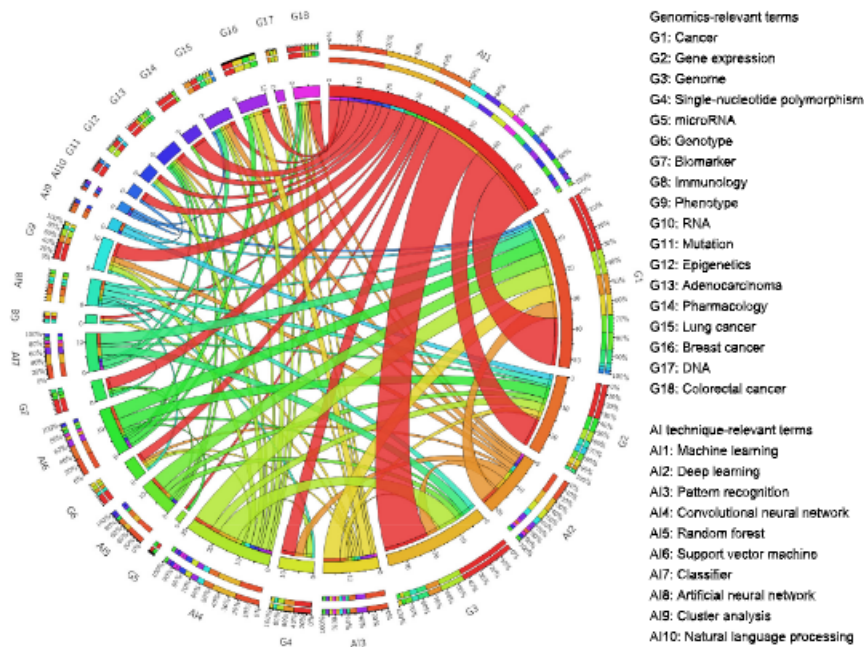
Create and add a graphic that represents these 4 categories depicted as the following:
Wearable on-body devices = fitness tracker on a silhouette of a body or arm

In-home devices = home with data/radio waves coming out of it

Community IoMT systems = Ambulance with data/radio waves coming out of it

In-clinic IoMT systems = hospital

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. Provided below is an example of a co-occurrence network of disease and genomic-relevant terms.



Source: see attached Elsevier paper

1. 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).
2. In-home devices that support telemedicine applications such as remote patient monitoring, and emergency response.
3. Community IoMT systems, such as emergency response intelligence systems that connect patients and first responders, mobility services, and devices for measurement and regulation of temperature, blood pressure, and others.
4. In-clinic IoMT systems that support administrative functions that allow medical workers to help patients remotely, track hospital assets and equipment, and others.

IoMT devices fall into four categories:

5. Wearable on-body devices, including consumer health devices (e.g., fitness watches, sleep trackers), and clinical-grade devices (regulated by health agencies, and prescribed by healthcare professionals).
6. In-home devices that support telemedicine applications such as remote patient monitoring, and emergency response.
7. 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.
8. In-clinic IoMT systems that support administrative functions that allow medical workers to help patients remotely, track hospital assets and equipment and others.

Some examples of top IoMT applications include:

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

IoMT enables the following benefits, including:

- **Enhanced Patient Outcomes.** By enabling continuous monitoring and personalized care, IoMT contributes to improved patient outcomes. Timely access to health data allows for early detection of potential issues, better management of chronic conditions, and more proactive interventions.
- **Efficiency and Cost Savings.** The implementation of IoT in healthcare streamlines workflows, reduces manual tasks, and enhances the efficiency of healthcare delivery. This not only improves the quality of care but also contributes to cost savings by minimizing unnecessary hospitalizations, optimizing resource utilization and minimizing administrative costs.
- **Patient Engagement and Empowerment.** IoMT empowers patients to actively participate in their healthcare journey. Access to real-time health data through wearable devices fosters a sense of ownership and encourages individuals to make informed decisions about their lifestyles and treatment plans.

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

- **Security and Privacy Concerns.** The vast amount of sensitive health data transmitted through IoT devices raises significant concerns about data security and patient privacy. Ensuring robust cybersecurity measures and compliance with privacy regulations is crucial. 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 Internet of Medical Things holds immense promise for the healthcare industry, facilitating a future where patient care is personalized, efficient, and technologically advanced. However, to realize this promise, the healthcare industry ecosystem must evolve and adapt its practices, operations, policies and regulations.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 23: Environmental Sustainability. IoT supports environmental sustainability through real-time monitoring, optimizing resource usage, and facilitating data-driven decision-making across infrastructure and multiple sectors of the economy.

IoT devices monitor environmental conditions, optimize usage of resources, and control operational processes. The data collected from IoT devices is analyzed and used to inform policymaking, enforce regulations and monitor progress and success of programs and initiatives. In other cases, IoT technologies initiate actions and control operational processes that support sustainability outcomes.

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

- **Monitor air quality.** Air quality sensors measure the concentration of pollutants in the air, including particulate matter (e.g., soot or black carbon), and gas pollutants (carbon monoxide, nitrogen dioxide, etc.). This information informs residents of a community whether to go outside exercise or not. The collected data may be used by city and health officials to identify areas of poor air quality, and to devise programs to mitigate its effects (such as planting trees in the area, restricting traffic at certain hours, banning idling cars at certain hours, providing residents with respiratory healthcare information, etc.).
- **Optimize water use.** Farming consumes a lot of water. Soil moisture sensors, integrated with automatic irrigation systems, measure moisture levels and activate the irrigation systems in those spots in the field where the water is needed. This helps save water (and the corresponding expenses) by precisely directing water to those spots where it is needed. IoT monitoring can detect leaks and other issues in water transport. Optimizing water usage by applying water where it is most needed, and reducing waste and conserving resources, are examples of how IoT supports sustainability.
- **Reduce carbon emissions.** By leveraging IoT technologies, emissions associated with upstream and downstream supply chains (scope 3 emissions) IoT can measure, collect, and compile data regarding manufacturing, transportation, agriculture production, and end-of-life practices for economic activity. Great transparency of scope 3 emission with enable the implementation of effective mitigation strategies and contribute to national and global efforts to reduce carbon dioxide (or equivalent) emissions.
- **Reduce energy use.** Buildings are one of the largest consumers of electricity. Room occupancy sensors turn off lights in empty rooms. Smart thermostats learn the behavior of building occupants and autonomously manage ambient temperatures based on those patterns. Automated demand response systems, connected to building automation and energy management systems, automatically reduce energy use by turning things off during peak demand periods while minimizing impact on building occupants.

- **Optimize use of renewable energy sources.** IoT optimizes and maximizes the use of renewable energy sources to power communities and cities. Smart inverters in solar power systems and sensors in batteries communicate with the local electrical grid to continuously manage how much electricity is stored, discharged to the grid, and used to power loads in the home and business. This maximizes the ability of renewable energy systems to meet demand in the local grid, while delaying the use of upstream fossil fuel power generation plants to meet local community demand.

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

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

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

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

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

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

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 are deployed in public spaces to monitor and detect unusual activities or potential threats in real-time. For example, connected audio sensors detect the sound of gunshots or breaking glass, identify the location and notify police so they can respond faster. Smart cameras detect and report suspicious and unpermitted behaviors, such as unattended luggage or packages, trespassing into secure areas, lack of social distancing, or fighting, display of a gun and other illegal activities. These smart applications enable and accurate monitoring and review 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 active disaster areas to provide responders with a fast assessment of the scene to inform on deployment of resources and activities. Water level sensors monitor upstream river and stream levels to provide communities with knowledge of real-time conditions and enhance flood response, evacuation, and mitigation activities. Sensors that detect Wi-Fi signals from mobile phones allow first responders to know how many people are inside a building and where they are at. Air quality sensors monitor the pollution levels of communities and inform public health officials of intervention programs to mitigate respiratory illnesses. The use of IoT for situation awareness facilitates where to focus initial resources to save human lives.

Responder Monitoring. Wearable IoT devices, such as body cameras, biometric monitors, and communication devices, enhance the capabilities and safety of first responders during operations. These IoT devices inform operations managers of responder stress levels, conditions of the surrounding environment and state of responder equipment. For example, sensors on oxygen tanks provide responders with a real-time estimate of the remaining time left and considers responder exertion and stress levels. Body cameras on police provide a record of how officers respond to activities, document actions,

hold officers accountable and provide a record of activities that is reviewed to improve future operations.

- **Connected patient monitoring.** Emergency response vehicles equipped with IoT devices monitor the health of the people being treated at accident or disaster scenes, as well as those critically injured transported by ambulances. This monitored patient information can be viewed in real time by Emergency Room doctors, who may instruct paramedics to apply additional measures to stabilize and treat patients before they reach the hospital. For the most critically injured, the additional information could mean the difference between life and death.

[the team will add findings related to the need to study whether communities would benefit from a list of vetted/proven and interoperable IoT for emergency use and the value/viability of a stockpile of such technology. Also include some of the challenges that hindered the Board from recommending those, including the rapid pace of technology evolution (concerns about the stockpile becoming quickly obsolete), logistical difficulties (how to get the needed technology to the appropriate site quickly), and funding challenges. Study could include looking for ways to keep the IoT stockpile current and refreshed.]

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

- **Improved Situational Awareness.** IoT devices provide real-time data, supplementing existing information. and enabling public safety agencies, first responders, disaster and resilience managers, and health officials to have a comprehensive and real time view of ongoing and developing situations. This improves decision-making and facilitates resource allocation during emergencies.
- **Increased Response Effectiveness.** Connected devices enable faster communication and response coordination. Emergency services can be dispatched more efficiently, reducing the time it takes to address critical situations.
- **Preventive and Predictive Capabilities.** IoT sensors enable the collection of data for predictive analytics. For example, information collected from gunshot detection sensors can be analyzed to predict when and where potential future incidents may occur. The police can anticipate potential risks and take preventive measures like stationing more officers at the predicted times and locations, to reduce the likelihood of incidents.
- **Data-Driven Decision-Making.** The data collected from IoT complements existing and historical information and knowledge to inform and enhance decision-making. For example, air quality monitors identify areas of a city where poor air quality consistently exists. Using this knowledge, along with the

correlation between increased death rates and air pollution,¹²³ public health officials can decide to target this area for information campaigns to prevent COVID-19 exposure, as well as to station medical resources for early intervention and treatment of COVID related illnesses.

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

- **Cybersecurity Concerns.** The use of connected devices leads to increased cybersecurity vulnerabilities and risks. Cybercriminals may use vulnerable devices to gain unauthorized entry into the systems used by law enforcement and other public agencies. This may result in access of sensitive information, and the operational compromise of public safety devices and systems.
- **Privacy Issues.** The extensive data collection capabilities of IoT devices raise privacy concerns. For example, traffic cameras may be used outside of its original and authorized scope to surveil private citizens. Cameras in public spaces may be equipped with facial recognition capabilities to identify people for detention. These concerns may lead to a lack of community support and ban of these technologies in the communities they serve. The use of IoT requires the development of policies and legislation that balance the benefits of data-driven public safety with individual privacy considerations.
- **Interoperability Challenges.** The IoT devices used to support public safety may face interoperability challenges in integrating and communicating with the various systems used by public safety agencies. This lack of interoperability makes it difficult for the various systems to share and process information in real time for operations, decision-making and situational awareness.
- **Scalability and Infrastructure.** Scaling IoT deployments to cover large geographic areas requires robust and modern infrastructure. This infrastructure must be scalable and interoperable to accommodate a growing number of future devices, and be reliable and critical for use under harsh conditions. It must cover remote areas, such as for wildfire detection or flood monitoring, where limited connectivity infrastructure currently exists.
- **Funding.** A lack of funding prevents public safety and public health agencies from procuring, deploying and operating IoT-enabled applications and systems. These systems may be costly, and limit agencies to what they can purchase. Traditional funding sources have been through a variety of agency funding vehicles, including grants, internal capital budgets, and capital improvement budgets. Other than grants, funding is based on agency priorities and availability, and can be subject to long procurement cycles.

¹²³ Air pollution linked with higher COVID-19 death rates, <https://www.hsph.harvard.edu/news/hsph-in-the-news/air-pollution-linked-with-higher-covid-19-death-rates/>

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 25: True end-to-end supply chain visibility is 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.

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.

This is attributed to a number of reasons, including (if you use it verbatim, please cite our Draft NIST report. I can provide the citation).

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. Data sharing across supply chains and firms is rare.

Intermediary Network: Between shippers and customers lies a network of logistics service providers, including carriers, warehouse operators, and terminal operators worldwide. Harmonizing their IT systems, standards, and knowledge levels requires significant organizational effort.

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.

Amazon's Efficient and Integrated Supply Chain Model. Amazon has achieved a highly efficient supply chain¹²⁶ due to its vertically integrated business model, which involves owning various aspects of its supply chain, including shipping and logistics. This allows Amazon to maintain end-to-end visibility and control over its operations, reducing dependencies on external partners and streamlining processes. Moreover, Amazon invests in technology and innovation, leveraging advanced data analytics and automation to optimize inventory management, fulfillment processes, and delivery operations.

FLOW Program Overview: The White House FLOW pilot program¹²⁷ aims to boost supply chain resilience by enhancing data transparency and collaboration among supply chain stakeholders. Created as part of a whole-of-government approach to address supply chain disruptions caused by the Covid-19 pandemic, FLOW began with a few participants and has now expanded to over 70, with 60 more being onboarded¹²⁸. 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.

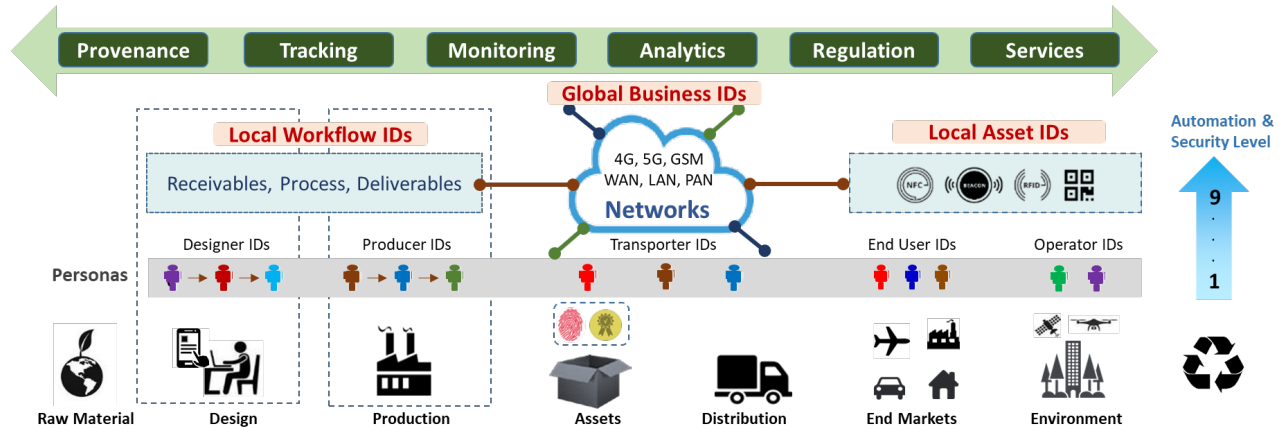
IoT and FLOW Integration Using Business IDs: The FLOW pilot addresses a specific challenge in the supply chain, including data sharing and collaboration. There is an opportunity for IoT to leverage this program's future data-sharing capability to provide cross-border end-to-end visibility by using Global 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. DHS Customs and Border Protection has initiated pilot programs on Global Business Identifiers¹²⁹ for a variety of physical goods including pharma, electronics and chips.

¹²⁶ <https://dfreight.org/blog/an-insight-into-amazon-supply-chain-strategy/>

¹²⁷ <https://www.bts.gov/flow>

¹²⁸ <https://www.cnbc.com/2024/03/20/biden-administration-is-expanding-its-real-time-supply-chain-tracker.html>

¹²⁹ <https://www.cbp.gov/newsroom/national-media-release/cbp-launches-global-business-identifier-pilot-increase-supply-chain>



REVISED GRAPHIC

Global Identifiers enable trusted traceability of businesses, products, and data across borders, facilitating market preference by monitoring imports of essential goods. By linking Global Identifiers to Local Identifiers, that 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 overtime this will foster trusted digital marketplaces and fuel digital economies.

[Insert a paragraph or 2 describing how this finding relates to which recommendations.]

Finding 26: IoT technologies in the industrial sector need to be properly and responsibly governed and applied.

Industrial operations are heavily monitored and controlled in a variety of industries, including energy, mining, chemicals, and transportation. These technologies are also prevalent in manufacturing, monitoring, process control and operations, and supply chain management. Many equipment manufacturers use Industrial Control Systems, (ICS) that are used to control processes like manufacturing, product handling, production, and distribution. ICS includes Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and programmable logic controllers that incorporate IoT technologies. These technologies are often also referred to Operational Technologies (OT). OT is comprised of hardware and software that detects or causes a physical change through the direct monitoring and/or control of industrial equipment.¹³² OT devices are as distinct from ‘consumer IoT’ due to their usage in commercial operations and are not available or readily available for sale to the public.

132 From: Wikipedia https://en.wikipedia.org/wiki/Operational_technology

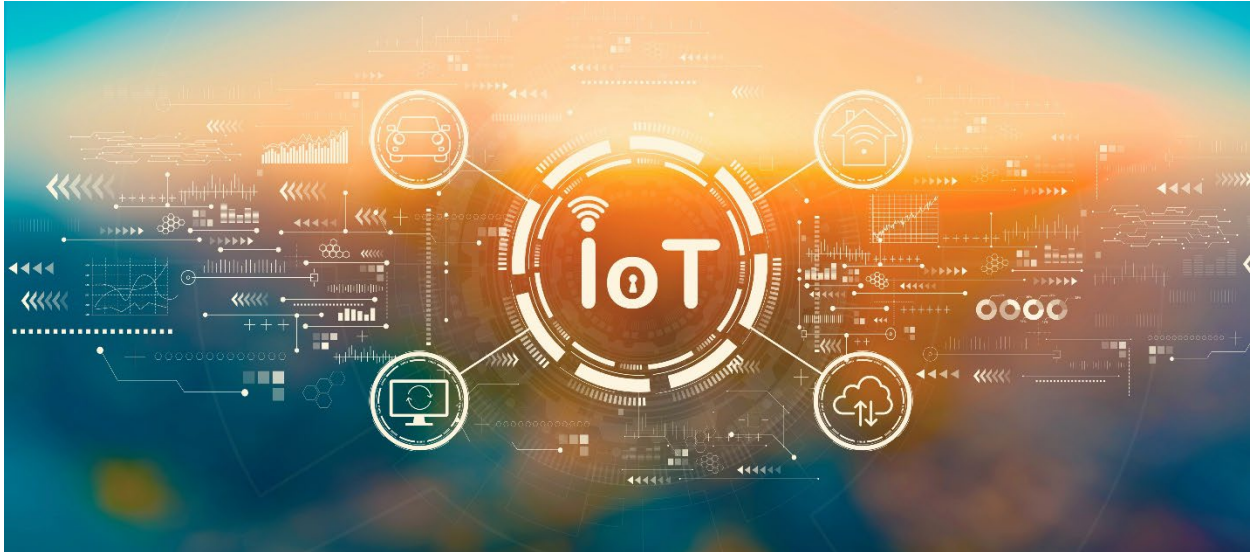
There are numerous benefits from the use of IoT in an industrial context, including:

- Increased efficiency, productivity and quality in manufacturing operations, and associated cost reduction;
- Reduction of errors;
- Predictive maintenance; and,
- Improved Safety
- Data driven insights that support reporting and compliance.

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

- investment to upgrade brownfield to greenfield environments, including the need to ensure **interoperability** with other machines and systems;
- monitoring of **reliability** for industrial devices with IoT technologies 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 for **scalability**, as industrial systems with IoT technologies often involve a large number of devices and must be scalable to accommodate growth., whereas consumer systems with IoT technologies may be smaller in scale;
- **larger attack surfaces** of industrial devices with IoT technologies due to their connectivity, leading to vulnerability from various types of cyber threats such as hacking, malware, and ransomware; and,
- **criticality** related to the cybersecurity of industrial devices with IoT technologies that are vital for the operation of critical infrastructure.

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.



Recommendations of the IoT Advisory Board

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

1. Establishing a National IoT Strategy
2. Modernizing IoT Infrastructure
3. Establishing Trust in IoT
4. Fostering a IoT-ready Workforce
5. Facilitating Industry Adoption of IoT
6. ~~Facilitating~~ Promoting 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. The Board remains in place until [date] to clarify any points for the IoTFWG or to answer any questions about these recommendations.

Establishing a National IoT Strategy

Objective 1: Congress and the White House must work together to create and implement a coherent, comprehensive, and coordinated national IoT strategy.

Key Recommendation KR1.1: Establish a United States national strategy for taking full advantage of the opportunity presented by the IoT.

Supported by Finding x.x

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, multi-faceted research initiative in these areas.¹³³ They said, "those agencies tackling problems whose solutions entail instrumenting the physical world ... should conduct research to design, fabricate, and test sensors that are problem-domain specific and that are cheaper, smaller, better packaged, lower powered, and more autonomous than those available today."

In 2011, an OSTP/NSTC White Paper outlined many reasons why we needed a more comprehensive and strategic approach for taking advantage of the Cyber-Physical System (IoT) opportunities over the horizon to grow our economy and help solve our national challenges.¹³⁴ 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."

¹³³ The 2010 PCAST report is available from: <https://www.nitrd.gov/pubs/PCAST-NITRD-report-2010.pdf>

¹³⁴ The OSTP/NSTC white paper is available from: <https://www.nitrd.gov/pubs/CPS-OSTP-Response-Winning-The-Future.pdf>

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 CPS.¹³⁵

As shown in the earlier section, [The Current State of IoT](#), these predictions from 2011 and 2012 were accurate, and the lack of a national strategy has impacted growth. 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 multi-disciplinary 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,

¹³⁵ The 2012 NITRD report is available from:

https://www.nitrd.gov/nitrdgroups/images/6/6a/Cyber_Physical_Systems_%28CPS%29_Vision_Statement.pdf

all facilitated by dedicated focus, authority, and a central online presence to share strategies, engage stakeholders, and monitor progress.

Enabling Recommendation ER1.1.1: Congress and the White House should Further improve and elevate inter-agency coordination including an IoT National Coordinating Office and appoint a full time Chief Technology Officer .

Supported by Finding x.x

For more than a decade, there was a Cyber-Physical System (CPS) Inter-Agency 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 inter-agency 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 CTO office provided that IoT is added back, as recommended elsewhere in this document.

Enhancing inter-agency 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.

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

Supported by Finding x.x

IoT is critical to U.S. prosperity and socioeconomic success and still faces many barriers to adoption. IoT must be added back to the CET to ensure that the government remains aware of new opportunities to apply IoT and ensure adequate oversight. Yet IoT is no longer included in the list of critical emerging technologies <https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf>.

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.¹³⁶ Others are “coming up”, including edge data and app platforms, serverless/Function-as-a-Service, cloud-connected sensors, edge AI chips, and low code/no code development platforms and satellite IoT connectivity.¹³⁷ 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.¹³⁸

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

[Link](#)

¹³⁷ *ibid.*

¹³⁸ *ibid.*

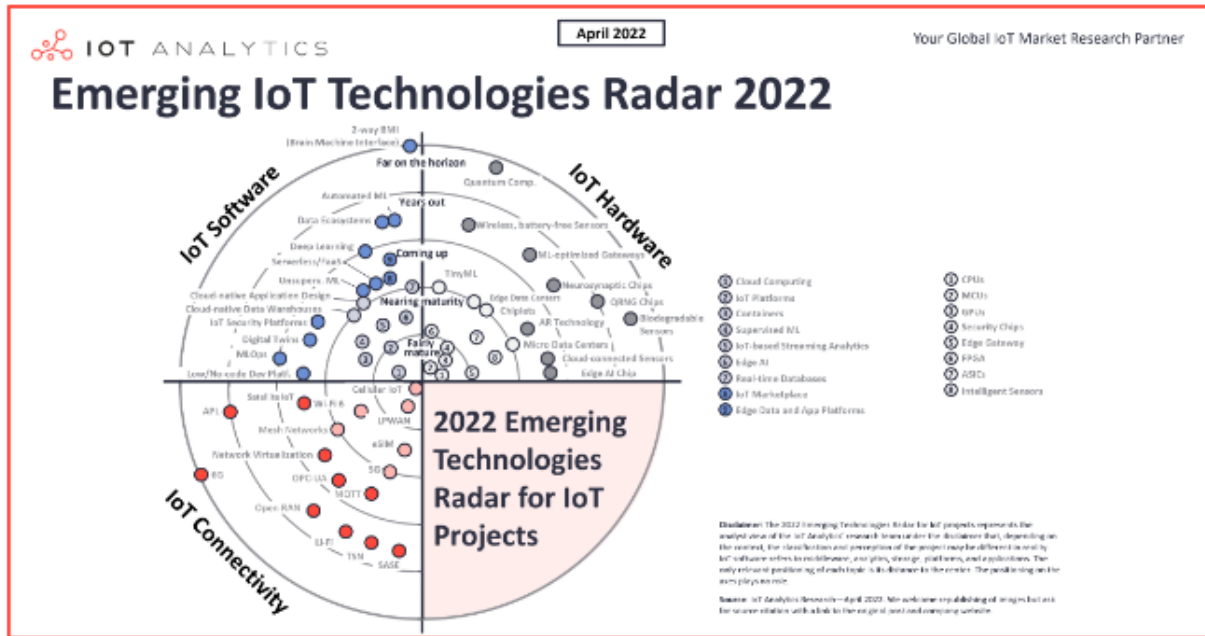


Figure 18 - Caption TBD

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 impacts of Quantum computing and post-quantum cryptography.

Supported by Finding x.x

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 of the primary concerns is that “quantum computers have the potential to bypass the encryption locks that currently protect the world’s communications and data.”[3]

As quantum computing matures, traditional encryption methods are rendered obsolete, leaving IoT devices and their data vulnerable to interception and manipulation. As an example of the power of quantum computing, in a 2019

experiment, Google performed and completed a target computation in 200 seconds that would take the world's fastest supercomputer 10,000 years to complete.¹³⁹

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

¹³⁹ "Quantum Supremacy Using a Programmable Superconducting Processor," J. Martinis, and S. Boixo. Google AI Quantum, October 23, 2019. [Link](#).

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 ERI.1.4: Congress should study the impact of IoT components and modules produced by Chinese companies and other foreign adversaries to assess and understand the risks to cybersecurity, the IoT supply chain, and economic and national security.

Supported by Finding x.x

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. The top two companies currently hold 48% of the global market with one estimate projecting this number will rise to 75% by 2030. 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 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.

Innovation Leadership

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

Supported by Finding x.x

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 technologies is a key component to overcome existing IoT challenges (e.g., cybersecurity, communications, privacy, etc.), 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 startups. 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, 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 pilot project demonstrations.

Supported by Finding x.x

The Board 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 ARPA, DOE, NSF, and DOT. It may also require a more significant role for OSTP in IoT-related research. Failure to do so will slow down government efforts and cut our IoT opportunity short.

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 ERI.2.2: Congress should accelerate adoption of IoT technologies manufactured by small.

Supported by Finding x.x

The federal government should consider actions that accelerate the adoption 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 business 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 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 should 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

or leading startups and small businesses can be referred to others for best practice and learning.

- The Federal Government should 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 SBIR awards. The Federal Government should encourage local governments to leverage its local startup accelerator network to develop technology and fast-track it to local adoption on successes.

The Federal Government can modify guidelines for grant programs and funding mechanisms already in existence for small businesses to allow for greater incorporation of IoT technologies, examples include:

- The U.S. Department of Commerce, Minority Business Development Agency (MBDA) (<https://www.mbda.gov/who-we-are/overview>)
- DOE Office of Small and Disadvantaged Business (<https://www.energy.gov/osdbu/office-small-and-disadvantaged-business-utilization>)
- National Science Foundation Program for Small Business (<https://www.nsf.gov/funding/smallbusiness.jsp>)

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

Supported by Finding x.x

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

- In smart, connected transportation IoT can improve safety in things such as vulnerable road users (i.e., pedestrians at crosswalks), traffic intersections, school, and work zones. Furthermore, opportunities for IoT technologies in electrified transportation manufactured 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.

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 an 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 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 should 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 ERI.2.4: Congress and the Executive Branch should specify and use innovative IoT technologies and applications.

Supported by Finding x.x

The federal government, through its procurement and funding activities, can influence and facilitate action to improve IoT adoption. For example, the GSA and the U.S. Army Corps of Engineers specified the use of Building Information Modeling (BIM) in its projects. As a result, contractors had to comply with the requirement and used BIM tools, which enabled both the government and the contractor to reduce construction and project risks. A similar approach was used to accelerate the utilization of small and disadvantaged businesses (SB and SB8a) in federally funded transportation projects. 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.¹⁴⁰ 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 of infrastructure planning, construction and operation projects. These projects include projects owned by non-federal stakeholders (municipalities, utilities, agencies, states, etc.) and federal stakeholders (federal facilities, infrastructure, etc.).

The 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 and dust and particulate matter generated during construction in order to comply with local air quality regulations. When air quality levels reach certain levels, mitigation measures can be implemented to minimize impacts to worker and community health. IoT sensors and intelligent traffic solutions can be specified into roadway projects to support future intelligent highway and 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.

¹⁴⁰ <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/>

Enabling Recommendation ERI.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 Finding x.x

The federal government should continue to support and fund technology research, through industry, university and its 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.

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 KRI.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 Finding x.x

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

- In smart, connected transportation IoT can improve safety in things such as vulnerable road users (i.e., pedestrians at crosswalks), traffic intersections, school, and work zones. Furthermore, opportunities for IoT technologies in electrified transportation manufactured 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.

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 an 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 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 should 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 ERI.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 Finding x.x

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

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

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

Supported by Finding x.x

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 2017.¹⁴¹ The federal government’s substantial buying power allows it to influence and drive desired outcomes. The government can use direct procurement,

¹⁴¹ “Federal Contract Spending in the Last 5 Years,” K. Bernal, GovConWire, May 25, 2022. [Link](#).

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.¹⁴² While providing the CIA with innovative capabilities, this contract award signaled confidence in the technology to the market.

“For many years, the pace of cloud adoption was slowed by concerns over data 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.”¹⁴³

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 ERI.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 Finding x.x

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

¹⁴² “Amazon Wins \$600 Million CIA Cloud Deal As IBM Withdraws Protest,” K. McLaughlin, CRN, October 30, 2013. [Link](#).

¹⁴³ “CIA’s move to cloud a game changer for public sector,” M. Albertson, Silicon Angle, June 16, 2017. [Link](#).

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. 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. While agency funding and budget allocations for IoT may not be a priority, 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 Finding x.x

Many government facilities are reliant on IoT systems on which functional, operational, and safety needs depend. These can serve as gateways for malicious actors who can 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.

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.

Environmental Protection Agency (EPA) has a program for Energy Star Building Certifications and there could be a similar program that addresses cybersecurity within a building. There are some efforts already underway within the commercial real

estate sector that could be leveraged (<https://buildingcybersecurity.org/>). There are also parallels that could be explored such as the National Cyber Labeling Program for Consumer IoT versus Energy Star on appliances. Owners of buildings used by federal organizations should, at a minimum, use basic cyber hygiene best practices (i.e., changing default passwords, segmentation of networks by using items such as firewalls, installing patches) as directed within requirements. NEMA has developed a cyber hygiene best practice document for end users that is available at the following URL: (<https://www.nema.org/standards/view/cyber-hygiene-best-practices-part-2>)

Executive Order 14057, in tandem with the Federal Sustainability Plan, serves 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.

Enabling Recommendation ER1.4.3: 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 x.x

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 ERI.4.4: The Executive Branch should integrate IoT considerations into the development of national AI strategy and strategic initiatives.

Supported by Finding x.x

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.

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 its 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.

Modernizing IoT Infrastructure

Objective 2: Congress and the Executive Branch should call upon and collaborate with industry to enhance and modernize the infrastructure that enables and supports IoT. Such collaboration should include the provision of clear direction and support for 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.

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.

The Board 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.

Supported by Finding x.x

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. This includes:

- Conducting the research and developing the frameworks that informs 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.
- Collaborate with international governments to harmonize geographic and region-specific standards and practices

In support of this key recommendation, the board has 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.

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

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:¹⁴⁴

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 independently used were 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:¹⁴⁵

¹⁴⁴ IoT research paper, Benson to provide citations

¹⁴⁵ "A Consensus Framework for Smart City Architectures", IES-City Framework Release 1.0, IES-City Framework Public Working Group, September 30, 2018. [Link](#).

- 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*, 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)
- Consider 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.¹⁴⁶

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 x.x

¹⁴⁶ "Smart City Interoperability Reference Architecture," U.S. Department of Homeland Security Science and Technology Directorate, July 8, 2022. [Link](#).

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.¹⁴⁷

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.¹⁴⁸ 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.”¹⁴⁹

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.¹⁵⁰” 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.”¹⁵¹

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.¹⁵² 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.

There are ongoing industry efforts to develop consensus standards including:

- Integrating the Healthcare Enterprise (IHE) promotes the coordinated use of established standards such as DICOM 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)

¹⁴⁷ “The case for medical device interoperability,” V. Gowda, H. Schulzrinne, and B. Miller. JAMA Health Forum, January 14, 2022. [Link](#).

¹⁴⁸ Ken Fuchs, IEEE 11073 Standards Committee Chair, IHE DEV Domain Co-Chair.

¹⁴⁹ IoT research paper, Benson to provide citation

¹⁵⁰ “Medical device interoperability. A safer path forward.” Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. [Link](#).

¹⁵¹ Ken Fuchs response comment to article. [Link](#).

¹⁵² “Medical device interoperability. A safer path forward.” Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. [Link](#).

- 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”.¹⁵³ 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”.¹⁵⁴ 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.

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.¹⁵⁵
- 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 Finding x.x

¹⁵³ “Medtech and the Internet of Medical Things: How connected medical devices are transforming health care,” Deloitte Center for Health Solutions, July 2018. Figure 9. [Link](#).

¹⁵⁴ Ken Fuchs response comment to article in Note 147. [Link](#).

¹⁵⁵ Medical device interoperability. A safer path forward.” Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. [Link](#).

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 supply chains.

Incentivizing Unique 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 Identifier Standards¹⁵⁶ in procurement contracts and regulatory frameworks will optimize risk, cost, and value in supply chain management.

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 services¹⁵⁷. By driving the adoption of IoT technology, the government can minimize supply chain risks 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. supply chains competitive and resilient.

¹⁵⁶ NEED TO ADD REFERENCE FROM GS1 AND ANGELA'S PRESENTATION IN EARLY 2023

¹⁵⁷ NEED TO ADD REFERENCE TO DON DAVIDSON PRESENTATION FROM EARLY 2023

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 Finding x.x

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.

Fostering Innovation and Competition: Establishing common standards will foster innovation and competition throughout the supply chain, simplify integration and maintenance, and potentially reduce costs while ensuring regulatory compliance.

Facilitating Integration and Efficiency: Common standards enable businesses to seamlessly integrate IoT solutions into their supply chain operations, facilitating data exchange and improving decision-making processes.

Collaborative Development: 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.

Education and Awareness: The government should promote these standards through education and awareness campaigns, providing resources and guidance to help businesses implement IoT solutions effectively.

Stakeholder Engagement: 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.

Promoting IoT standards in supply chain management will drive innovation, improve efficiency, and ensure security and reliability. This approach 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 Finding x.x

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 WAVE Project¹⁵⁸ in the streaming media industry. Hosted by the 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 traffic and other data collected from IoT and non-IoT sources.

Supported by Finding x.x

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.

¹⁵⁸ <https://CTA.tech/WAVE>

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 Finding x.x

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 adopting 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 on-board, over-the-air and back-office IT systems. By sharing standardized communication technology solutions, public transportation systems in different cities and regions can achieve interoperability, provide better passenger experience, and manage the transportation system more efficiently. Industry benefits as well, as vehicle manufacturers and integrators gain efficiencies with interoperability to reduce cost and accelerate innovation and enable better

access to the global transit market. ITxPT has a growing international base of support, driven by its international members and by transit agencies around the world eager to deploy smart systems based on open standards and not proprietary solutions. If its adoption is delayed in the USA, the transit industry could lose competitive advantage in an increasingly global market.

- Positive Train Control (PTC). There are numerous PTC systems deployed in North America, with varying features and capabilities though all designed and proven to prevent train accidents. Where train operators share tracks, especially when a mix of passenger and freight rail, multiple PTC systems are installed on rail vehicles. The 3GPP consortium has targeted certain use cases for core support within 5G, including public safety, connected vehicle and train control. In collaboration with International Union of Railways (UIC), 5G is supporting the requirements of the Future Railway Mobile Communication System (FRMCS), of which the main goal is to fully digitalize railway operations, support an increasing level of automatic train operations, and take advantage of the broader capabilities of 5G for passenger travel as well. Train control based on FRMCS has a growing international base of support. If adoption is delayed in the USA, the rail industry could lose competitive advantage in an increasingly global market.

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, US 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. (<https://www.nema.org/standards/view/connected-vehicle-infrastructure-roadside-equipment>). 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 Finding x.x

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 US, particularly rural and tribal communities, where broadband infrastructure is not available. Furthermore, there are large areas of the country, including forests, deserts and the sea and ocean areas adjacent to land, that are remote, barren and unconnected. These unconnected areas of land and sea offer many opportunities for IoT.

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 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. 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 is expensive, not cost effective for rural areas, takes decades to deploy and may not reach all areas
- Service from wireless carriers and operators is best for high density areas but the lack of sufficient financial returns stops wireless operators from entering rural and tribal communities with low population densities
- Geosynchronous satellite broadband service offers coverage over wide areas but suffer 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 includes service bandwidth, spectrum allocation, new connectivity technologies to support IoT at scale, energy efficiency, interference and sixth generation (6G).

-
- **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 for last mile connection. 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 x.x

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.”¹⁵⁹ 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.¹⁶⁰

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

As has been noted, IoT applications are expanding, and continued growth is expected.¹⁶¹ 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.

¹⁵⁹ “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. [Link](#).

¹⁶⁰ IoT Research report – Benson to provide citation

¹⁶¹ *Op cit* the prior background discussion on billions of IoT devices in coming years.

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 spectrum whether existing private sector bands, or underutilized federal spectrum.

Repurposing under-utilized 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 the CTA report, [Unlicensed Spectrum and the U.S. Economy: Quantifying the Market Size and Diversity of Unlicensed Devices](#).

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

Supported by Finding x.x

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

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

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

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

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

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 Finding x.x

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.¹⁶² This is a major challenge as farms occupy vast stretches of land, with the largest farm in the United States spanning 190,000 acres.¹⁶³ 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 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

¹⁶² [“Examining Current and Future Connectivity Demand for Precision Agriculture”, Interim Report FCC, Precision Agriculture Connectivity Task Force, December 2022, Page 2. Link](#)

¹⁶³ [“Top 5 Farms with the Largest Acreage in the U.S.”, E. O’Keefe, Successful Farming, September 28, 2019. Link](#)

- 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 digital infrastructure initiatives to the digital transformation of enterprise business processes.

Supported by Finding x.x

The digitalization of all business functions (e.g., design, production, marketing, procurement, distribution) enables more efficient IoT product management, greater visibility, and transparency over supply chains to track products, monitor quality, and fix issues or defects. By using cryptographic methods, digitalization can have a major impact in improving IoT security, reliability, integrity, and trust of data produced in supply chains and edge applications.

By providing incentives for businesses to adopt digital tools, the federal government can help promote ecosystems that create opportunities for businesses and workers in any value chains which will drive economic growth. Furthermore, digitalization enables digital transformation whereby IoT device suppliers become connected to their customers which enables new business models and services revenue streams.

The government can assist by working with industry stakeholders to develop and communicate clear guidelines and criteria for eligibility of subsidies for digitalization. Agencies may encourage orchestrated PPPs to work on Proof of Concept (PoC) projects to assess the economic value before investing in solutions to deploy at scale. 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.

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.

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 x.x

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.

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 promote 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, goods, and data, to enable cross-border trade, supply chain resilience, and ultimately trusted digital marketplaces.

Supported by Finding x.x

The U.S. (including USTR) should lead a collaboration with the EU and allied nations¹⁶⁴ to develop, promote and adopt a secure cross-border Global Digital Identifier facilitate trade of goods and related data. A global standard like the Universally Unique Identifier¹⁶⁵ (UUID) but optimized for this purpose, can accelerate the use of IoT technologies for cross-border trade, enhance 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, 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

¹⁶⁴ The U.S.-EU TTC should be renewed and can lead with trade agreements to adopt industry consensus standards.

¹⁶⁵ https://en.wikipedia.org/wiki/Universally_unique_identifier

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.

Enabling Recommendation ER2.4.3: The Executive Branch should encourage trusted digital twins and digital threads for accelerating IoT adoption across supply chains and IoT application markets.

Supported by Finding x.x

Promote the use of digital twins¹⁶⁶ and digital threads¹⁶⁷ across disaggregated supply chains, 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 chains¹⁶⁸. The government should incentivize companies to digitalize their workflows, starting from design and manufacturing, to support the development of digital twins across supply chains.

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 supply chains 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.

¹⁶⁶ 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.

¹⁶⁷ Digital flow of data connecting business processes products assets and bill of materials in a value chain. For the electronics value chain the digital thread includes of HBOM, SBOM and other Digital Bill of Materials (DBOM)

¹⁶⁸ McKinsey & Company - [Reimagining fabs: Advanced analytics in semiconductor manufacturing](#)

Encouraging the use of digital twins and digital threads will modernize supply chain IoT infrastructure, improve efficiency, security, and visibility, and foster innovation. This approach will drive economic growth by creating trusted digital marketplaces and enhancing overall supply chain performance.

Establish Trust in IoT

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

Cybersecurity Improvement

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

Supported by Finding x.x

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 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 Finding x.x

This recommendation to strengthen cybersecurity measures focused on IoT across supply chains, and networks aims to address the growing concerns around data privacy, confidentiality, 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 those vulnerabilities most likely to be applicable to IoT product developers.

Supported by Finding x.x

Provide guidance to IoT developers to help them efficiently meet requirements in standards or best practices for addressing “critical vulnerabilities” (or similar requirements for making sure known or identified vulnerabilities are addressed). This may be accomplished, for example, by providing a list of known IoT operating system vulnerabilities that developers should be aware of and address, or a means to filter an existing list for such vulnerabilities.

The government provides key guidance to the private sector in many categories. For IoT, CISA has guidance for IoT acquisition (<https://www.cisa.gov/resources-tools/resources/internet-things-iot-acquisition-guidance-document>), use (<https://www.cisa.gov/news-events/news/securing-internet-things-iot>), and for specific sectors ([https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper 3.6.19%20-%20FINAL.pdf](https://www.cisa.gov/sites/default/files/publications/CISA%20IoT%20White%20Paper%203.6.19%20-%20FINAL.pdf)).

The government also maintains vulnerability lists, including the National Vulnerability Database (NVD) maintained by NIST (<https://nvd.nist.gov/vuln/Vulnerability-Detail-Pages>)

and the Known Exploited Vulnerabilities Catalog (KEV Catalog) maintained by CISA (<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>).

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

One can already filter by “IoT” as a keyword in the National Vulnerability Database, which pulls up 1100+ hits. Those results include many product-specific hits. For example, CVE-2023-23575 is, “*Improper access control vulnerability in CONPROSYS IoT Gateway products allows a remote authenticated attacker to bypass...*” That information is useful to users of the CONPROSYS product, but not to IoT developers. But buried in that the same set of results are items relevant to IoT developers. For example, CVE-2023-23609 is, “*Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. Versions prior to and including 4.8 are vulnerable to an out-of-bounds write...*” As Contiki is an IoT operating system, this result would potentially be useful in this context.

While there is a national interest in IoT developers addressing critical vulnerabilities, there appears to be no resource in the public or private sector that can be mapped to IoT vulnerabilities. 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: The Executive Branch should accelerate the promotion and adoption of IoT technologies to enhance the electric grid's security, reliability, and resilience. (Updated)

Supported by Finding x.x

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 cyber-attacks, 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 the use of technologies enabled by IoT, such as smart inverters and energy storage systems. So, if we can't 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 man-made 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: <https://www.energy.gov/articles/us-department-energy-announces-48-million-improve-reliability-and-resiliency-americas>

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 ER3.1.4: Congress and the Executive Branch should support domestic IoT cybersecurity labeling initiatives by establishing incentives for manufacturers to participate.

Supported by Finding x.x

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 ER3.1.5: Congress must ensure adequate and ongoing funding for the Cyber Trust Mark consumer education campaign.

Supported by Finding x.x

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

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

But a public service advertising campaign is required as well. This PSA campaign must be broad and effective enough to create high Mark recognition among the U.S. population. Such results are beyond the reach of manufacturers and retailers. The U.S. government must take a leading role.

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

Enabling Recommendation ER3.1.6: 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 x.x

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

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

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

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

Going forward, NIST, as the central agency of IoT cybersecurity expertise, should be part of such harmonization discussions. As program ownership is determined, as is the case of FCC with the U.S. Cyber Trust Mark, that program owner should also be deeply involved in harmonization discussions. State, with international relationship responsibility, can assist in convening or coordinating.

Enabling Recommendation ER3.1.7: The Executive Branch should recognize and promote existing standards and conformity assessment schemes that facilitate cybersecurity in industrial IoT applications.

Supported by Finding x.x

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

Data Privacy Policy and Regulation

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

Supported by Finding x.x

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

To effectively implement this regulation, several challenges need to be considered. These include addressing four key aspects of data privacy - collection, storage, use, and sharing - and carefully considering the costs associated with implementing and enforcing the new regulation. Additionally, there needs to be a well-thought-out

transition period and set compliance deadlines for businesses presently operating under various State laws.

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

Enabling Recommendation ER3.2.1: Congress should include IoT in proposed comprehensive privacy legislation.

Supported by Finding x.x

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 ER3.2.3: The Executive Branch should promote "Privacy by Design" in IoT device development, deployment, and implementation.

Supported by Finding x.x

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 potential resistance from the private sector, which might perceive PbD implementation as risky or costly. Another significant challenge is developing universally accepted privacy standards for IoT.

For the successful execution of this recommendation, the involvement of key U.S. government agencies is essential. The Office of Science and Technology Policy (OSTP), the National Institute of Standards and Technology (NIST), and the Federal Trade Commission (FTC) are identified as critical players in championing this recommendation.

To effectively implement PbD in IoT, the U.S. government needs to consider several factors. These include the development of clear PbD guidelines and the provision of incentives to companies that comply. It's also important to ensure the adaptability of these principles across various IoT devices and to align them with international privacy standards. Support for small and medium enterprises (SMEs) in adhering to these principles is crucial, as is the regular evaluation and refinement of guidelines and incentives. 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 ER3.2.4: Congress and the Executive Branch should establish clear policies for third-party data sharing and IoT device data use.

Supported by Finding x.x

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 Department of Energy (DOE), the United States Department of Agriculture (USDA), and the Office of the National Cyber Director (ONCD), are identified as key players who could assist or champion the recommendation, contributing to the establishment of a more secure and transparent IoT ecosystem.

Enabling Recommendation ER3.2.5: Congress and the Executive Branch should encourage the use of plain language in IoT privacy policies.

Supported by Finding x.x

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 ER3.2.6: Congress and the Executive Branch should develop and implement privacy transparency mechanisms.

Supported by Finding x.x

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 ER3.2.7: Congress and the Executive Branch should endorse universal opt-out signals for IoT devices and companion apps.

Supported by Finding x.x

In an initiative to bolster privacy and data protection in the Internet of Things (IoT) realm, the U.S. government is recommended to endorse Universal Opt-Out Signals for IoT devices and their companion apps. This proposal is driven by the growing need to safeguard user privacy in an increasingly interconnected digital world. Adopting Universal Opt-Out Signals would simplify the process for consumers, enabling them to easily manage their privacy settings across various IoT devices and applications. Standardized guidelines or legislation may be necessary to ensure uniform adoption of the Universal Opt-Out Signals.

Resistance from IoT manufacturers and app developers is anticipated, primarily due to the potential costs and complexities of implementing these signals. Additionally, the technological constraints of harmonizing these signals across different platforms and devices pose a significant challenge. Another crucial aspect is effectively communicating to consumers how Universal Opt-Out Signals can facilitate easier management of their privacy rights.

Several agencies within the U.S. government could play pivotal roles in championing this initiative, including the Federal Trade Commission (FTC), the National Institute of Standards and Technology (NIST), the Federal Communications Commission (FCC), and the Department of Commerce.

In formulating the implementation strategy, the government should consider leveraging existing frameworks and regulations. This includes the National Cybersecurity Strategy Implementation Plan of July 2013, which suggests initiating a U.S. Government IoT security labeling program. Furthermore, existing privacy laws like the California Consumer Privacy Act (CCPA) and its amendment, the California Privacy Rights Act (CPRA), along with the Colorado Privacy Act (CPA) and the Connecticut Data Privacy Act (CTDPA), provide valuable precedents for enforcing privacy provisions starting from 2024. These laws and initiatives could serve as models for developing a comprehensive and effective system of Universal Opt-Out Signals in the IoT space.

Enabling Recommendation ER3.2.8: Congress and the Executive Branch should require IoT Privacy information on new car automobile “Monroney Labels”.

Supported by Finding x.x

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 now 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, which reveals that all 25 car brands reviewed in this report collect personal data, with most sharing or selling this information. The report further indicates that most brands offer limited control over drivers' data, and many have concerning records regarding privacy breaches. Notably, the report notes that none of the car brands reviewed that participate under the Alliance for Automotive Innovation adhere to voluntary consumer protection principles focusing on data privacy.

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 prepare for possible resistance from automakers concerned about cost implications, the task of educating consumers about the importance of this information, and the complexity of the regulatory landscape governing IoT and privacy.

A united effort from various U.S. government agencies is imperative to successfully implement this recommendation. Agencies such as the Federal Trade Commission (FTC), National Highway Traffic Safety Administration (NHTSA), Federal Communications Commission (FCC), Department of Transportation (DOT), and the 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 ER3.2.9: Congress should add "Location Tracking Enabled" disclosure to future U.S. device labeling initiatives.

Supported by Finding x.x

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 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 ER3.2.10: The Executive Branch should promote the use, development, and implementation of Privacy-Enhancing Technologies (PETs) in IoT systems.

Supported by Finding x.x

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 of the primary hurdles in this endeavor is the resistance from the private sector, often stemming from perceived risks or costs associated with PET integration. A U.S. government initiative that not only promotes PETs but also offers guidelines and support could be instrumental in helping manufacturers. Such an initiative would facilitate the production of more privacy-conscious IoT devices, thereby reinforcing the security and trustworthiness of IoT systems in the eyes of users and manufacturers alike.

Enabling Recommendation ER3.2.11: 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 x.x

Follow NIST sanitization standards for government automobiles before resale:

In enhancing privacy and security in the used automobile sector, the U.S. government faces a crucial recommendation: to mandate that car seller organizations adhere to the National Institute of Standards and Technology's (NIST) media sanitization guidelines before reselling vehicles. This recommendation aligns with the e-Stewards Standard, supported by the Environmental Protection Agency (EPA) Recycling Program. The core objective is to protect consumer privacy and prevent unauthorized access to sensitive data that modern vehicle systems often store.

The implementation of this recommendation, however, is not without its challenges and considerations. The U.S. government must account for the financial implications for car sellers, who would bear the cost of implementing these sanitization standards. Additionally, there's a need for comprehensive training and awareness programs to familiarize car sellers with the NIST guidelines. The technological infrastructure to support these sanitization processes is another vital consideration, along with robust mechanisms for monitoring and ensuring compliance.

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 standards for automobiles before resale:

In response to the emerging privacy and security challenges associated with the resale of government automobiles equipped with IoT technologies, a significant recommendation has been proposed: Mandating NIST Sanitization Standards for Government Automobiles Before Resell. This narrative encapsulates the key aspects of this recommendation.

The U.S. government is advised to ensure that before reselling, all agencies adhere strictly to the media sanitization guidelines set forth by the National Institute of Standards and Technology (NIST) before reselling. This requirement is not just a procedural formality but a critical step to safeguard consumer privacy and prevent unauthorized access to sensitive information that might be stored in modern vehicle systems. Such an approach aligns with the e-Stewards Standard, supported by the Environmental Protection Agency (EPA) as part of its Recycling Program.

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 KR3.4: 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 Finding x.x

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. This will build trust in the data and functionality of IoT systems across the entire ecosystem.

Importance of Traceability. Supply chain and life-cycle 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 SBOM¹⁶⁹ to trusted HBOM¹⁷⁰ in IoT

¹⁶⁹ Software Bill of Materials for Electronic parts and Software modules used in the assembly of a device or systems.

¹⁷⁰ Hardware Bill of Materials must include a Root of Trust and Entropy for security and unique ID (fingerprint).

systems, industries can help mitigate the risks associated with supply chain security, compromised components, and ensure the security and reliability of critical systems.

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 supply chain 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.

Enabling Recommendation ER2.4.3 should be here

Enabling Recommendation ER3.4.1: 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 Finding x.x

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 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. The government's active role in promoting these capabilities can contribute to more resilient supply chains and valuable end-to-end solutions.

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.

Objective 4: The U.S. should invest in and promote initiatives that will improve the knowledge, skills, and abilities of those who develop, implement, and operate IoT devices, applications and systems.

Key Recommendation 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 Finding x.x

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.¹⁷²

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.

¹⁷² Highway Funding for Workforce Development. U.S. Department of Transportation. [Link](#).

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

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 Finding x.x

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 operations 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 Finding x.x

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 hinder 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 Finding x.x

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.

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 BIL, IRA, CHIPS Act, NSF, Justice40, 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 Finding x.x

- Integrate this training into existing or planned federal initiatives
- Curriculum Development: Collaborate with industry experts, academia, and data privacy authorities to create a robust curriculum focusing on the latest data protection laws, regulations, and best practices.
- Certification Programs: Establish certification programs to validate the expertise of IoT professionals in data privacy and security, ensuring they are well-equipped to handle sensitive information responsibly.
- Continuous Education: Implement mandatory continuing education requirements to keep the workforce updated on evolving data privacy standards and emerging threats.
- Awareness Campaigns: Launch awareness campaigns to emphasize the importance of data privacy, promoting a culture of security and compliance.
- Partnerships: Partner with leading technology companies and data privacy advocacy groups to provide cutting-edge training resources and tools.
- Assessment and Monitoring: Develop mechanisms to assess the effectiveness of the training programs regularly and make necessary adjustments to address new challenges and technologies in the IoT landscape.

Facilitating Industry Adoption of IoT

Objective 5: The United States is recognized as an international leader in the innovation, deployment, and operation of IoT technology. Actions by U.S. government leaders set an example for private sector stakeholders and international partners.

Leverage Federal Grants and Programs To Improve IoT Technology Use

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

Supported by Finding x.x

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

IoT enables new business and operating models. Economic service models to assist could include extended funding for O&M for select applicants (i.e., rural, tribal, small towns, etc.), encourage regional cost sharing for multiple cities in a region to apply as one, and encourage innovative models (e.g., corporate sponsorships).

Funding models to consider include extending funding for O&M for select applicants (rural, tribal, small towns, etc.); regional cost sharing where multiple cities in a region apply as one group; and innovative models that partner with industry or sponsors.

Enabling Recommendation ER5.1.1: The Executive Branch should encourage other financial or funding models to help adopting organizations to sustain and support IoT projects.

Supported by Finding x.x

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 short-term due to limited funds. Current grant application criteria may also exclude those unable to sustain long-term operations.

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 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.

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 benefit from IoT adoption.

Supported by Finding x.x

The federal government should develop programs and grants to help underserved and less developed communities benefit from IoT adoption.

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 x.x

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

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

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

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

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 Finding x.x

Developing a comprehensive Agricultural IoT Strategy is essential for enhancing productivity, resource efficiency, and environmental sustainability in agriculture.

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 Finding x.x

Farms have a variety of equipment and machinery from different manufacturers that can't communicate or exchange data with each other, each with its own data formats and languages. The agriculture industry model is to develop s/w and devices in proprietary formats.¹ This lack of interoperability hinders data sharing, automation of processes, and timely diagnosis and analysis of problems to create positive outcomes. In addition, costly manual labor is required to extract the data for use.

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.

Enabling Recommendation ER5.2.3: Congress and the Executive Branch should facilitate small farm/ranch adoption of IoT technologies.

Supported by Finding x.x

Small farms (< \$350,000 GCFI)² are 90% of all U.S. farms (~1.8 million farms), own 49% of farmland, but represent 20% of production. They operate with <10% margins. Because of their small scale and low margins, they are cash flow constrained and do not have the capability to buy IoT or smart equipment, even if they want to.

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 Finding x.x

Smart equipment cannot be fixed by farmers. In many cases, it required servicing by the equipment dealer technicians. These repairs are expensive and may take a long time to get fixed. These may occur at sensitive times for farmers who can't afford the wait, such as during harvest season. Today, farmers are getting around this by purchasing "hacked" software from Eastern Europe or buying older non-smart equipment that they can maintain and repair themselves.³

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 communities.

Supported by Finding x.x

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 x.x

The federal government should facilitate and support the development and use of smart community / sustainable infrastructure reference models that capture and document the ecosystem.

Smart communities are complex ecosystems of communities, neighborhoods, districts, buildings, other cities, utilities, and businesses that co-exist, collaborate occasionally and interoperate with each other. A framework is 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.

Enabling Recommendation ER5.3.2: Congress and the Executive Branch should develop Smart Community and Sustainability Extension Partnerships (SCSEP).

Supported by Finding x.x

IoT can bring great economic and societal benefits to our cities, but specific smart community and sustainable infrastructure expertise in industry is limited, unevenly distributed, and fragmented. Some cities and agencies also lack the tools and resources, and even smaller cities and agencies may be even more constrained. Municipalities and agencies may not have the budget, the empowerment, or the ability to engage the necessary resources.

A different way to engage these resources is needed. The public procurement processes to engage private sector resources are burdensome. A SCSEP similar to existing partnerships (e.g., MEP, USDA) would be a worthwhile investment, and would provide an improved model over the current public procurement process to engage private sector resources. SCSEP should be put in place and operational to support sustainable infrastructure projects funded through the Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act (IRA). The role of states should be defined. In particular, some BIL and IRA funding may be given to states to manage and allocate. Consideration should be given as to whether some of these activities can be performed through the existing extension offices and infrastructure, or through partnerships with regional consortiums or states.

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 and equity of benefits of IoT and smart technologies for local communities.

Supported by Finding x.x

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 communities/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: 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 Finding x.x

The government should facilitate smart community opportunities and adoption of IoT for rural communities. This may include:

- Coordination with federal agencies (USDA, NTIA, EPA, DOT, etc.) to drive community awareness of IoT opportunities, and support programs that encourage industry participation.
- Offering project grants for community related IoT projects and deployment projects (e.g. environmental monitoring).
- 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).

Rural communities lack many of the same resources, services and amenities that residents in urban areas benefit from. The lack of infrastructure, low population densities, private sector investment and other factors contribute to the urban/rural divide. For example, many rural areas are considered medical deserts with limited number of healthcare providers and facilities. As a result, healthcare access inequities

exist. Telehealth and home healthcare monitoring are IoT-enabled services that can alleviate some of these inequities.

Enabling Recommendation 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 Finding x.x

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.

Enabling Recommendation ER5.3.6: The Executive Branch should Facilitate small to medium city adoption of smart community technologies.

Supported by Finding x.x

There are 1300 cities that have less than 250,000 people. These cities lack the funding, expertise and resources to implement, operate and maintain smart community technologies. At the same time, these smaller cities have needs that are different from their larger city counterparts and may require grants that are more aligned to their needs.

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.

Enabling Recommendation ER5.3.7: The Executive Branch should Facilitate equity in realization of smart community benefits.

Supported by Finding x.x

Benefits of IoT and smart community technologies are not available to all members of a community. Socioeconomically challenged and rural communities may not have the broadband infrastructure or have limited resources to implement and operate smart community technologies. The new jobs created by IoT, smart communities and digital transformation require skills and education that members of underserved communities may not be able to develop. Some services enabled by these technologies require smart phones and Internet service to access, which some

community members may not have, while others are offered in ways that cannot be accessed by residents (e.g., due to language barriers or lack of digital literacy skills).

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 x.x

Enabling Recommendation ER5.4.1: The Executive Branch should include privacy and data usage policies in federally-funded public safety and smart community projects that use IoT technologies.

Supported by Finding x.x

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 awareness and understanding of these technologies is a major cause of these concerns. The community is often unaware of how these technologies work, its 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.

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.

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, potential bidders will need to discuss how they will market this program to its customers (public safety agencies, cities, etc), 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.

Communities have very limited ability to purchase IoT equipment for public safety on their own, with supplemental funding from external sources. This includes systems that support law enforcement, fire, emergency management services, and public safety access points.

The adoption of IoT for public safety is limited for a variety of reasons, including a lack of awareness, lack of funding, interoperability challenges, privacy concerns and community support. Each community has its own unique priorities, needs and systems that translate to different types of IoT systems and applications that best serve their community.

IoT devices, systems and applications should be interoperable with the FirstNet network. This at least drives us toward some sort of connectivity and perhaps functional interoperability. Grants offered could 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.

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. Grants offered should support or integrate into, as relevant and applicable, next generation 911 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.

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 x.x

Enabling Recommendation ER5.5.1: The Executive Branch should promote IoMT as an enterprise priority, including to healthcare facilities' leadership teams.

Supported by Finding x.x

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.

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 Finding x.x

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 those vulnerable legacy equipment and devices that cannot be patched, or upgradeable, or were not subject to compliance with section 524B of the Federal Food, Drug, and Cosmetic Act (FD&C Act).

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.

Healthcare and medical IoT devices and systems are susceptible to cyberattacks. These cyberattacks not only expose sensitive and personal health data and information, but they could lead to disruption to the operation of the devices and systems, leading to potential injury and loss of life. Areas of healthcare and medical device IoT cybersecurity concerns include:

- Vast attack surface due to the interconnected nature of IoT and IoMT devices. Each connected device represents a potential entry point for malicious actors seeking to exploit vulnerabilities.
- Protecting data in transit and at rest is of concern because the data generated by IoT and IoMT devices in healthcare include sensitive patient information. Encryption is critical to preventing unauthorized access.
- Unauthorized access to healthcare data can have severe consequences, ranging from identity theft to compromised patient care. Robust authentication and access control mechanisms is essential to restrict data access to authorized personnel only.
- Patching millions of IoT and IoMT devices is logistically and operationally challenging. These devices often have a longer life cycle than traditional IT devices, and some lack the capability for regular software updates. Not all device and system owners apply patches and firmware updates.
- Legacy systems and devices that cannot be patched or updated with the latest software to address known vulnerabilities
- Compliance with regulatory frameworks (e.g. HIPAA) can be challenging due to the dynamic and evolving nature of IoT and IoMT technologies.

Securing endpoints (devices) and gateways against unauthorized access and breaches is critical as they act as crucial points in the data transmission process for IoT and IoMT devices.

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 x.x

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. In addition, many have limited transit options to go see a doctor on a regular basis.

As a result, healthcare access inequities exist. Telehealth, home healthcare monitoring and consumer health tracking are IoT-enabled services that can alleviate some of these inequities by providing access to healthcare and improving their health outcomes.

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 Finding x.x

Facilitating the adoption of AI in IoT for healthcare is crucial for improving health outcomes through advanced data analysis and personalized treatments.

Challenges in AI for Healthcare include:

- **Automating Data Analysis:** AI can automate the analysis of vast amounts of IoT and health record data, but creating clinically appropriate, reliable, and personalized outcomes remains a challenge. Ensuring AI recommendations are explainable and accurate is critical for patient trust.
- **Edge AI Technologies:** For healthcare devices, it is important for Edge AI technologies to function without needing high bandwidth connectivity to backend cloud services. This is especially beneficial in rural locations and healthcare facilities with lower connectivity levels, as Edge AI devices are less vulnerable to remote attacks.
- **Complexity of Healthcare Data:** AI algorithms analyze patient data, provide recommendations, and sometimes take autonomous actions. However, diagnosing complex diseases like cancer and identifying effective treatments for individuals is challenging due to varying patient reactions and the potential for outdated, biased, or incomplete data. The lack of explainability in AI decisions can lead to adverse outcomes and reduced confidence in AI systems.

Providing incentives, R&D grants, and awards for edge networks and peer-to-peer capabilities is essential. Healthcare institutions need digital health data to be processed at the edge, reducing the amount of information exchanged with central servers and the cloud. This approach enhances the privacy of digital health data.

Adopting AI in IoT for healthcare, particularly through Edge AI technologies, will improve data privacy, enhance the reliability and accuracy of medical recommendations, and build patient trust. This strategy will lead to better health outcomes, especially in rural areas with limited connectivity, and ensure the secure and efficient use of AI in healthcare settings. This approach will significantly increase the privacy of digital health data.

Enabling Recommendation ER5.5.5: Congress should enact HIPAA-like protection for users' medical data in mobile applications and IoT devices.

Supported by Finding x.x

Many consumer-grade IoT devices and mobile apps collect users' sensitive medical data. Consumers tend to believe that this data is protected similarly to medical data in a healthcare facility, but it is not.

Consider medical data as a category for defined data protections. It should be noted that this Recommendation represents a major change. Many organizations have IoT products but no HIPAA experience. While the direction should be clear, the impact should be understood in advance through study, and the transition period adequate to allow manufacturers to adapt without unnecessary impact.

The desired goal is to extend HIPAA protections to these classes of devices and mobile apps or enact a similar type of protection.

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 Finding x.x

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 x.x

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.

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.

Data from these traditional and community environmental sensor systems should 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.

For maximum benefit, a number of barriers that 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.

Enabling Recommendation ER5.6.2: Congress should facilitate and support the research, development and deployment of low-cost Air Quality sensors.

Supported by Finding x.x

The Board observed that there is a need to shift from expensive (i.e., highly sensitive regulatory grade) monitors that limit deployment by organizations and municipalities. Furthermore, there is a widespread interest in participatory science (aka citizen science) where communities or individuals are actively engaging in air quality monitoring. While such monitors are vital for particular purposes, large scale deployment of these types of monitoring equipment would be expensive and difficult. Low-cost air quality sensors enable widespread monitoring for numerous applications and by multiple types of users.

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

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

Agencies should encourage automated and consistent measurement and can facilitate research in low-cost sensing technologies for criterial regulated air pollutants. Additionally, research should be supported for other emerging chemical of concern.

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 x.x

Develop a comprehensive, nationwide water monitoring infrastructure that leverages IoT technology for real-time, accurate, and cost-effective water quality and quantity data collection. This infrastructure should support data-driven decision-making, address the challenges of water scarcity, contamination, and climate change, and integrate with existing NOAA water models for enhanced forecasting and management capabilities.

Current water monitoring systems are often fragmented, inefficient, and insufficient to address the growing challenges of water management. IoT technology enables real-time, remote, and continuous data collection, allowing for proactive responses to

water-related issues. For example, integration with NOAA water models could enhance forecasting and management capabilities, leading to more effective water resource planning and allocation.

Efficient water management is crucial for consumption, agriculture, and industry, ultimately contributing to environmental and economic sustainability. 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.

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 x.x

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 emission with enable the implementation of effective mitigation strategies and contribute to national and global efforts to reduce carbon emissions.

These actions are particularly important because greenhouse gas reporting protocols are recently experiencing increased adoption and many of these reporting protocols include greenhouse gas emissions beyond those associated emitted at the company's site (scope 1) and emissions associated with the generation electricity that the company consumes (scope 2). These indirect, "scope 3" emissions can be challenging

to monitor since they are distributed across supply chains of products and services a company uses (e.g., the transportation of the company's product).

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 complement and support wide area environmental situational awareness capabilities to monitor and inform on a variety of environmental conditions and hazards in environmentally sensitive areas.

Supported by Finding x.x

The use of proprietary technologies and systems are common in systems used to monitor various environmental conditions for first responder, scientific research, and safety applications.

The federal government should facilitate and promote the use and integration of IoT technologies to complement and support wide area environmental situational awareness capabilities to monitor and inform on a variety of environmental conditions and hazards in environmentally sensitive areas. Examples of opportunities where IoT technologies should be incorporated include forest monitoring, wildfire monitoring, earthquake detection, flood, air quality, etc.

Many existing environmental monitoring platforms today use proprietary technologies. One example are the stream gauges used by various federal and state agencies, local governments and private water rights owners to monitor water flow conditions to determine river health and warn on flooding situations. Data collected

from proprietary systems are not easily shared nor integrated with data from other sources, thus limiting timely analysis and responsive actions.

Environmental situational awareness monitoring is crucial for ecological health, public safety, and disaster recovery. 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 man-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.

Smart Transportation

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

Supported by Finding x.x

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 Finding x.x

Many of these transportation technologies incorporate the use of IoT. Federal funding can also serve to increase private sector investment.

Greater adoption of smart, connected, and electrified transportation technologies could help in the following examples:

- Incorporation of technologies enabled by IoT: Opportunities for IoT technologies in smart, connected transportation include sensors, cameras, and

edge computing devices that can improve safety in things such as vulnerable road users (i.e., pedestrians at crosswalks), traffic intersections, school and work zones. Opportunities for IoT technologies in electrified transportation include in car systems or mobile apps that can locate charging stations, as well sensors that manage charging stations to gather data about usage and performance, to anticipate maintenance needs, and troubleshoot problems.

- Improving overall traffic safety: Vehicles that have technologies such as Cellular Vehicle to Everything (C-V2X) can communicate basic safety messages and information to corresponding infrastructure and other road users thereby reducing traffic and pedestrian fatalities.
- Reduction in greenhouse gas emissions: The transportation sector generates the largest share of greenhouse gas emissions a big contributor to climate change. Electrification of transportation away from traditional fossil fuels are a viable option for transportation. Also smart, connected transportation can improve traffic flow and reduce congestion which is also better for the environment.

With the Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act (IRA) the Federal Government is already taking steps to electrify the transportation sector. Funds are being directed to the states to deploy electric vehicle charging stations via the NEVI Formula Program (<https://afdc.energy.gov/laws/12744>). Under the IRA tax credits are available for EVs that are primarily assembled in North America. 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. (https://www.nema.org/docs/default-source/nema-documents-libraries/whitepaper-on-outcomes-based-contracting.pdf?sfvrsn=f3ad2716_2)

Earlier this year ITS America published the National V2X Deployment Plan which includes a call to action for the federal government, as well as state and local transportation agencies, automotive OEMs, and other stakeholders to install V2X systems for public safety – beginning with signalized intersections, other road users and selected production vehicles (<https://itsa.org/advocacy-material/its-america-national-v2x-deployment-plan>)

Promoting an IoT Enabled Economy

Objective 6: The U.S. can facilitate economic and societal benefits by taking specific actions to advance the integration of IoT with supply chain operations, public-private partnerships, and artificial intelligence.

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

Supported by Finding x.x

Monitoring and evaluating the progress of IoT adoption in supply chain logistics is essential to ensure strategies are effective, 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 Finding x.x

[Need to draft text regarding how the government can support innovation and investment in the use of IoT for supply chain operations. The result would be enhanced competitiveness]

The U.S. would benefit from additional jobs and economic growth, including business benefits from improved effectiveness and efficiency. Increased visibility will also promote sustainability and productivity.

Financial incentives will help, but funds are limited so the government should have 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.

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

Public and Private Partnership

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.

Supported by Finding x.x

The federal government should lead the formation of collaborative public-private partnerships (PPPs) to accelerate the adoption of Internet of Things (IoT) technologies within supply chain logistics operations. These partnerships bring together a diverse array of stakeholders, including government agencies such as the Department of Commerce, logistics providers, IoT technology companies, and academic institutions such as MIT's Center for Transportation & Logistics. This will foster collaboration and knowledge exchange, driving adoption of IoT technologies for supply chain 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 in supply chain operations.

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 the supply chain industry. 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 Finding x.x

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.

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.

Implementation Considerations. 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 Finding x.x

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 throughout the supply chain. This flow of information—from raw materials to installed systems—can inform security and product integrity. Each stage in the supply 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: Actively promote and support the adoption of AI in IoT applications to improve decision-making, optimize resource utilization, and enhance productivity.

Supported by Finding x.x

AI has the potential to revolutionize the way workers in many sectors analyze and use IoT data. By leveraging advanced algorithms and machine learning techniques, AI can enable personnel to identify patterns, optimize resource allocation, and make better informed decisions. This will result in benefits for various stakeholders, including business owners, policymakers, and consumers.

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.)

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. This can be achieved through collaborations with extension centers, universities, and industry experts. Agencies could also offer workshops, webinars, and online courses to ensure widespread access to knowledge and training opportunities.

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 Finding x.x

The government should promote trusted AI-IoT (AIoT) platforms within circular value chain ecosystems to enhance transparency, sustainability, and economic growth. Circular supply chains aim to keep resources in use for as long as possible through sustainable processes like recycling and remanufacturing. 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. This initiative ensures a foundation for responsible and sustainable technological advancement.

Key Recommendation ER6.4: Congress and the Executive Branch should provide overarching regulatory guidance for the unmanned aerial systems (drone) industry.

Supported by Finding x.x

Drones integrated with IoT technologies can leverage real-time data and automation capabilities to enhance functionality and efficiency. The adoption of drone technology can significantly impact key sectors, including agriculture, energy, and environmental monitoring, specifically:

- **Agricultural Efficiency.** In agriculture, drones equipped with advanced sensors can efficiently scout farms, pinpointing areas of pest infestations, disease, or poor irrigation. This drives precision farming by reducing excessive chemical use, enhancing productivity, and ensuring environmental sustainability.
- **Energy Sector Monitoring.** For the energy sector, drones can monitor electric grids, detect faults, and identify maintenance needs, helping to prevent power outages and ensure a stable power supply. This increases reliability and reduces operational costs.
- **Environmental Monitoring.** Drones are crucial for environmental monitoring, such as detecting wildfires early, which helps mitigate their devastating effects. Drones can also perform tasks like spraying pesticides or fertilizers, reducing human exposure to harmful chemicals and ensuring precision.

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 and facilitate equity in the accessibility, realization and distribution of value and benefits created from the adoption and use of IoT.

Supported by Finding x.x

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 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.

Conclusion

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

References

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

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

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

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

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

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

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

U.S. & UK Data Bridge (Added to the Privacy Shield Replacement)

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

Acknowledgements

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

Include speakers with links to meeting materials

Appendix A: IoT Stakeholders

The Internet of Things (IoT) provides the potential significant economic and societal benefits to individual personas, communities, businesses, and academic and government organizations across the United States. Some of these benefits provide incremental value, while others are more significant and transformational. The benefits offered by IoT are not uniform but vary across groups of people, organizations, and application markets. The benefits range from positive outcomes from the use of IoT to creation of new jobs related to IoT and those indirectly related to IoT. This section provides a brief description of which stakeholders and personas are impacted, and in what ways.

Manufacturers

IoT in manufacturing can best be categorized via the following types: companies that design and manufacture chips and modules (i.e., Intel, Qualcomm, Samsung), companies that assemble modules and produce branded products (i.e. Cisco), contract manufacturers that receive a chip design and deliver a packaged chip (i.e. GlobalFoundries), and manufacturers who receive a design and Bill of Materials, assemble them as part of their manufacturing operations, and deliver a finished product (i.e. Rockwell). There are two types of manufacturers involved with the production of IoT. Component manufacturers produce the basic IoT products that are used in the development of IoT-enabled “smart” products. For example, semiconductor and sensor manufacturers produce the core components used in IoT devices. Module manufacturers then purchase and assemble these semiconductors, radios, and sensors together to build modules that brand developers (see below) and device manufacturers purchase.

Manufacturers benefit from IoT in a variety of ways. The demand for IoT products creates significant direct and related revenue, jobs and business expansion opportunities in a variety of markets. IoT products generate immediate revenue for existing products, as well as pull through demand for other higher margin products, such as faster processors, storage devices, and sensors. For example, the continuing evolution of IoT demand has created the need for higher price and margin AI capable microprocessors. In addition, the buildout of IoT systems creates demand for edge servers and storage.

Manufacturers face a variety of barriers. The fragmented nature of the IoT ecosystem adds confusion and complexity in the marketplace and hinders adoption. Slower than expected market adoption of IoT hinders manufacturer investment and continuing product evolution. Overseas competition creates margin pressure on domestic suppliers and limits business expansion. Supply chain disruptions limit the ability to produce enough products and components to meet customer orders. Manufacturers of hardware products have an opportunity to alleviate such barriers by making their products smart-connected IoT products and offer new services including remote support and new Hardware as a Service capabilities.

Developers

In the IoT ecosystem, there are various types of developers. “Brand developers” are businesses whose core product is not IoT but incorporate and integrate IoT technologies into their existing products. For example, a machine tool manufacturer incorporates IoT into their product line, to create “smart milling machines”. The brand developer buys or licenses the IoT technology from a 3rd party, or contracts with a product development firm to develop it for them.

“IoT technology developers” offer hardware, software, and cloud application development services. They contract with brand development companies to create IoT or IoT-enabled products. Technology developers may also work with implementers (see below) to create custom IoT applications to support business, government and other organizations using IoT. Examples of IoT technology developers include product development firms, software development firms, and original design manufacturers (ODM).

IoT offers brand developers a variety of benefits. The addition of IoT to an existing product line creates new value and enables the brand to charge higher prices and is often accomplished with partnerships. The IoT-enabled product line may generate new revenue streams from recurring subscription based models arising from better visibility to the end application including online support, quicker turnaround time of RMAs and bug fixes, and upgrades based on customer changing needs

In addition, the new product line may be more attractive to buyers and allows the brand to expand existing markets and enter new ones. Overall, IoT helps brand developers increase revenues, create recurring revenue opportunities and enhance profitability.

Brand developers face a number of barriers. Digital products require a business process change including infrastructure, operational capabilities, functions, skills, and resources that are different compared to non-digital products. The addition of IoT and digital technologies to traditional businesses and business models brings new complexity and requirements that they may not have the expertise, skills, resources and infrastructure to support. Adding digital capabilities to traditional product lines creates new issues and risks, such as cybersecurity, privacy and interoperability and liability that the developer is unaware of.

New business and operating models enabled by IoT require significant investments that brand developers may be unwilling to commit to or may not be able to sustain for long. Despite the brand developer’s reputation, customers may not be willing to adopt the new IoT-enabled products because of the higher risks associated with cybersecurity and privacy vulnerabilities. Some brand developers pursue a path of digitalization to upgrade the existing infrastructure before embarking to digital transformation which involves a broader business prices change.

Implementers

Implementers are businesses who resell, install and set up, and maintain and service IoT and IoT-enabled equipment to corporate, government, consumers and other buyers. Some businesses, such as retailers, only resell, but not install or service these IoT products, while others offer a full range of services. Typically, the more complex the IoT product is, the more services the implementers offer. Implementers may contract with IoT technology developers to build and implement custom solutions. For example, a HVAC contractor sells a smart HVAC system to a building owner. The contractor will install it, connect it to the network and the building energy management system, configure and test it for proper operation. They sell the building owner a maintenance contract, which requires them to come back on a quarterly basis to maintain the system and optimize its performance. On the other hand, a retailer may only sell a IoT solution but require the buyer to install and set up the solution or find a 3rd party to do so.

For implementer businesses, IoT provides a wide range of benefits. For example, IoT enables to sell add-ons to existing products, or new products, services, leading to a new source of revenue. IoT enables implementers to create new businesses and services on top of existing products and services. This leads to new revenues from existing customers, or new revenues from new customers. Many of the business models enabled by IoT enable implementers to shift away from “one-time” transactional sales to create long lasting recurring revenue streams from subscription services.

Implementers face a number of barriers that hinder their ability to develop, operate and sustain their businesses. Their existing workforce may not be well suited to support and service these new technologies. There is a lack of a suitable and sufficient workforce with the digital skills and capabilities to install, integrate, configure and optimize these technologies. While IoT enables to create new business models, transitioning to those business models are operationally challenging because they may require business process changes and digital transformation, or a shift away from “one-time” large revenues, to recurring small revenues. This requires changing operational and business models. While IoT may offer new long-lasting value, customer adoption of these technologies may take longer. These long sales cycles may drive implementers to abandon these products and services in favor of traditional “tried and true” offerings that drive sales for the business now.

Administrators

Administrators are the owners and buyers of IoT and IoT equipment for business, government and other organizations. They are responsible for the overall management of these technologies and systems, including procurement, integration, operation, maintenance and optimization within the organization. IoT technologies bring together traditional separate functions together, including information technology, operations, and the business units (marketing, technical support, finance and others). Administrators may perform some or all of these functions, or they may contract with 3rd parties, including implementers and developers, to conduct these

activities. Administrators may reside in each of these organizations, or they may be centralized in a single organization.

Administrators are concerned with the benefits of IoT from an organizational perspective. The benefits of IoT depend on the application and usage, but include increased revenues, cost savings and profitability. IoT can create or enhance services and products, and lead to new revenue streams. The usage of IoT may lead to cost prevention, increased operational efficiencies, and staff and resource effectiveness. Other benefits include increased customer satisfaction, retention and loyalty.

Administrators face a number of barriers to IoT adoption in their organizations. These include cybersecurity and privacy concerns, and complexities in integrating IoT into existing information technology (IT) and operational technology (OT) or industrial processes and systems. The joining together of IT into OT and industrial operations creates resistance as it requires these separate functions and teams to break out of silos to work together. Job roles and responsibilities will change, and the workforce may not have the modern digital skills, in integration, data science and programming, to fully utilize these systems.

Operators

Operators are users that use IoT products and IoT-enabled equipment to carry out their day to day jobs in a business, government or other organization. For example, operators in a factory use sensors to monitor and control the manufacturing process to increase finished product quality and reduce scrap. Operators in a power generation facility use sensors and analytics to monitor critical turbine performance to minimize unplanned downtime. Technical support staff remotely monitor sensor data to diagnose equipment deployed in the field. Resellers monitor how customers are using their equipment and make recommendations to optimize performance and outcomes. Facilities operators monitor a building's sensors and systems to optimize comfort, energy usage and operations.

While the benefits to operators vary by operator organization, there are some common benefits. These include higher productivity and performance, reduced quality defects and customer complaints, increased proactiveness and responsiveness to customer needs, reduced operating downtimes and inefficiencies, and lower operating costs and staffing resources, which collectively reduce OPEX.

Operators face a variety of barriers hindering adoption and the full realization of benefits. Operators may require training and reskilling in digital and data skills to properly use IoT-enabled equipment. While IoT increases operations visibility and leads to more transparency and accountability, it may also be perceived as “worker tracking” and is resisted by employees and their unions. Operators may resist adoption because they fear that IoT leads to operational efficiencies, automation and less need for staff. Some operators feel that their “tried and true” experiences and intuition is more relevant and resist the use of the IoT technologies. Finally, the use of IoT may lead to changes in roles and responsibilities, which operators may not be comfortable with or suited for.

Consumers

Consumers purchase and use IoT and “smart” products for their personal or family use. For example, they use “smart watches” to monitor their health and physical activities, receive and communicate messages, and run a variety of apps. They use “tracker” devices to locate their wallets, handbags, keys, luggage and other things. They use “smart assistants” to turn on and off appliances and other devices, get information, listen to music, communicate and run “voice apps”. They use “smart thermostats” to keep the home at a comfortable temperature and save on energy bills. They also use connected cars for real-time navigation, vehicle health monitoring, Bluetooth mobile phone connectivity and personalized driving experiences.

IoT provides a variety of benefits to consumers, including saving money and time, increased convenience and peace of mind, improved awareness, health, safety and performance. The actual benefits vary by IoT devices and their intended uses.

Consumers face a variety of barriers and concerns that hinder adoption, and their ability to fully realize the benefits of IoT. Consumers are concerned about privacy, how the information collected is being used, and whether that information is used intentionally or unintentionally in a manner adverse to them. Consumers with low levels of digital literacy, as well as those with limited access to broadband service, may not be able to fully realize the utility and benefits offered by IoT. Products that are poorly designed, hard to set up and operate, result in consumers limiting their use of IoT or result in poor results. High product costs and subscription fees may preclude consumers who are on fixed incomes, or those that are on the lower end of the socio-economic scale from having these devices.

Table of Abbreviations

(still being significantly updated)

AAM	Advanced Air Mobility
ADPPA	American Data Privacy and Protection Act
AI	Artificial Intelligence
AIS	Automated Indicator Sharing
APEC	Asia-Pacific Economic Cooperation
AQ	Air Quality
ASCE	American Society of Civil Engineers
AASHTO	American Association of State Highway and Transportation Officials
AV	Automated vehicle
BABA	Buy America, Build America
BIL	Bipartisan Infrastructure Law
BIM	Building Information Modeling
BX	
CAGR	
CCPA	California Consumer Privacy Act
CESMII	
CET	Critical and Emerging Technologies
CIA	Confidentiality and Integrity and Assurance
CIO	
CISA	Cybersecurity and Infrastructure Security Agency
CPA	Colorado Privacy Act
CPAP	
CPRA	California Privacy Rights Act
CPS	Cyber-Physical System
CTDPA	
CV	Connected Vehicle
DBOM	Data IDs and Bills of Materials
DCS	
DFAR	Defense Federal Acquisition Regulation
DHHS	Department of Health and Human Services
DL	Deep learning
DoC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation

EERE	
EIA	
EmT	Emerging Technology
EPA	Environmental Protection Agency
ERP	Enterprise resource planning
EV	Electric vehicles
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAR	Federal Acquisition Regulation
FCC	Federal Communications Commission
FDOT	Florida Department of Transportation
FedVTE	Federal Virtual Training Environment
FEM	
FRM	
FTC	Federal Trade Commission
GCTC	Global City Teams Challenge
GDPR	General Data Protection Regulation
GIST	Global Innovation through Science and Technology
GLS	
GSA	General Services Administration
HBOM	
HIPAA	
HVAC	Heating, ventilation and air conditioning
IAM	Identity and Access management
ID	Information and data
IoMT	Internet of Medical Things
IoT	Internet of Things
IoTAB	Internet of Things Advisory Board
IoTFWG	Internet of Things Federal Working Group
IP	Intellectual property
IRA	Inflation Reduction Act
IT	Information technology
ITU	International Telecommunications Union
KEV	Known Exploited Vulnerabilities
KPI	Key performance indicators
LEO	Low-earth orbit
LPWAN	Low Power Wide Area Networks
MBDA	Minority Business Development Agency
MEP	Manufacturing Extension Partnership

Working Draft IoT AB report

ML	Machine learning
MVA	Manufacture value added
NAAQS	
NDAA	
NEMA	National Electrical Manufacturers Association
NESHAP	
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	
NOAA	
NSF	National Science Foundation
NSTC	National Science and Technology Council
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
O&M	
ODM	Original design manufacturers
OEM	Original Equipment Manufacturers
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OSTP	Office of Science and Technology Policy
OT	Operational technology
PANDA	
PbD	Privacy by Design
PCAST	President's Council of Advisors on Science and Technology
PET	Privacy-Enhancing Technologies
PHI	
PID	
PII	Personally identifiable information
PoC	Proof of Concept
PPDSA	Privacy-Preserving Data Sharing and Analytics
PPE	Personal protective equipment
PPP	Public-private partnerships
PQC	Post quantum computing
PV	
QC	Quantum computing

RFID	
RFP	
ROI	
RSR	
SB	Small and disadvantaged businesses
SBA	
SBIR	Small Business Innovation Research
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SCSEP	Smart community and Sustainability Extension Partnerships
SDO	Standards Development Organizations
SENSOR	
SMB	
SME	Small and medium enterprises
SSDF	Secure Software Development Framework
STEM	Science, technology, engineering, and mathematics
STTR	Small Business Technology Transfer
THEA	Tampa Hillsborough Expressway Authority
TMF	Technology Modernization Fund
UAS	
UF	University of Florida
UI	User interfaces
UNECE	
USDA	U.S. Department of Agriculture
USMCA	United States-Mexico-Canada Agreement
USNSS	
UX	
VC	
VOC	