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

May 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, 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

Executive Summary

The United States stands at a critical juncture: the Internet of Things (IoT) is rapidly evolving, presenting a historic opportunity for economic leadership. The US is undergoing a fourth industrial innovation 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 technological innovation to economic benefits across all industries of our nation.

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

In the last decade, industry analysts* have identified that economic investments in IoT haven fallen below their estimated targets due to slow adoption with shortcomings attributed to change management, cost, talent, and cybersecurity. However, recent estimates* indicate the expansion in IoT is still increasing from $56.3B to $370.2B and a survey of industry leaders indicated 27% have been using and 78% plans to use in next two years.

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.

This IoT Advisory Board (IoTAB) set out to understand the landscape of challenges in the advent of this report and position US leadership to seize economic opportunities that benefit the federal government, organizations, 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 address the adoption and growth, 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	• 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	• Startups that drive new technology • Requires new business models / platforms to scale • AI critical to unlocking value of IoT • Insufficient people / skills
Future Landscape	• Business Ecosystem partnerships Needed for solutions • Convergence of AI /IoT
Across Sectors (as identified in the charter)	• Agriculture • Communities and Infrastructure • Transportation • Healthcare • 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, 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.

Achieving US Leadership Through Action

The Approach to Action

The IoT Advisory Board (e.g., IoTAB or the board) developed initial recommendations and refined them with initial feedback from 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 as:

1. Establishing a National IoT Strategy and Leadership
2. Modernizing IoT Infrastructure
3. Establishing Trust in IoT
4. Fostering a IoT-ready Workforce
5. Facilitating Adoption
6. Incentivizing the IoT Economy including a Resilient

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.

A. Establishing a National IoT Strategy and Leadership

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

LEADERSHIP	**Key Recommendation KR1.1:** Establish a strategic national approach for taking full advantage of the opportunity presented by the IoT.
Enabling Recommendations include an emerging technology list, inter-agency coordination, upgrade legacy infrastructure, specify and use IoT technologies in federal projects, fund research and develop technologies, and lead the way in adoption and promotion of IoT in existing operations.	

LEADERSHIP	**Key Recommendation KR1.2:** 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.
Enabling Recommendations include policies, procedures, and funding to accelerate adoption, and a focus on startup organizations.	

LEADERSHIP	**Key Recommendation KR1.3:** Promote international collaboration in IoT adoption across global supply chains to share knowledge, best practices, and resources.
Enabling Recommendations include specific data minimization guidance.	

B. Modernizing IoT Infrastructure

Objective 2: The U.S. should call upon and collaborate with industry to enhance and modernize the infrastructure that enables and supports IoT. Such collaboration should include the provision of clear direction and support for consistent and resilient communications among devices, update of legacy computing and networking systems, improved connectivity and interconnection among technologies.

MODERNIZE	**Key Recommendation KR2.1**: Promote collaborative development across industries to adopt existing industry standards and protocols.
Enabling recommendations include interoperable standards for public safety, data exchange interoperability and standards for the Internet of Medical Things (IoMT), standards for supply chain logistics, and standards for IoT technology in supply chain management.	

MODERNIZE	**Key Recommendation KR2.2**: Establish methods to foster interoperability for IoT technology to the greatest extent possible, through the use of consistent models, protocols, application interfaces, and schemas.
Enabling recommendations include a data taxonomy for exchanging data collected, and a minimum baseline interoperability for technologies.	

MODERNIZE	**Key Recommendation KR2.3:** Expand and improve programs that ensure sufficient availability, reliability and connectivity for IoT in all areas of the country.

Enabling recommendations include spectrum policy, funding of broadband deployment in rural areas, and promote the use of satellite narrowband IoT.

C. Establishing 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.

TRUST	**Key Recommendation KR3.1:** Provide specific and consistent cybersecurity guidance for IoT providers and adopters to ensure secure operations in a whole-of-government approach.
Enabling Recommendations include cyber across supply chain concerns, guidance to IoT product developers, more reliable electric grids, incentivize cyber labeling initiatives for manufacturers, funding for Cyber Trust Mark campaign, international harmonization of IoT cyber programs & requirements cross sector, and promote existing standards and schemes.	

TRUST	**Key Recommendation KR3.2**: Congress should pass comprehensive federal privacy legislation.
Enabling recommendations include IoT in proposed privacy legislation.	

TRUST	**Key Recommendation KR3.3**: The White House and Congress should facilitate/support the development of a Data and Privacy Policy Framework.
Enabling recommendations include promote privacy by design in IoT lifecycle, third party data sharing and device data use, plain language in policies, privacy transparency mechanisms, universal opt-out signals for IoT devices/applications, IoT privacy on automobile stickers, add "location Enabled" notice to IoT devices, promote use of Privacy-Enhancing Technologies in IoT systems, and sanitization standards for government resale of automobiles.	

TRUST	**Key Recommendation KR3.4**: Support trusted IoT architectures and infrastructure that enable supply chain provenance, and traceability of IoT systems starting from chip design and manufacturing.
Enabling recommendations include incentivize stakeholders and speed adoption end-to-end, promote collaborative IoT platforms, digital twins and threads across markets, creation of ecosystems to enable models and revenue, and consistent levels of IoT documentation in digital threads.	

D. Fostering and IoT Ready Workforce

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.

WORKFORCE	**Key Recommendation KR4.1**: Integrate the needs of the future IoT workforce into existing initiatives and programs with industry, academia and state and local government efforts.
Enabling recommendations include aligning and integrating workforce needs to strategy, collaborate, and create the workforce, collaborate and place workforce in areas of opportunity, and making use of student loan forgiveness in exchange for needed skillsets.	

E. Government Support to Facilitate 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.

ADOPTION	**Key Recommendation KR5.1:** Consider new financial models for sustaining and supporting programs when considering IoT project feasibility.
Enabling recommendations include financial for funding models to sustain projects and grants to the underserved communities.	

ADOPTION	**Key Recommendation KR5.2:** Develop a comprehensive Agricultural IoT Strategy.
Enabling recommendations include deployment of a 'farm of future', interoperability of agriculture machines, small farm/ranch adoption of IoT, federal right to repair, legislation to address instability, and provide overarching drone guidance.	

ADOPTION	**Key Recommendation KR5.3:** The government should implement specific actions to further promote IoT adoption through smart communities.
Enabling recommendations include financial for funding models to sustain projects, program and grants to underserved communities, use of smart community infrastructure reference models, build partnerships, facilitate opportunities and equity of benefits for local communities, buildout broadband infrastructure, interoperability of cross sector smart communities, small to medium city adoption of smart communities, and equity in community benefits.	

ADOPTION	**Key Recommendation KR5.4:** Promote IoT adoption that will improve public safety.
Enabling recommendations include emergency stockpiles of IoT devices, privacy and data use policies in federally funded public safety and community projects, IoT adoption considerations in procurement, and a program that enables local communities to purchase IoT systems.	

ADOPTION	**Key Recommendation KR5.5**: Promote IoT adoption in the health care industry.
Enabling recommendations include promoting IoMT as enterprise priority to leadership teams, cyber in IoT in healthcare devices, use and adoption of healthcare of IoT in rural areas, AI in IoT healthcare research and workforce, and HIPAA like protection for users' medical data in IoT devices.	

ADOPTION	**Key Recommendation KR5.6:** Promote IoT adoption that will improve sustainability and environmental monitoring.
Enabling recommendations include support for development of IoT data repositories keeping data open and available, research and development of low-cost air quality sensors, implementation of nationwide IoT based water monitoring infrastructure, and	

promoting the use of IoT technologies to complement wide area situational awareness capabilities for hazards.

ADOPTION	**Key Recommendation KR5.7**: Promote IoT adoption in Smart Transit and Transportation.
Enabling recommendations include policies for smart transport.	

F. Facilitating and 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.

ECONOMY	**Key Recommendation KR6.1:** Monitor and evaluate progress of IoT adoption for supply chain logistics.
Enabling recommendations include financial incentives to encourage businesses and mix of policies incentives and requirements to support sustainable IoT supply chains.	

ECONOMY	**Key Recommendation KR6.2**: Facilitate public-private partnerships (PPPs) focused on IoT adoption to facilitate collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia.
Enabling recommendations include Public Private Partnerships, digital infrastructure incentives, and promote digital threads and marketplaces.	

ECONOMY	**Key Recommendation KR6.3**: The government should actively promote and support the adoption of AI applications to improve decision-making, optimize resource utilization, and enhance productivity.
Enabling recommendations include promoting trusted AI-IoT platforms for sustainability.	

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.

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:

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

a. the identification of any Federal regulations, statutes, grant practices, programs, budgetary or jurisdictional challenges, and other sector-specific policies that are inhibiting, or could inhibit, the development of the Internet of Things;

b. situations in which the use of the Internet of Things is likely to deliver significant and scalable economic and societal benefits to the United States, including benefits from or to:

   i. smart traffic and transit technologies;
   ii. augmented logistics and supply chains;
   iii. sustainable infrastructure;
   iv. precision agriculture;
   v. environmental monitoring;
   vi. public safety; and
   vii. health care;

c. whether adequate spectrum is available to support the growing Internet of Things and what legal or regulatory barriers may exist to providing any spectrum needed in the future;

d. policies, programs, or multi-stakeholder activities that:

   i. promote or are related to the privacy of individuals who use or are affected by the Internet of Things;
   ii. may enhance the security of the Internet of Things, including the security of critical infrastructure;
   iii. may protect users of the Internet of Things; and
   iv. may encourage coordination among Federal agencies with jurisdiction over the Internet of Things;

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

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

f. any international proceeding, international negotiation, or other international matter affecting the Internet of Things to which the United States is or should be a party.

In addition, the charter provides for the following:

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

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?

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 1.

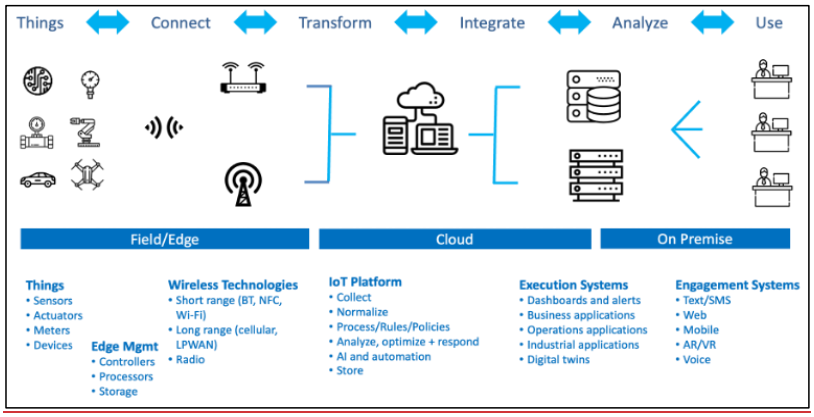


Fig. 1 - High Level Internet of Things Architecture

Specific Applications of IoT

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

IoT in the Industrial Sector

Industrial operations are heavily monitored and controlled in a variety of industries, including energy, mining, chemicals, and transportation. These technologies are also prevalent in manufacturing, monitoring, process control and operations, and supply chain management. Many equipment manufacturers use Industrial Control Systems, (ICS), that are used to control processes like manufacturing, product handling, production, and distribution. ICS includes Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and programmable logic controllers that incorporate IoT technologies. These technologies are often also referred to Operational Technologies (OT). OT is comprised of hardware and software that detects or causes a physical change through the direct monitoring and/or control of industrial equipment.[2] 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.

2 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

Formatted: No bullets or numbering

Formatted: Normal

Formatted: No bullets or numbering

Adoption and improvement of i~~: The data collected by industrial devices incorporated with IoT technologies can be analyzed to gain valuable insights. This data-driven decision-making can lead to innovations, process improvements, and a better understanding of customer needs. It can also simplify regulatory compliance by automatically recording and reporting data required for compliance purposes.~~

Formatted: No bullets or numbering

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

- ~~**Use/Scope**: IoT in industrial devices are used in settings for manufacturing, transportation, energy, and other critical infrastructure.~~
- ~~**Utility:** IoT in industrial devices are used for enhancing productivity, improving efficiency, quality and reducing costs in industrial processes.~~
- ~~**Applications:** IoT in industrial devices are used for industrial applications such as monitoring and control of machinery, inventory management, and supply chain optimization. These operations may be in harsh environments, require low latency and may operate in long time scales before replacement.~~

- **Impact:** Cybersecurity breaches in industrial devices with IoT technologies can cause significant damage to critical infrastructure, including production downtime, supply chain disruptions, and safety risks.

- **Life Support:** Some industrial devices with IoT technologies such as medical devices and aerospace systems may involve human safety, and their cybersecurity vulnerabilities can lead to fatal outcomes.

- **Automation:** Industrial devices with IoT technologies are often automated and may interact with other machines and systems.,

- **Reliability:** Industrial devices with IoT technologies must operate reliably and continuously in harsh environments.

- **Privacy and Confidentiality:** privacy-related information and confidential organizational information including Industrial devices with IoT technologies may collect sensitive data, but the privacy concerns may differ based on the application. The data being transmitted and processed in Industrial IoT environments can be highly sensitive and critical to business operations. This includes manufacturing data, process control information, supply chain data, and proprietary intellectual property. Confidentiality in Industrial IoT extends beyond personal information to safeguard critical industrial processes and trade secrets.

- Considerations for s**Interoperability:** Industrial devices with IoT technologies are often part of larger systems and must be interoperable with other devices and systems, including legacy equipment and other operations technologies.

  Scalabilityealability: Industrial systems with IoT technologies often involve a large number of devices and must be scalable to accommodate growth., whereas consumer systems with IoT technologies may be smaller in scale

- **Attack Surface:** Industrial devices with IoT technologies have a larger attack surface due to their connectivity and may be vulnerable to various types of cyber threats such as hacking, malware, and ransomware.

- **Criticality:** The cybersecurity of industrial devices with IoT technologies is critical for the operation of critical infrastructure.

The advancement of IoT technologies in industrial applications can further amplify the efficiencies of the manufacturing process, allowing for production goals and outcomes to reach levels of scale that are previously unimaginable and physically attainable. And when properly and responsibly governed and applied, these

technologies can achieve these efficiencies while enhancing workers safety and privacy while fostering energy and environmental stewardship.

~~IoT for the Consumer~~

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

Commented [GW1]: Convert this section to a simple Consumer IoT graphic per above

~~Convenience: Tracking tags attached to keys, purses and luggage, help locate and recover lost items no matter where they are. Smart appliances can be monitored and operated remotely, allowing consumers to control them from anywhere and anytime. Smart refrigerators monitor grocery quantities, and create weekly shopping lists.~~

Formatted: Heading 2, No bullets or numbering

~~Safety: Connected baby monitors and security cameras monitor activity to protect people in and around the home. Smart doorbells and smart door locks prevent unauthorized access to homes. Security systems, integrated with cameras, monitors, smart doorbells and locks, are connected with call centers to protect the physical safety of residents.~~

~~Maintenance/Monitoring: Connected devices can report on their own status, such as an air purifier alerting of the need for a filter change. They can monitor conditions; for example, a smart water leak detector senses water flow through pipes and can send an alert for even small water leaks.~~

~~Cost Savings: Smart irrigation controllers can incorporate data about weather conditions and sensor inputs on soil moisture, to optimize the frequency and amount of lawn watering. Connected thermostats monitor and maintain home temperatures while minimizing energy usage.~~

~~**Health: Wearable devices such as fitness trackers and smartwatches encourage users to track their health data and increase their physical activity, often "game-ifying" the experience to promote regular use. Other connected devices such as body scales, blood pressure monitors, and CPAP machines allow consumers to see trends in their data, improve compliance, and optionally report back to the health provider.**~~

~~**Entertainment: Consumers stream a wide selection of video and audio content on their smart TVs and wireless speakers, and connected cameras inside the home can provide hours of entertainment watching and interacting with house pets remotely.**~~

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

~~**Cybersecurity: The number of devices connected to a home network increases the potential cyber-attack surfaces, and as a result, the security of the home router and of all the devices connected to the network becomes a critical link. There are particular concerns around child safety, such as intruders on baby monitors or smart speakers.**~~

~~**Privacy: IoT devices collect sensitive and non-sensitive user data. IoT device cybersecurity vulnerabilities may allow this data to be accessed by cyber-criminals. The collected data may also be used by product manufacturers and other third parties in an undisclosed or unauthorized manner, or in a manner that may lead to adverse outcomes for the consumer.**~~

~~**Usability: Not all consumers are technically or digitally tech-savvy, and many current IoT products are difficult to set up, use, troubleshoot and maintain without technical knowledge. In some cases, the user experience and user interfaces are not intuitive, making the product hard to use and realize benefits from.**~~

Formatted: Heading 2, No bullets or numbering

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

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

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

~~IoT in the Smart Home~~

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

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

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

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

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

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

Formatted: Heading 2, No bullets or numbering

~~**Remote access, control and autonomous operation. The connected nature of IoT technologies allows users to remotely control and operate smart home devices and equipment. For example, a resident can unlock a smart door lock remotely to allow a guest into the home. A resident can turn house lights on and off through a control panel in the home, or remotely through a mobile phone app. Smart home applications can be controlled manually, or autonomously in response to pre-set threshold conditions or intelligent algorithms that learns from specific patterns in data. A smart irrigation system turns off the garden sprinklers when it senses rain or delays operation if soil moisture levels are high. A IoT-enabled HVAC system automatically resets to lower setpoints when it senses no occupants at home.**~~

~~**Optimize home operations through intelligence. The use of data collected from IoT connected devices have made homes more livable, safer, convenient, and economical to maintain. Algorithms analyze the data to optimize the use of home systems. For example, smart HVAC systems can be optimized based on patterns of use, automatically turning on thirty minutes in the morning before first activity and turning off thirty minutes before occupants go to bed, based on historical data. Similarly, a home with a solar panel and battery system optimizes the mix of electricity stored, discharged to the grid, and used by the home users based on past data.**~~

~~Automate functions to increase convenience and simplify tasks. Home automation platforms integrate various systems together, such as lighting, energy management, blinds, audio video, IoT-enabled systems (appliances, thermostats, etc.) and others. This integration enables the various systems to orchestrate and work together. Combining monitoring, control, and optimization capabilities permits home systems to operate autonomously with little human input. For example, smart home algorithms know when occupants return each day, and what rooms they used in the house. Sensors detect the resident's car entering the driveway and initiates an automated sequence to open the garage door, turn on the lights in the areas of the house used by the resident, turn on the HVAC systems, turn on the oven, and turn on the television system to the right channel. As the evening progresses, lights in the sleeping portions of the home are turned on while the common areas are turned down. Select appliances, such as the dishwasher and the laundry appliances activate at midnight when the electricity rates are the lowest.~~

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

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

~~**Privacy. Smart home technologies collect a lot of information that may be private to a resident. For example, the collected data may contain both personally identifiable information (PII) as well non-PII information. While some data collection is unavoidable in order to offer personalized and relevant experiences and outcomes, smart home users are concerned with how that data is used, stored, and secured, as well as who has access to it.**~~

~~**Cybersecurity. Smart home technologies create new vulnerabilities and attack surfaces in the home network. While home networks are smaller and simpler compared to their enterprise network counterparts, they are also less secure. Enterprise networks are well maintained and updated frequently. In contrast, home networks are seldom updated, configured correctly, and maintained. The integration of IoT devices into this network greatly increases cybersecurity risks. Cybercriminals can penetrate these networks through vulnerable IoT devices and gain access to sensitive homeowner information, as well as plant malware into the devices and network. In other cases, cybercriminals can access IoT devices and intercept the data streams, such as a video feed from a camera system.**~~

~~**Subscription Plans. Many smart home technologies are offered as a hardware purchase and a subscription service. For example, one manufacturer sells a smart doorbell and an accompanying subscription service to access stored video. Because IoT and smart home technologies collect a lot of data, storing growing amounts of data over a period of time is expensive. Many manufacturers, especially smaller ones, are unable to "absorb" that cost and must pass it on to the consumer and homeowner. In other cases, smart home technology manufacturers offer "premium" features on a subscription basis. While there may be justification for these subscription costs, buyers are accustomed to paying once and feel that they are "nickel and dimed" by these subscription services.**~~

Formatted: Heading 2, No bullets or numbering

User Experience. Smart home and IoT technologies offer benefits to its buyers, but those benefits may not be equally accessible to all. Complex configuration and setup processes hinder less sophisticated owners and require 3rd party installers. It may lead to improperly configured devices that function poorly. In addition, some devices are poorly designed with little thought for user experience. These poorly designed user interfaces (UI) and experiences (UX) discourage users with limited digital literacy from fully accessing and using the technology to its fullest. For example, smart home technologies that are controlled by voice commands can be challenging. The commands must follow a specified format and not in a "natural language" and have trouble accurately recognizing accents.

Maintenance and Upgrades. Smart home technologies must be maintained and updated frequently to stay current, secure and functional. However, some users are hesitant to do so because in an integrated smart home, software upgrades to one component in a system may "break" the integration with other components in the same system or other systems. Repair of this breakage may require reconfiguring of select components in the system and are beyond the capabilities of most users. These "breaks" are more likely between components from different brands. Not all upgrades are performed "over the air" as some must be done in-person. These "truck rolls" are expensive and may hinder upgrading firmware.

IoT in the Industrial Sector

~~Industrial operations are heavily monitored and controlled in a variety of industries, including energy, mining, chemicals, and transportation. These technologies are also prevalent in manufacturing, monitoring, process control and operations, and supply chain management. Many equipment manufacturers use Industrial Control Systems, (ICS), that are used to control processes like manufacturing, product handling, production, and distribution. ICS includes Supervisory Control and Data Acquisition (SCADA) systems, distributed control systems, and programmable logic controllers that incorporate IoT technologies. These technologies are often also referred to Operational Technologies (OT). OT is comprised of hardware and software that detects or causes a physical change through the direct monitoring and/or control of industrial equipment.3 OT devices are as distinct from 'consumer IoT' due to their usage in commercial operations and are not available or readily available for sale to the public.~~

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

~~Increased efficiency in manufacturing operations. IoT gives manufacturers and industrial operators the ability to automate and optimize their operating equipment efficiency and/or utilization. The use of robotics and automated machinery can boost productivity and help manufacturers streamline productions, reducing unplanned equipment downtime. Using sensors, manufacturers and utilities gain valuable insight into operational performance of pieces of equipment as well as entire systems.~~

Formatted: Heading 2, No bullets or numbering

~~3 Wikipedia https://en.wikipedia.org/wiki/Operational_technology~~

~~Reduction of errors. Through digitalization, manufacturers can reduce operational and manufacturing errors generally associated with manual labor. IoT can help reduce errors in operations, even in those operations that are automated like in continuous manufacturing operations. For example, IoT sensors can detect anomalies and/or variabilities in a chemical processing operation and adjust certain parameters to reduce process waste and increase yields. AI and machine learning can do much of the required computing and data analysis and make subsequent predictive recommendations which can improve a manufacturing process.~~

~~Predictive maintenance. IoT technologies can alleviate issues and unplanned machine downtime associated with reactive maintenance. By monitoring equipment performance consistently, industrial operators are able to identify issues before they occur and allows them to schedule maintenance prior to any downtime.~~

~~Improved safety. A fully functioning manufacturing operation that incorporates sensors and other IoT technologies can use the collected data to bolster worker and product safety. Integrated systems can protect workers by providing alerts which could automatically and safely cease operations if an accident is predicted or until an incident is resolved. Safety can be improved with sensors monitoring hazardous conditions and sending alerts when necessary, such as detecting chemical leaks or equipment malfunctions, reducing the risk of accidents.~~

~~Cost reduction. The data provided to manufacturers through Industrial IoT technologies is giving them the knowledge and tools to reduce costs and increase marginal revenue. By using data-driven insights into operations, production, marketing, and sales manufacturers can steer their business into a more profitable direction.~~

~~Enhanced Productivity & Quality: IoT technologies can improve productivity by providing workers with real-time data and insights. Continuous monitoring of product quality can automatically adjust processes to maintain consistent quality levels.~~

~~Data-Driven Insights, Reporting, Compliance: The data collected by industrial devices incorporated with IoT technologies can be analyzed to gain valuable insights. This data-driven decision-making can lead to innovations, process improvements, and a better understanding of customer needs. It can also simplify regulatory compliance by automatically recording and reporting data required for compliance purposes.~~

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

~~Use/Scope: IoT in industrial devices are used in settings for manufacturing, transportation, energy, and other critical infrastructure.~~

Formatted: Heading 2, No bullets or numbering

~~Utility: IoT in industrial devices are used for enhancing productivity, improving efficiency, quality and reducing costs in industrial processes.~~

~~Applications: IoT in industrial devices are used for industrial applications such as monitoring and control of machinery, inventory management, and supply chain optimization. These operations may be in harsh environments, require low latency and may operate in long time scales before replacement.~~

~~Impact: Cybersecurity breaches in industrial devices with IoT technologies can cause significant damage to critical infrastructure, including production downtime, supply chain disruptions, and safety risks.~~

~~Life Support: Some industrial devices with IoT technologies such as medical devices and aerospace systems may involve human safety, and their cybersecurity vulnerabilities can lead to fatal outcomes.~~

~~Automation: Industrial devices with IoT technologies are often automated and may interact with other machines and systems.,~~

~~Reliability: Industrial devices with IoT technologies must operate reliably and continuously in harsh environments.~~

~~Privacy and Confidentiality: Industrial devices with IoT technologies may collect sensitive data, but the privacy concerns may differ based on the application. The data being transmitted and processed in Industrial IoT environments can be highly sensitive and critical to business operations. This includes manufacturing data, process control information, supply chain data, and proprietary intellectual property. Confidentiality in Industrial IoT extends beyond personal information to safeguard critical industrial processes and trade secrets.~~

~~Interoperability: Industrial devices with IoT technologies are often part of larger systems and must be interoperable with other devices and systems, including legacy equipment and other operations technologies.~~

~~Scalability: Industrial systems with IoT technologies often involve a large number of devices and must be scalable to accommodate growth., whereas consumer systems with IoT technologies may be smaller in scale~~

~~Attack Surface: Industrial devices with IoT technologies have a larger attack surface due to their connectivity and may be vulnerable to various types of cyber threats such as hacking, malware, and ransomware.~~

~~Criticality: The cybersecurity of industrial devices with IoT technologies is critical for the operation of critical infrastructure.~~

~~The advancement of IoT technologies in industrial applications can further amplify the efficiencies of the manufacturing process, allowing for production goals and outcomes to reach levels of scale that are previously unimaginable and physically attainable. And when properly and responsibly governed and applied, these technologies can achieve these efficiencies while enhancing workers safety and privacy while fostering energy and environmental stewardship.~~

What can IoT do?

IoT creates new value

[New graphics in development] 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

INFOGRAPHIC EXAMPLE

Asset Tracking
Problem: Lost or misplaced assets
Solution: Location tags/sensors track movement and location of equipment, machines, vehicles, and other resources and assets
Applications – shipment tracking, high value equipment tracking, etc.

Benefits

- Time savings from searching for equipment and assets
- Route optimization for shipment and supply chain
- Increased resource efficiency and productivity

Remote condition monitoring
Problem: Asset status unknown or unmonitored, leading to its underutilization, unplanned downtimes, and underperformance
Solution: Sensors monitor and inform on conditions of equipment, machines, people, and other resources and assets
Applications – Machine status, patient health, manufacturing operations monitoring
Benefits

- Increased equipment productivity and effectiveness
- Early detection and resolution of issues

- Frees up labor to be redeployed to other tasks

IoT Transforms Business Models

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

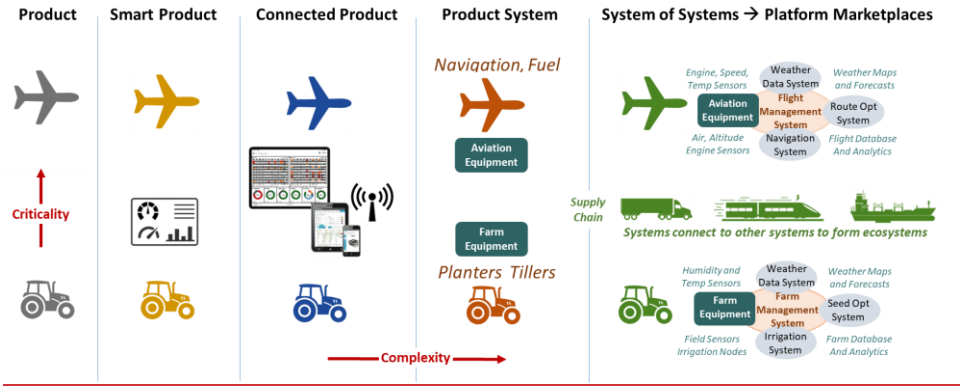
Connectivity creates opportunities for product suppliers to change their mindset about growing their business. Instead of viewing their business as being suppliers of smart-connected products, IoT leaders view their business as **being smart-connected suppliers** to their customers using their products.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

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

[4] Deloitte - https://www.linkedin.com/pulse/unlock-limitless-possibilities-empower-your-customers-rochak-sethi/

IoT Transforms Business Ecosystems

Smart, connected products reshape competition within industries and expand industry boundaries. The basis of competition shifts from discrete products to product systems to systems of systems, to platform ecosystems and marketplaces[5].



The Current State of IoT

Current state of market adoption

The adoption of IoT is growing in the United States. One industry analyst estimated the value of the U.S. IoT market to be $56.3 billion in 2022, growing at 15.6% CAGR and projected to reach $270.2 billion by 2033.[6] Research published in the 2021 Microsoft IoT Signals found that 94% of business decision-makers, IT decision-makers and developers at U.S. enterprise organizations (1000+ employees) surveyed are "IoT adopters"[7], meaning that they are either learning about IoT, conducting a trial or proof of concept, purchasing IoT, or using IoT.[8] Of this, 27% have projects in the "use" phase, while 78% reported that they are planning to use IoT more within 2 years.[9]

However, this growth is below expectations. Adoption of IoT is hindered by a variety of industry-specific challenges. For years industry projected 10's of billions of IoT units in use by ca. 2022. And in 2014 the World Economic Forum and McKinsey & Co. projected that IoT, and adjacent technologies (analytics, cloud computing, big data and ML/AL)

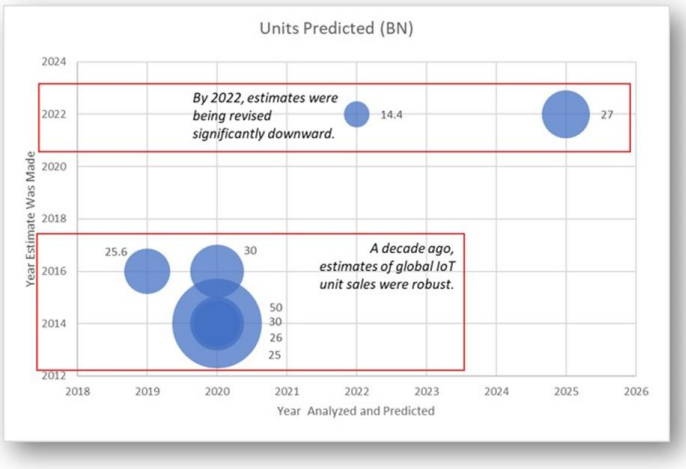
[5] https://hbr.org/2014/11/how-smart-connected-products-are-transforming-competition
[6] "United States IoT Market is expected to surpass revenues worth U.S.$ 270.23 billion by 2032: Persistence Market Research Report," Persistence Market Research Press Release, May 24, 2023. Link
[7] "IoT Signals - Edition 3|October 2021", Microsoft, October 2021. Exhibit 3. Link
[8] Ibid. Exhibit 2.
[9] Ibid. Exhibit 3.

will produce $9.6 to $21.6 trillion of value for the global economy by 2022. And Verizon's State of the Market: Internet of Things 2016 report noted, *"The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019, hitting 30 billion in 2020."* Verizon was by no means an outlier at that time; while numbers varied, most analysts expected this kind of growth over the next few years.

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

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

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



Commented [GU2]: Mike Bergman: This diagram uses some data not cited in the report. If we want to use something like this to show "headwind effect", I can provide the spreadsheet and references.

Commented [GW3R2]: This would be helpful, Mike. Thanks

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

Market Consolidation

There is no "one size fits all" IoT technology. The market is an organically-developing but fragmented ecosystem of sensors, chips and processors, modules, devices and software platforms10. For example, there were 613 IoT software platforms in the market in 2021, down from 620 in 2019, but up from 450 in 2017.[11] The fragmented nature of the market has created confusion for IoT buyers who have struggled with understanding, selecting and integrating hardware and software from a vast array of technology providers to meet their specific requirements.

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

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

10 [1] "IoT platform" is an application or service that provides IoT product suppliers with tools and capabilities that they would otherwise need to develop in-house. Platforms ease development and assist with the product lifecycle after the product is shipped by providing such features as automated software updates or data analytics.

11 "IoT platform companies landscape 2021/2022: Market consolidation has started," P. Wegner, IoT Analytics, November 23, 2021. Link

The IoT platforms landscape is consolidating, as reported by IoT Analytics[12], with a growing trend in forming end-to-end solutions partnerships using these platforms. This approach accelerates IoT technology adoption by offering incentives to partners who utilize these platforms, which benefits their businesses, creates new workforces, and fuels economic growth.

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

Number of IoT Platforms Consolidating

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

Typical IoT Platforms Capabilities

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

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

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

IoT Solutions Partnerships for Specific Use Cases

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

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

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

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

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

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.[13] 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.[14] Still others like data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, QRNG chips, biodegradable sensors, 6G and quantum computing are only just hitting the market or are still in research labs. still "years out" and require continued research investments.[15]

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.

[13] "55+ emerging IoT technologies you should have on your radar (2022 update)," S. Sinha, IoT Analytics, April 6, 2022. Link
[14] ibid.
[15] ibid.

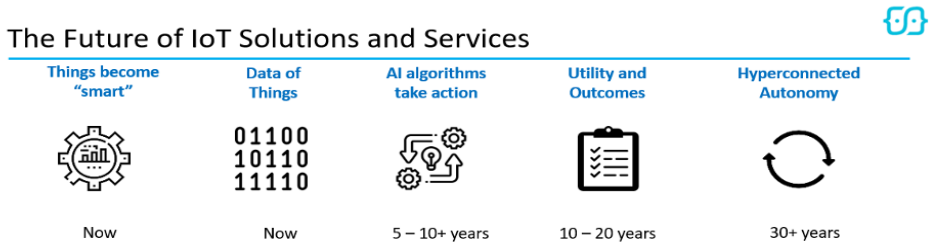


Figure XX. Evolution of IoT.

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, interconnect with other IoT devices to create connected device systems. These systems connect with other systems to create "systems of systems" and platforms to offer "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 is 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

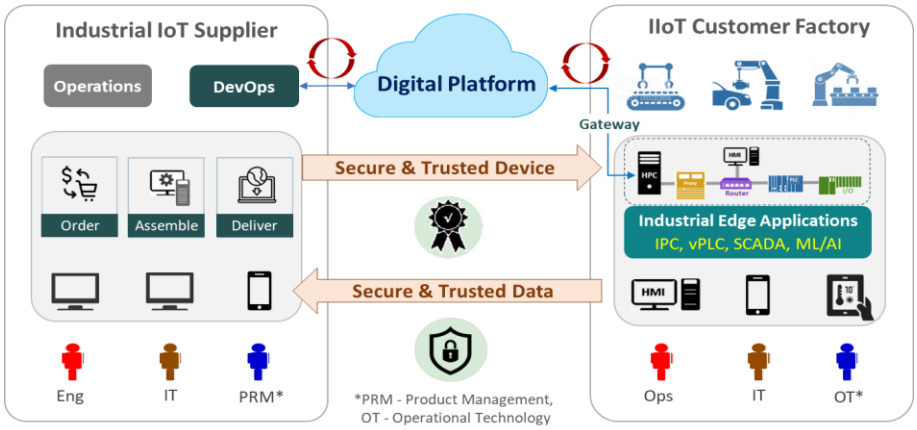
The continuing evolution of IoT facilitates the creation of IoT platform-based industry ecosystems that develop and deliver innovative offerings and outcomes to the economy and civil society.

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."[16] 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 IoT[17] 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. Account representatives review usage patterns and offer advice to optimize machine performance and efficiency. Operations teams predict maintenance needs and schedule downtimes to service the equipment.



[16] https://www.applicoinc.com/blog/what-is-a-platform-business-model/
[17] https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/implementing-a-digital-transformation-at-industrial-companies

This example highlights how suppliers of Industrial IoT products become ***Smart-connected IIoT suppliers*** by digitalizing their operations, updating processes, and 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 optimizeof workflows that lead to enhanced productivity.
- **Trusted data for digital twins** ensure accurates simulations, timely predictive maintenance and better process optimization boosting operational efficiency.
- **Growth of XaaS[18] 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, create value and evolve
- 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 technologies, digital platforms and ecosystems to work together in a structured manner to create solutions

[18] https://www2.deloitte.com/us/en/pages/consulting/solutions/xaas-everything-as-a-service-model.html

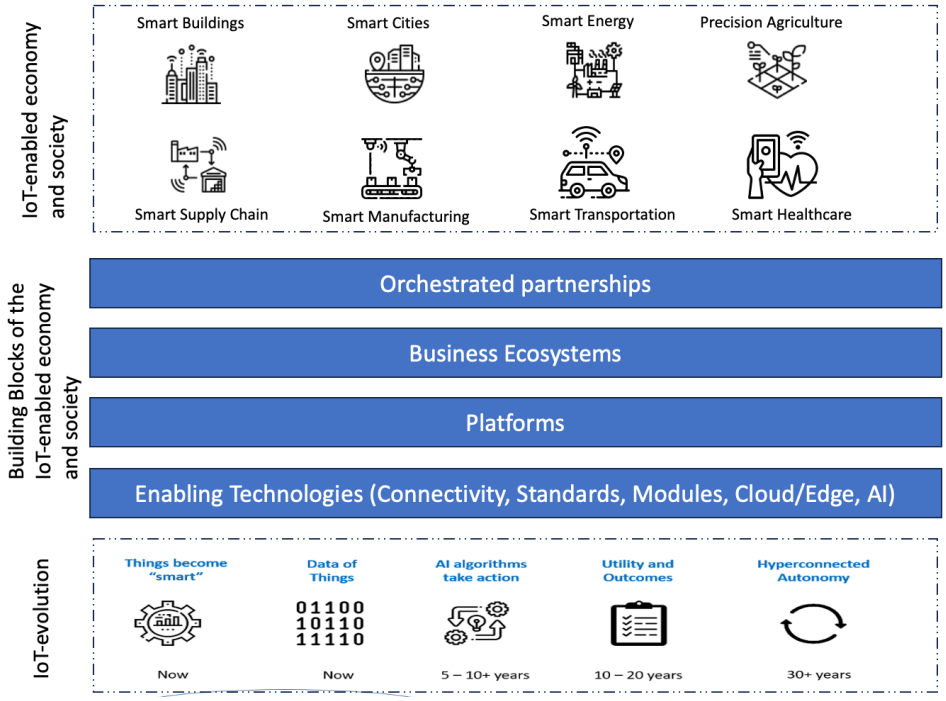
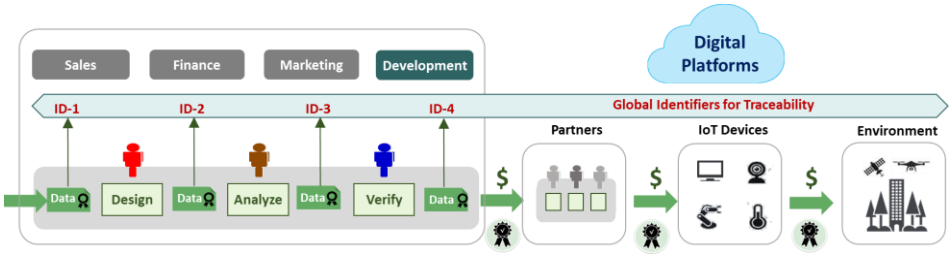


Figure xx1.

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 that 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 digital marketplaces 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 Ecosystems[19]

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. These ecosystems aggregate interconnected platforms, applications, and services that enable multi-stakeholder collaboration, value exchange, and co-innovation. By fostering symbiotic relationships and co-opetition among participants, platform-based business ecosystems drive innovation, monetization, agility, and scalability enable through open architecture, governance, and network effects[20].

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

[19] https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/
[20] https://www.wallstreetprep.com/knowledge/network-effects/

stakeholders, organizations can leverage each other's strengths to develop integrated solutions that seamlessly different part of the IoT ecosystem. Partnerships include:

- **IoT Private-public partnerships** 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 ecosystems[21], 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 architecture[22] to create 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 participants[23], 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) by mitigating individual stakeholder self-interest driven actions that undermine the overall value structure[24].
- 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 SMB's, especially the ones that are domain experts in specific market applications and application

[21] https://www.bcg.com/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition
[22] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/data-ecosystems-made-simple
[23] https://www2.deloitte.com/xe/en/insights/focus/industry-4-0/partner-ecosystem-industry-4-0.html
[24] https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3Dihub

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

- **They facilitate regional development.** Tech hubs[25] 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 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.

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.

[25] https://www.eda.gov/funding/programs/regional-technology-and-innovation-hubs

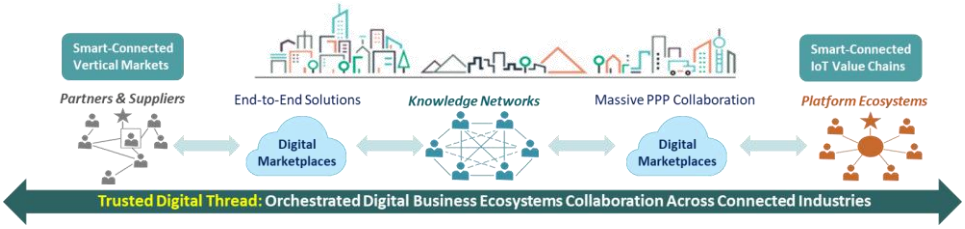
Smart Connected Manufacturing: Factories using sensor data to improve efficiency, automation, and quality.

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



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

IoT technologies. With appropriate orchestration and incentives, the few trillion-dollar giants can multiply the growth of the many SMBs.

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

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

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

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

The convergence of IoT and platform giants leading the development of orchestrated business ecosystems represents an unparalleled opportunity to grow our GDP. Through

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

Findings of the IoT Advisory Board

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

General findings – High Level

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

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

Industry findings – High Level

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

General Findings – Specific Considerations

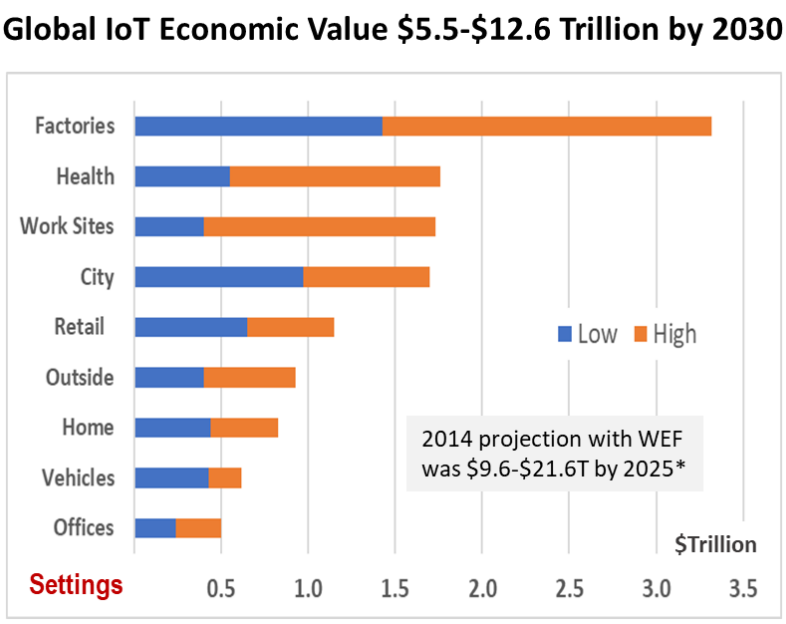
Finding 1: Industry adoption is slower than expected and hindered by a variety of challenges.

Supports Recommendation(s) (Multiple across many themes)~~x.x, x.x~~

In 2014 the World Economic Forum and McKinsey & Co. projected 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 2022[26].

Commented [GW4]: Need to update the graphic to show how much less the resulting adoption was vs projected

In 2021, McKinsey & Co. clarified in a new report[27] that the above projection was off mainly due to The IoT has faced headwinds related to change management, cost, talent, and cybersecurity, and slow market adoption of digitalization and cyber-resilience particularly in enterprises.



[26] www.weforum.org/press/2014/01/increased-cyber-security-can-save-global-economy-trillions/
[27] www.mckinsey.com/capabilities/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it

The 2021 report revised the IoT forecast to $5.5 to $12.6 trillion by 2030 concentrated in certain settings as shown above. For each setting, it provided a min-max range for projections factoring **adoption rates**, **impact**, and **scale**. Each setting was analyzed for tailwinds and headwinds, opportunities and risks and the settings were ranked based on size and growth rates as shown in the chart above. The convergence of physical and digital worlds was cited as a fundamental trend underlying the digital transformation of businesses that can fuel the global economy.

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

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

- **Complexity and Integration.** IoT is a set of disparate technologies offered by a fragmented ecosystem of hardware suppliers, software platforms and connectivity service providers. It is not a “one size fits all” and components must be assembled together to create a solution that meets the specific requirements. In addition, IoT implementations often require integration with existing systems and infrastructure. Integrating IoT devices and platforms with legacy systems is a significant barrier, costly, and requires technical skills that is in short supply, especially for industries with established processes.

- **Cybersecurity Concerns.** IoT introduces a vast number of potential attack surfaces, leading to very real concerns that hinder adoption. Many industries, particularly those dealing with sensitive data or critical infrastructure, are cautious about the potential vulnerabilities associated with IoT devices. Significant progress has been made in IoT security but many manufacturers have not yet moved to secure by design/ secure by default cultures. Policies must focus on ensuring adoption of best practices and ensuring regular updates to IoT devices.

- Cyberattacks may disrupt the operation of IoT devices and services, or lead to a breach of back office and enterprise systems that the IoT devices connect to.

- **Interoperability.** The inability for devices to communicate with each other or to the broader enterprise, legacy systems and operations technology systems, is a major barrier. In some cases, the lack of interoperability is caused by a lack of standards and protocols. In other cases, there are multiple competing standards as each solution provider creates “walled gardens” or “walled ecosystems”. One major challenge is the integration of IoT devices with legacy and operations technology systems, which are commonly found in many industrial and enterprise environments.

- **Data Privacy and Compliance.** Concerns related to data privacy and regulatory compliance are significant barriers to IoT adoption. Industries must navigate complex legal frameworks and ensure that IoT implementations comply with data protection regulations, which can slow down the adoption process. While privacy concerns cut across multiple markets and industries, certain markets are more sensitive to privacy issues, including smart communities, retail, insurance and healthcare.

- **High Implementation Costs.** The upfront costs associated with implementing IoT solutions, including the purchase of devices, infrastructure, and integration expenses, can be a deterrent for many potential adopters, especially for those operating on tight budgets. It is estimated that the cost of the IoT solution represents 30% of the total cost, while implementation and deployment accounts for the other 70%.

- **Lack of Skilled Workforce.** Implementing and managing IoT technologies require a skilled workforce with expertise in wide variety of areas such as cybersecurity, data analytics, application development, cloud operations, and system integration. The shortage of professionals with these skills hinder adoption, particularly in industries that have not traditionally require digital talent. In addition, the ongoing labor shortage contributes to the struggle to attract and retain such talent.

- **Uncertain ROI and Business Value.** Some industries are more hesitant to adopt IoT technologies due to uncertainty about the return on investment (ROI) and the overall business value. This is particular true for industries, such as mining, construction and agriculture, that have not traditionally incorporated digital technologies into its operations. There is a lack of clear use cases and success stories demonstrating tangible benefits are essential for convincing businesses to invest in IoT.

- **Resistance to Change.** Resistance to change within organizations is a common challenge. Many potential adopters have limited awareness and

education of IoT, and what it can do. Employees and management may be accustomed to traditional processes and may resist adopting new technologies. Complexity, industry regulations and structure, and organization culture are additional barriers hindering the adoption of IoT.

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

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

Supports Recommendation(s) KR1.1, KR1.3, KR2.2, KR3.1, KR3.3, KR3.4, KR5.2, KR5.3, KR5.4, KR5.5, KR5.6, KR5.7

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 harm. 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:

1. Technical Challenges:

- Infrastructure limitations and compatibility issues
- Data security and privacy concerns
- Scalability and interoperability problems
- Limited battery life and connectivity range

2. Regulatory Framework:

- Lack of clear regulations and standards
- Complex compliance requirements
- Data privacy laws and cybersecurity regulations
- Limited understanding of the potential risks and benefits

3. Business Model Challenges:

- Difficulty in monetizing IoT data
- High initial investment costs
- Integration with existing business processes and workflows
- Lack of understanding of the value proposition

4. Infrastructure and Connectivity:

- Limited connectivity infrastructure in rural and underserved areas
- High costs of connectivity and data plans
- Infrastructure vulnerability to outages and security threats

5. Security and Privacy Concerns:

- Data breaches and security vulnerabilities
- Privacy concerns related to data collection and use
- Concerns about the potential for job displacement

6. Organizational Challenges:

- Lack of awareness and understanding of IoT technology
- Resistance to change and organizational adaptation
- Limited IT resources and expertise
- Lack of clear governance and accountability

7. Social and Cultural Factors:

Commented [GW5]: This is a very long bulleted list with a lot of good information; should we try to condense it or is the plethora of information worth the page count?

- Public skepticism and privacy concerns
- Cultural and societal resistance to technological change
- Lack of understanding of the potential benefits

8. Economic Factors:

- High initial investment costs
- Ongoing maintenance and operational expenses
- Return on investment (ROI) uncertainty

9. Lack of Collaboration:

- Limited collaboration between stakeholders
- Difficulty in coordinating efforts across organizations
- Lack of open-source software and hardware

10. Ethical Considerations:

- Concerns about the use of IoT technology in sensitive industries
- Potential for job displacement and societal disruption
- Ethical implications of data collection and surveillance

Finding 3: The adoption and operation of innovative IoT applications are hindered by various existing policies and regulations at local, state and federal levels.

Supports Recommendation(s) KR1.1, KR1.3, KR2.2, KR3.1, KR5.1, KR5.2, KR5.4, KR5.5, KR5.6, KR6.3~~x.x, x.x~~

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 ~~is moving and changing fast, and~~rapidly and is often used in ways that have never been ~~used or studied before~~well studied. ~~These w~~Well intended policies may conflict with one another, resulting in barriers to adoption, use, compliance and commerce of IoT. Government policies and regulations play a critical role in advancing or stifling the use, the beneficial outcomes and the scaling and evolution of IoT.

Examples of policies affecting the use of IoT include:

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

- Autonomous drones can perform ~~a variety of~~ labor-saving tasks on large farms, including monitoring plant health and crop spraying. However, FAA regulations require one operator per drone, and it must be operated within line of sight. This limits the utility and value that can be obtained from the use of drones in agriculture.

- Telematics devices generate ~~a lot of~~ information about a car and driver's behaviors. This information can be used by automobile insurance companies to create personalized insurance products and set premiums. Insurance is regulated at a state level, and each state determines what information ~~can~~ may be used. For example, California only allows insurance companies to use mileage data.

Finding 4: Equity in access, opportunities, benefits and outcomes is necessary for the sustainable integration of IoT into all aspects of the national economy and civil society.

Supports Recommendation(s) KR1.1, KR2.3, KR4.1, KR5.1, KR5.4, KR5.5~~, x.x, x.x~~

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

builders, developers and operators of IoT products and services should take equity in consideration to create offerings that are relevant, effective, and sustainable.

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

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

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

Equitable outcomes from data. IoT devices collect vast amounts of private and non-private data to make decisions, drive actions and create outcomes. However, the use of this data may lead to negative outcomes intentionally or unintentionally. For example, the use of facial recognition on people of color has been found to have a higher probability of error and lead to inaccurate results. Because of this, people of

color have been negatively impacted at higher rates than other demographic groups. Similarly, vehicle telematics data can be used by insurance companies to determine risk and set personalized premiums. However, while this leads to good drivers receiving lower premiums, bad drivers may be relegated to a class of "uninsurables" who are unable to get insurance at any premium. In the past, these drivers would have been placed into a larger risk pool, where their higher risks may be offset by others with a lower risk. Equity considerations and protections must be incorporated in using data to create beneficial outcomes for the economy and society.

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

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

Equitable access to workforce development and employment opportunities. The integration of IoT into the economy and society creates new types of jobs and employment opportunities. Some of these jobs will require new skills, while others may be extensions to existing skills. For example, some IoT jobs will require digital skills, such as integration, programming, cloud application development, cybersecurity and data science. At the same time, other jobs will be needed to manufacture, install, service and maintain IoT devices and IoT-enabled equipment.

These employment opportunities are at risk of bypassing socioeconomically challenged and rural communities, whose residents may not have the language proficiency, digital literacy, access to education and development opportunities, and broadband service, to be included. Labor shortages exist in many industries today and hinders the American economy. Similarly, the inequitable access to employment opportunities created by IoT will hinder the country's full realization of the economic and societal benefits.

Finding 5: Small businesses can reap significant benefits from IoT, but significant barriers hinder adoption.

Supports Recommendation(s) KR2.3, KR3.1, KR4.1, KR5.1, KR5.4, KR5.7, KR6.2~~x.x, x.x~~

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

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

- **Financial.** The initial cost associated with purchasing and implementing IoT solutions may be beyond the means of small businesses. These businesses have limited financial resources, and many have cash flow constraints, hindering their ability to invest in IoT, hire skilled resources or contracting with service providers.
- **Skills and Expertise.** Integrating IoT technologies into existing business processes can be complex. Small businesses lack personnel with the expertise to successfully deploy and manage the integration. They face challenges in finding and retaining these employees. Training existing staff or hiring skilled workers can be difficult due to budget constraints and market competition for the same talent.

- **Infrastructure.** Small businesses often lack the infrastructure to support the integration, operation and scaling of IoT. Existing infrastructure may need to be modernized. Networks may require upgrading to ensure consistent and stable connectivity for their IoT implementations. Software applications may be upgraded to integrate data from IoT sensors. Some businesses employ legacy systems, adding further complexity to integrate with IoT solutions.

- **Cybersecurity and privacy concerns.** Cybersecurity breaches are extremely disruptive to small businesses, who often lack the resources and expertise to implement and keep up with robust security measures, and mitigate the impacts of cyber-attacks. The collection of data from sensors adds further complexity. Small businesses are concerned on how their proprietary data is used and shared, as it is their source of competitive advantage. They also lack the expertise, knowledge and tools to navigate complex regulations and ensure compliance with data protection laws on customer data collected from IoT.

- **Limited Awareness.** Many small businesses have very limited to no awareness and understanding about IoT solutions. These businesses have limited time and budget for exploring and staying updated on the latest technologies. Small businesses have limited exposure to industry conferences, trade shows, or forums where IoT trends are discussed. Many IoT solution providers focus their marketing efforts on larger enterprises, leaving small businesses unaware of available solutions that could benefit them. Small businesses may have difficulty finding relevant case studies or success stories that demonstrate the practical benefits of IoT in their specific context.

- **Adoption resistance.** Small businesses, especially those in survival or growth phases, prioritize immediate operational needs over exploring new technologies. IoT may be perceived as complex and technical, especially by individuals who are not well-versed in IT. Small business owners and decision-makers may feel overwhelmed by the technicalities associated with IoT, leading to a hesitancy to explore further. Small business owners may be unfamiliar with the potential advantages of IoT technologies and may hesitate to invest without a clear understanding of the return on investment. Misperceptions about the cost of adopting IoT technologies discourage exploration and investment in IoT solutions.

Finding 6: Small companies and startups are instrumental in developing many innovative and disruptive technology solutions and services but face a variety of barriers in getting adoption.

Supports Recommendation(s) KR1.1, KR3.1, KR5.2, KR6.1, KR6.2~~x.x, x.x~~

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

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

- **Customer procurement processes are not designed to purchase innovative offerings.** Existing government and enterprise procurement processes and policies are designed for sourcing established and mature products from established companies. These processes are not well-suited to buy "risky" offerings from start-ups with limited to no proof of performance, limited operating history, and innovative commercial models. Some larger companies address this by offering deep discounts or free proof of concepts to alleviate risk concerns, but small companies do not have the luxury to do so.

- **Legacy regulations and standards.** Certain industries, such as energy, healthcare and transportation, are subject to regulations and standards that were established for legacy systems and operations. The capabilities offered by IoT and other disruptive emerging technologies may deliver the desired outcomes in innovative ways, but may do it in ways that conflict with these existing industry standards and regulations. For example, drones are subject to FAA regulations specifying one drone, one operator. In addition, drones must operate within the line of sight of the operator. This prevents the development and operation of autonomous drones in farming, where drones could be used to collect imagery information of plant health, or conduct crop spraying.

- **Market incumbents.** Many start-ups offer technologies and solutions that disrupt and compete against existing incumbent legacy solutions. Incumbents are well established, and hinder market adoption of innovative solutions in a variety of ways. This includes limiting access to infrastructure and systems and creating "walled garden" ecosystems. For example, one equipment manufacturer "maliciously complies" with an industry standard for

communications, but encrypts the data traffic going through it, which effectively blocks access to the data by other machines.

- **Low market awareness.** At this early stage, there is very limited market awareness of innovative IoT technologies and solutions. Start-ups often invest considerable resources and time to establish credibility and educate their target market about the technology, approach, benefits and value proposition of their innovative solutions. In addition, many start-ups lack the market credibility compared to larger and more established companies. Government adoption and use of innovative IoT solutions helps start-ups establish credibility, and more importantly, credibility of IoT.

Finding 7: IoT enables new innovative business models which requires new business and technology platforms and ecosystems to support and scale it.

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

Finding 8: Interoperability is a key challenge for IoT across multiple industries.

Supports Recommendation(s) KR1.3, KR3.3, KR5.2, KR5.3~~x.x, x.x~~

Interoperability allows heterogeneous devices and systems to integrate, communicate and share information with each other and automate. For example, information collected from one IoT device is used as input data by another different device, or devices from different brands may communicate and work together in a system. While interoperability is enabled by standards, it is challenging to achieve for a variety of reasons. In some areas, IoT technology is still new and rapidly evolving. There are many areas of IoT technology to be standardized and attaining agreement on a standard takes time. While open standards provide the potential for seamless interoperability, the current market is filled with products with proprietary standards, "walled garden"[28] device ecosystems and differing international standards and protocols. Some vendors believe their proprietary standard is technologically superior, some were first to market before standards developed, while others are concerned with commoditization of their offerings. For IoT to evolve, interoperability and

[28] 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.

standards across devices, industries and countries are critical. (source: NIST IoT report draft)

Finding 9: A variety of connectivity challenges is hindering IoT adoption, operation and scaling.

Supports Recommendation(s) KR2.3, KR5.2, KR5.5~~xx, x.x~~

The availability of connectivity service coverage is a necessary prerequisite for IoT adoption and operation. The COVID-19 pandemic highlighted the impact of the digital divide and the need for connected communities. Several government and private sector initiatives offer the potential to make connectivity ubiquitous. For example, a portion of the $65 billion in the federal Bipartisan Infrastructure Law will build infrastructure in underserved areas. California is building a $6 billion middle mile fiber network to facilitate the creation of last mile services to underserved areas.[29] The FCC is considering the potential use of the frequencies in the TV white space for connecting IoT devices over wide expanses of rural areas. Several satellite operators are planning or have launched next generation Low Earth Orbit (LEO) broadband and IoT connectivity services to rural and underserved areas. These initiatives are supplemented by private enterprises establishing LTE and 5G private networks to connect campuses, factories and other facilities augment commercial telecommunications services. (source: NIST IoT research report draft)

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

- **Lack of fixed and wireless connectivity infrastructure.** While urban areas have the infrastructure to offer different connectivity service options, rural areas and remote regions lack the same. This may be manifested in the lack of fiber infrastructure, as well as a lack of sufficient wireless infrastructure. Limited infrastructure, low population and population densities, terrain challenges and poor economic returns limit industry connectivity investments in these areas.

- **Future use cases require higher bandwidth symmetric services.** Future IoT use cases, such as drone and remote machinery operation applications in agriculture, require higher bandwidth symmetric connectivity services. The FCC's current 25/3 broadband service level definition is insufficient to support those applications.

[29] State of California Middle-Mile Broadband Initiative,

- **Insufficient spectrum to support future needs of IoT at scale.** As the number of devices and IoT-enabled services continue to grow, additional wireless spectrum is needed to minimize performance issues. These issues include interference, latency, quality of service and reliability. IoT devices supporting first responder and medical applications, are especially vulnerable. Urban and metropolitan centers, having a large number of building structures, high wireless device density, are most susceptible to disruptions and issues.

- **Sunsetting of connectivity technologies.** There are millions of IoT devices that are connected through 2G and 3G networks in the United States. As 4G and 5G networks enter into service, these older networks are turned off or "sunsetted" over a period of time. For example, the various carriers started turning off their 2G networks between 2017 (AT&T) to 2022 (T-Mobile). Similarly, carriers turned off their 3G networks between 2021 and 2022. In many cases, it is not possible on a practical basis to replace and update the transmitters in the devices to newer protocols, rendering the devices useless. Managing the sunset and replacement of the devices is a major task and cost burden for IoT users and owners.

Finding 10: A lack of trust in IoT is a major barrier to widescale adoption.

Supports Recommendation(s) KR2.1, KR3.1, KR3.2, KR3.3, KR3.4, KR5.4, KR5.5~~x.x, x.x~~

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

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

Finding 11: Artificial Intelligence (AI) is critical to unlocking and accelerating the value of IoT.

Supports Recommendation(s) KR1.1, KR2.3, KR5.5, KR5.6, KR6.3~~xx, x.x~~

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

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

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

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

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

the physical environment and the day-to-day interactions with humans. (source: NIST research report).

Artificial Intelligence (AI) Considerations

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

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

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

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

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

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

- **Digital Twins:** A digital twin is a digital representation providing the elements and the dynamics of how a device or ecosystem operates and lives throughout its lifecycle. Digital twins combine sensor data with ML and software analytics, which are then used to create spatial graphs that provide a digital simulation model that is updated and changes in real time in tandem with their physical counterparts.
- **Energy Management:** Within manufacturing, the consumption of energy remains a primary cost and concern for plant managers and the key decision makers of the company. While the cost of energy may be variable a company's energy use is fully within its control. However, in order to better assess and control energy consumption within a manufacturing environment, machines must be equipped with sensor technology. Energy usage must be tracked at a granular level in order to assess key ratios, such as energy consumption versus productivity. The use of AI can make this tedious and data-intensive process much more efficient and effective.
- **Medical Image Analysis:** Analyzing images is a strong application for DL and CV within the realm of patient data processing. DL is now being applied to automate the analysis and increase the accuracy, precision, and understanding of images down to the pixel. Some of the more common applications include 3D CV (images analyzed and rendered into detailed 3D models), auto grading of eye diseases, and detection and segmentation of radiology images.
- **Safety Enhancement in Buildings:** Employers have an incentive to ensure better compliance with safety standards and protocols. One example of how DL is being used to help ensure better compliance includes tools that allow

employers to leverage photos and videos to identify workers who are missing hard hats, gloves, or other safety equipment.

- **Street Lighting:** Street lighting is an essential element for any city. In addition to providing better visibility for pedestrians and motorists, it adds a feeling of safety and security and can often deter criminal activity. Smart communities are adding AI capabilities to street lighting, which is designed to not only provide lighting, but also perform other tasks by incorporating CV, ML, and IoT connectivity. Streetlights can be equipped with an array of sensors to monitor traffic flow, as well as send signals to traffic lights and other traffic control devices.

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

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

Generative AI

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

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

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

Finding 12: There is an insufficient number of people in the current workforce with the technical, digital and analytic skills required to develop, integrate and deploy, operate and maintain IoT devices and IoT-enabled systems and applications.

Supports Recommendation(s) KR1.1, KR1.2, KR1.3, KR2.1, KR3.1, KR4.1, KR5.5

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

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

- **IoT requires different skills.** Despite its connected nature, IoT is not IT. IoT is a disparate set of technologies requiring an interdisciplinary combination of existing and new technical, digital and analytic skills. The workforce must develop expertise in working with new connectivity technologies, such as LoRaWAN and 4G/5G, integration of IoT devices into internal and external networks, and the cloud. In addition, the workforce must develop skills in working with the cloud, and application development. Finally, the amount of data collected required data professionals to manage the data and analyze it to create optimal outcomes.

- **Non-digital industries and systems go digital.** Many pre-digital industries required limited technical and digital skills. For example, the installation and

integration of HVAC systems into a building requires mechanical, electrical and ventilation expertise. However, smart HVAC systems incorporating IoT and other technologies now require technicians with networking skills to integrate them into the building's IT network, and systems integration skills to interoperate with building and energy automation systems. Furthermore, smart HVAC systems collect vast amounts of data that must be studied by analytics-savvy operators to optimize occupant comfort and system performance, minimize operating costs and plan maintenance activities.

- **The convergence of IT, OT and IoT systems.** Industries such as manufacturing, energy and transportation employ operations technologies (OT), including supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLC), to monitor and control physical processes. On the other hand, business operations are supported by Information Technologies (IT) systems that process data and communications. In these industries, IT and OT systems operate independently of each other and are maintained by separate organizations. The incorporation of IoT into industrial processes require OT and IT systems to come together. This convergence requires a workforce with a specific set of digital skills, including understanding of IT and OT protocols and processes, cybersecurity, systems integration, cloud computing, programming and application development, IoT integration, data analytics.

- **The value of data analytics.** IoT collects vast amounts of data that can be used to create beneficial and innovative outcomes. Unlocking that value requires a variety of skills, including data management and governance, analysis, and development of insights. In addition, there is a need for the development of algorithms and the application of machine learning and AI tools. While the value of data analytics is understood, there is a current shortage of data savvy practitioners, analysts and scientists across all industries.

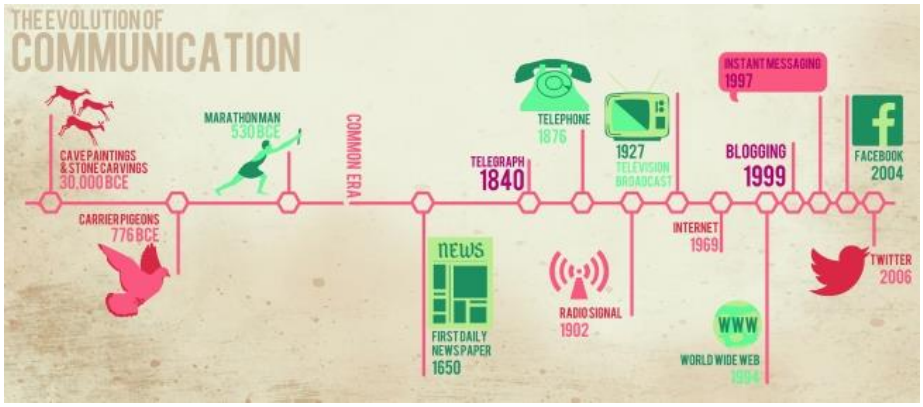
- **Interdisciplinary collaboration.** IoT involves the convergence of various disciplines, including information technology, data science, hardware development, and cybersecurity. Building an IoT-ready workforce requires individuals with interdisciplinary knowledge who can understand the complexities of both hardware and software components. Integrating these diverse skill sets within a single workforce can be a considerable challenge.

Finding 13: Many barriers to IoT adoption due to legacy infrastructure, security, and interoperability require multi-stakeholder platform-based business ecosystem partnerships that align business incentives on high value end-to-end solutions.

Commented [GW6]: Legacy infrastructure may hinder adoption - speak to the issue rather than the solution

Supports Recommendation(s) ~~x.x, x.x~~KR1.1, KR1.2, KR1.3, KR2.1, KR2.2, KR2.3, KR3.1, KR3.4, KR5.2, KR5.3, KR5.5, KR5.6, KR6.1, KR6.2

Communication has been transformative for markets and illustrates the potential of connectivity. From carrier pigeons to marathon sprint, to paper, to newspaper, to telegraph, to telephone, to radio, to television, communication have been transformative and drove major market shifts[30].



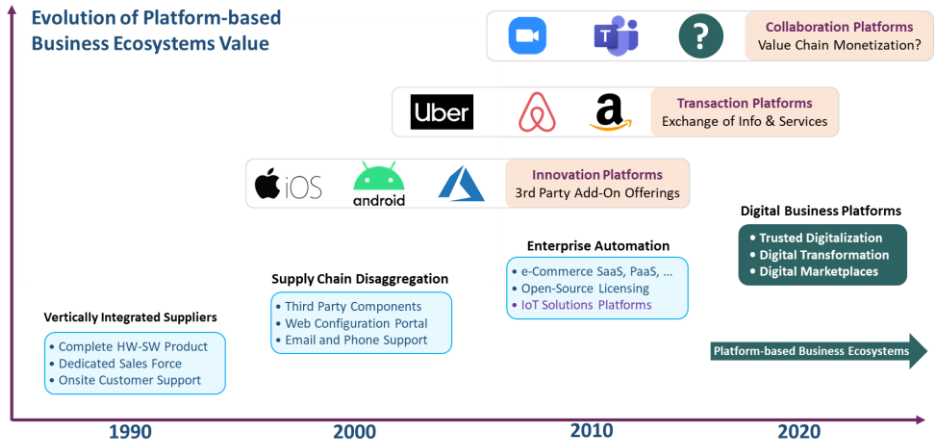
Internet connectivity has been even more disruptive. It began with ARPANET followed by the world wide web, commercializing Internet, instant messaging, etc. Facebook and Twitter leveraged connectivity to develop scalable social platforms and reach huge valuations rapidly. However, unlike social platforms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

Foundational platforms accelerate evolution of technology ecosystems. History shows that innovative businesses can't evolve in a vacuum. They must attract resources of all sorts, drawing in capital, partners, suppliers, and customers to accelerate growth through cooperative networks and ecologies of competition[31].

[30] https://sci10sectionm.wordpress.com/2013/12/08/the-evolution-of-communication-effects-on-the-world-of-science/
[31] https://hbr.org/1993/05/predators-and-prey-a-new-ecology-of-competition

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

Partnerships driven by connectivity gave rise to internet business platforms. Since the 90s disruptions, go market strategies, business platforms and revenue models advanced along with new generations of technologies on top of legacy infrastructure. In the new age of ecosystem partnerships[32] 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 effects[33]. Architecture platforms like Apple iOS and Android enable third parties to add apps to smart phones. Transaction Platforms like Airbnb and Uber enable supply-demand matchmaking for the exchange of goods, or services. Future Hybrid Platforms[34] combine the advantages of both. Collaborative platforms like MS teams and Zoom which grew rapidly during Covid-19, facilitate innovation, but not business orchestration.

Multi-stakeholder collaborative business platforms failures offer lessons for strategy. The IBM-Maersk TradeLens blockchain platform was taken out of the market[35] because it was not open and failed to gain stakeholder support in the

[32] https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/ecosystem-partnering
[33] https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/
[34] https://sloanreview.mit.edu/article/the-future-of-platforms/
[35] https://www.theregister.com/2022/11/30/ibm_and_maersk_tradelens_shutdown/

maritime supply chain. Collaborative platforms and ecosystems emerge as new organizational forms that provide distinct ways to cope with market failures (e.g. fragmented supply chain) or organizational failures (e.g. silos). Distributional and functional failures arise from self-interested actions by members, undermining the overall value structure[36]. Recognizing these failures is crucial for designing effective collaborative multi-stakeholder platforms across the IoT value chain, as they can inform strategies to prevent or mitigate failures, create value, and accelerate adoption.

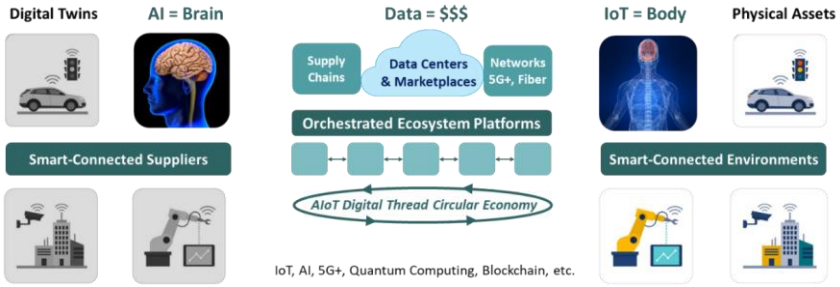
IoT creates opportunities for digital collaboration of orchestrated business ecosystems. As noted before, IoT provides the potential to transform linear supply chains and silos workflows to dynamic value chains and workflows. Transformative IoT platforms enable scalable business ecosystems[37] where enterprises collaborate to provide coherent end-to-end solutions that benefit all stakeholders. Platform-based business ecosystems based on Digital Orchestration, Governance and Network Effects will fuel Digital Marketplaces to drive economic growth.

Finding 14: Convergence of AI and IoT plus adjacent technologies and platforms serving circular supply chain ecosystems will accelerate sustainability and drive disruptive growth fueled by massive data centers in a hyperconnected planet.

Supports Recommendation(s): TBD ~~x.x, x.x~~

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 barriers[38].

[36] https://www.sciencedirect.com/science/article/pii/S0048733323001907?via%3Dihub
[37] https://sloanreview.mit.edu/article/how-healthy-is-your-business-ecosystem/
[38] https://hbr.org/2023/06/how-ai-will-accelerate-the-circular-economy



IoT is the body and AI is the brain, supply chains & networks are the arteries where data flows. Orchestrated AI + IoT (AIoT) platforms linking smart-connected suppliers with smart-connected environments powered by massive data centers will create digital marketplaces and sustainable ecosystems, which will surpass human intelligence in a few decades. AIoT and data are intricately interconnected in a circular, rapidly evolving technological landscape[39]:

1. **Data and IoT:** IoT devices generate vast amounts of data through sensors and connected devices, including temperature readings, location information, and user interactions. This data can be stored and analyzed to gain insights and make informed decisions, such as optimizing energy usage or monitoring machinery health.

2. **Data and AI:** AI relies heavily on data with machine learning algorithms requiring extensive datasets for training. Once trained, AI models can analyze and interpret data for tasks like natural language processing and predictive analytics, extracting valuable insights and patterns that may be too complex for manual analysis.

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

The convergence of IoT and AI will drive high value solutions across industries. Data is the new raw material or the "new oil" for AI, which, in turn, can be applied to analyze and extract valuable insights from the data generated by IoT devices. This synergy between data, AI, and IoT coupled with quantum computing powered by

[39] https://www.linkedin.com/pulse/transformative-power-data-ai-iot-shaping-worlds-future-jha/

massive data centers will drive advancements across various industries, including healthcare, manufacturing, transportation, and smart cities.

- **Smart Cities:** Implement AI-powered analytics on IoT sensor data to optimize traffic flow, waste management, energy usage, and public safety in urban environments.
- **Predictive Maintenance:** Use AI algorithms to analyze IoT data from industrial machinery and equipment to predict maintenance needs, reducing downtime and improving operational efficiency.
- **Healthcare Monitoring:** Combine IoT wearables with AI-powered analytics to monitor patients' health data in real-time, enabling early detection of health issues and timely medical interventions.
- **Supply Chain Optimization:** Employ IoT sensors to track goods in transit and use AI to predict potential disruptions, enhancing supply chain visibility and reducing inefficiencies.
- **Precision Agriculture:** Utilize IoT devices to gather data on soil moisture, weather conditions, and crop health, then apply AI algorithms to optimize irrigation, planting, and harvesting. Utilize sensors and analytics to measure spoilage in storage and distribution.
- **Energy Management:** Integrate AI algorithms with IoT-connected devices to optimize energy consumption in buildings, adjusting lighting, heating, and cooling based on occupancy patterns.
- **Connected Vehicles:** Use IoT sensors in vehicles to collect data on driving behavior and road conditions, then apply AI to improve road safety, traffic management, and vehicle diagnostics.
- **Environmental Monitoring:** Deploy IoT devices to collect environmental data (air quality, water levels, etc.), and employ AI to identify trends and potential hazards.
- **Smart Homes:** Integrate IoT devices like smart thermostats, cameras, and appliances with AI to create intelligent and automated home management systems.

- **Wearable Health Tech:** Combine IoT wearables with AI-driven analytics to provide personalized health recommendations based on continuous monitoring of vital signs.
- **Industrial Automation:** Use AI to analyze data from IoT sensors in manufacturing processes, optimizing production, quality control, and resource utilization.
- **Natural Disaster Management:** Combine IoT sensor networks with AI algorithms to predict and manage natural disasters, such as flood monitoring and early warnings.
- **Agricultural Automation:** Use AI and IoT to automate tasks like planting, watering, and harvesting in agriculture, leading to increased crop yield and reduced labor costs.
- **Energy Grid Optimization:** Utilize IoT-enabled smart meters and AI algorithms to balance energy demand and supply, improving efficiency and reducing costs.
- **Waste Management:** Combine IoT sensors on waste bins with AI analytics to optimize waste collection routes and schedules, reducing fuel consumption and operational costs.
- **Consumer Electronics:** Infuse AI capabilities into IoT-connected consumer electronics to create intelligent devices that can learn user preferences and adapt their behavior.
- **Smart Appliances:** Integrate AI and IoT to create appliances that can interact with users, optimize energy usage, and provide real-time feedback on performance.

Orchestrated platform ecosystems combining AI and IoT accelerate adoption and growth of digital economies. IoT produces data, AI consumes data, supply chains and networks transport data and data centers process applications to monetize data for a wide variety of use cases. Emerging trends in digital platforms include sustainability, connected manufacturing, creator economies, and new regulations[40]**:**

[40] https://mitsloan.mit.edu/ideas-made-to-matter/5-trends-mit-platform-report

1. **Integration of Artificial Intelligence (AI):** AI is becoming integral to digital platforms, offering scalability, flexibility, better decision-making, and personalized processes. Some platforms will offer AI as a service, while others will adopt AI for their own operations. Challenges include addressing biases, labor issues, and equitable share of AI benefits.

2. **Growth of Circular Platforms:** Digital platforms will support circular economies by enabling product and material exchanges, promoting reuse, repair, redesign, and recycling. Opportunities include material exchanges, reuse/resale marketplaces, sharing assets (e.g., cars, real estate), circular supplier networks, and sustainable logistics.

3. **Varied Platform Regulations:** Platforms face new regulatory oversight, with variations between geographic regions. For example, the US Section 230 offers legal immunity for content posted by third parties, while the EU Digital Services Act requires transparency and holds platforms liable for violating terms of service.

4. **Connected Manufacturing:** Manufacturing is adopting digital technologies with platform-based solutions leveraging data for smarter factory operations, optimized supply and demand forecasting, and predictive analytics. This enhances supply chain visibility and competitive advantage.

5. **Increasing Power of Influencers and the Creator Economy:** The creator economy, estimated at $100 billion, is driven by independent creators monetizing their activities. Influencers and creators face challenges like burnout and time management, with AI tools like ChatGPT offering assistance in saving time and managing workloads.

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

The explosive growth of AI and IoT platforms require monitoring and regulatory actions: The above use cases are a fraction the vast potential combining AI and IoT platforms fed by data transported through supply chains or networks which may or may not be trusted. ChatGPT platform reached 100M users in a fraction of time compared to Twitter and Facebook and 2M developers creating a plethora of APIs and

apps. Many of these developers rogue actors from adversary nations connecting remotely to AI platforms, so monitoring and regulating these platform ecosystems are key to mitigate risks and drive growth.

Finding 15: Quantum computing poses a major and serious threat to cybersecurity.

Commented [GW7]: Nick and Ranveer will review

Commented [GW8]: Note: These findings will be renumbered; retaining former numbers to help align with recent action item assignments

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] According to the White House National Security Memorandum/NSM-10 on Quantum Computing, "a quantum computer of sufficient size and sophistication — also known as a cryptanalytically relevant quantum computer (CRQC) — will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."[4].

IoT devices are particularly vulnerable to the risks posed by quantum computing for a variety of reasons, including:

- The decentralized nature of (IoT) networks, the use of static keys, static certificates, stored databases, and the use of Trusted Third Parties (TTP) and reliance on the Transport Layer Security (TLS) protocol makes nearly all IoT devices and technology at the edges vulnerable.
- In addition, 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.
- 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 use of quantum computing to conduct cyberattacks is high (either for access to their data or to spoof/corrupt the data)

However, with the introduction of quantum computing and AI into this mix, all of the exploits and vulnerabilities that exist now, will be magnified and made even more severely prone to malicious attacks at much greater speeds and to much greater detriment than at present.

While the concerns about the ability of quantum computers to break today's encryption algorithms are valid, the availability of cryptanalytically relevant quantum computers (CRQC) powerful enough to do so will not be developed until at least the 2030s.[6] The response to post-quantum cybersecurity is in its early stages. NIST is in the process of standardizing on a set of post quantum cryptographic algorithms. Four algorithms are in going through the standardization process (completion sometime in 2024) with three additional ones being considered for standardization.

The 2030s is not that far away, but there is limited industry development activity to prepare for the transition. Industry efforts are needed to develop standardized post-quantum cryptography solutions that are capable of operating on resource constrained devices, such as those with limited processing and power capabilities used at the network edges.

- There may be IOT networks that are important enough to protect at the network level as well, if not now then in the near to medium term;
- Development of post-quantum cryptography solutions should prioritize those that require a minimum of processing and power consumption at the edge;. and
- Quantum resistant technology will need to be highly decentralized, easily deployable on existing infrastructure, and utilize NIST standards.

Finding 16: 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. There are cybersecurity concerns from industry and government about IoT equipment and components (including modules) produced by companies in China.

These concerns were highlighted in a letter, 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 (Select Committee) 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 and present opportunities for malicious use—specifically, that 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, whether the FCC can 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 on the U.S. network; Whether requiring certification for modules would effectively counter PRC-based modules from affecting the U.S. network; and Whether the FCC needs additional statutory authority from Congress to address this concern.

These additional concerns build on existing IoT cybersecurity concerns, and may hinder adoption. Some of these concerns are manifested in various announced actions and news, including:

1. On August 7, 2023 Chair Mike Gallagher (R-WI) and Ranking Member Raja Krishnamoorthi (D-IL) of the House Select Committee on the Chinese Communist Party (Select Committee) wrote to FCC Chair Jessica Rosenworcel with a series of questions regarding the FCC's ability to track Chinese made IoT modules and the potential risks of Chinese-made IoT modules.

2. On February 29, 2023, citing National Security Concerns, the Biden-Harris Administration Announces Inquiry into Connected Vehicles. Source [commerce.gov].

3. Lawmakers raise concerns over Chinese-made LiDAR tech. Source [nextgov.com].

4. China's cornered the IoT market. That could be a cybersecurity nightmare. Source [techmonitor.ai].

5. Draft legislation covering federal procurement prohibition on covered IoT modules or devices manufactured in a country the government of which is a foreign adversary, as defined in section 8(c) of the Secure and Trusted Communications Networks Act of 2019 (47 U.S.C. 1607(c)); and

(B) includes—

(i) the People's Republic of China (including the Special Administrative Regions of the People's Republic of China, Hong Kong and Macau);

(ii) the Russian Federation;

(iii) the Islamic Republic of Iran;

(iv) the Democratic People's Republic of Korea;

(v) the Republic of Cuba;

(vi) the Maduro Regime of Venezuela; and

(vii) the Syrian Arab Republic.

Industry findings – Specific Considerations

Finding 17: Precision Agriculture. IoT brings significant value to agriculture, but adoption is slow.

Supports Recommendation(s) ~~X.X, X.X~~

Agriculture is undergoing a transformation driven by the integration of information and digital communications technologies, the Internet of Things (IoT), data analytics, automation and robotics and other emerging technologies.[41] This transformation offers the potential to increase agricultural productivity, operational efficiency, facilitate adaptation to climate changes and enhance overall competitiveness. IoT sensors on tractors, drones, and in the soil collect data on soil moisture, nutrient levels, and crop health. IoT-based irrigation systems monitor weather conditions and soil levels. Wearable IoT devices on livestock provide real-time data on animal health, behavior, and location. IoT sensors in fields continuously monitor environmental conditions and provide 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.

Commented [GW9]: Nick and Ranveer will review

Commented [GW10]: Note: These findings will be renumbered; retaining former numbers to help align with recent action item assignments

Commented [HN(MT11]: Renumber

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

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.

- Story 1: IoT can help small family farms be productive and profitable
    - 2 million farms in US. 98% are family farms. Small family farms (gross income < 350K) are 90% of all farms, 48.8% of all farmland, and 21.1% of production
    - 62 - 81% of these small family farms are operating on < 10% margins
    - Production expenses have increased by 18% in 2022
- Story 2: IoT can help agricultural producers navigate around the impacts of the changing climate.
    - Changing temps and precipitation patterns affect plant lifecycles, decrease crop yields, increase livestock stress and health, reproduction and milk and egg production
    - Corn yields have declined 3.8% and wheat yields have declined 5.5% (compared to no climate trends)
- Story 3: IoT can help increase agricultural production yields to support the upcoming food shortage
    - By 2050, UN estimates there will be a global food shortage

- Increase in half percent in yield was enough to end starvation and famine in India (Green Revolution)

IoT in agriculture suffers from a variety of challenges. The top barriers include:[42]

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

- **Digital skills.** As digital and emerging technologies are increasingly integrated into agricultural equipment and operations, the skills that agriculture workers need to be successful will change. For example, as smart machines increasingly automate previously manual activities, agriculture jobs will evolve from being low skill repetitive physical work to medium to high skill non-repetitive digital work. New skills include data analytics, precision agriculture, robotics and automation, networking, and systems integration.

- **Interoperability.** Farms have a variety of equipment, from the "latest and greatest" equipment with current technology to 30- to 40-year-old legacy equipment with limited technology and no connectivity. Interoperability challenges are a major barrier to IoT adoption and value realization in agriculture where old and new equipment need to coexist and work together. For example, some equipment may incorporate incompatible physical connections and require the use of adapters to communicate with other equipment. Others may have different formats (or syntaxes) for the same data, while others have different meanings for the data. Old equipment may not work with newer equipment, despite coming from the same manufacturer.

- **Adoption resistance.** Despite the benefits of IoT and precision agriculture technologies and solutions, uptake of these solutions have been uneven and

[42] 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

may take as long as 15 years for the technology to reach a critical mass.[43] Large producers are more likely to adopt these technologies compared to smaller farms because they have more education, are less wary of technology and can support larger economies of scale.[44] Some of these reasons, include the limited availability of broadband and connectivity in rural areas, "right to repair" concerns, trust in personal expertise over technology, and poor previous experiences with technology.

Finding 18: Smart communities and infrastructure. The development of smart communities in the United States is limited, uneven and slow to develop.

Commented [GW12]: Debra and Nicole

Supports Recommendation(s) x.x, x.x

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.

There are examples of IoT-enabled smart community applications in use today. These 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 notifies city staff immediately so that it can be replaced.
- Smart parking employs either in-ground sensors or cameras to monitor parking space availability. Open spaces are communicated to drivers through a mobile app or digital signage on the street or garage. This helps drivers navigate to the space directly, instead of driving around looking. In addition, it also helps identify parking space violations and direct parking enforcement officers to the spot directly without having to drive around.
- Community air quality networks are deployed in select areas of the community to monitor environmental conditions and inform residents and policymakers.

[43] "Adoption of Farming Technology, Or Precision Ag, Varies Across Generations", KTTN News, December 20, 2020. Link

[44] "Adoption of Precision Agriculture", USDA NIFA. Link

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, is very expensive. While larger cities may have the capabilities and some funding vehicles to support these projects, America’s small and medium size cities do have very limited capabilities. In some cases, federal, state and regional grants may be available, but securing these grants can be difficult.

- Lack of skills and resources. Many cities and communities lack the new innovation and digital skills and resources to plan, deploy, operate and support IoT applications. These resources are scarce in the market, and cities often cannot compete with the private sector for the same talent.

- Privacy Concerns. The extensive collection of data from IoT devices raises concerns about data security and privacy. Ensuring robust cybersecurity measures and transparent data handling practices is crucial to building and maintaining public trust.

- Community and political resistance: Candidates are not elected for building a smart 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.

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]

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

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

Finding 19: 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.

Commented [GW13]: Steve and Benson

Supports Recommendation(s) x.x, x.x

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.[45]
- 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.[46]
- A project with an auto maker and a bicycle safety platform maker to highlight the benefits of C-V2X-powered bicycle use cases.[47]
- A project with the Tampa Hillsborough Expressway Authority (THEA) to deploy and pilot Connected Vehicle (CV) applications to demonstrate safety and mobility benefits of the technology with respect to pedestrians in and around downtown Tampa.[48]
- 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.[49]
- 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.[50]
- Tri-Met in Portland, OR. The Tri-County Metropolitan Transportation District of Oregon (TriMet) serves an area of 500 square miles, operating a fleet of over 700 buses on 85 routes with thousands of stops. Smart systems maintain bus intervals and on congested corridors, prioritize bus travel over other vehicles by sensing bus arrival time then manipulating traffic signal phases[51]

---

[45] 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.

[46] 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#

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

[48] https://www.its.dot.gov/pilots/pilots_thea.htm
[49] https://teo.fdot.gov/architecture/architectures/d2/html/projects/projarch47.html
[50] https://www.digi.com/resources/customer-stories/new-york-city-dot-deploys-digi-solutions
[51] https://www.digi.com/resources/customer-stories/trimet-bus-fleet-management-with-digi-connectivity

- Positive Train Control- - SEPTA, LIRR, MNR, MBTA, AMTRAK. Positive Train Control (PTC) utilizes GPS, sensors and wireless communications technology to autonomously stop a train when necessary and to prevent train-to-train collisions, over-speed derailments, and unauthorized train movement. PTC helps ensures the safety of passengers by acting as a safeguard against human errors and other potential hazards.[52]

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

While there are several opportunities and benefits for personas that use these technologies, primarily in the realm of safety (e.g., emergency vehicle preemption, entering school or work zone, pedestrian crossing ahead), these technologies can also provide valuable support functions such as package, food, and medicine delivery. There are also environmental benefits from congestion mitigation and providing an orderly flow of traffic (See Carnegie Mellon Study for an example: https://www.cmu.edu/piper/news/archives/2012/october/smart-signals.html) as well as increased productivity (drivers spend less time stuck in traffic). Other personas may use these technologies to develop and operate innovative transportation services, such as those involving multimodal transit, ridesharing, and autonomous transportation of people and goods.

There also exist several barriers faced by personas seeking to implement these technologies. On the policy side clarity is needed with respect to data governance and privacy and what aspects of data jurisdictions can collect, retain, and subsequently use. Certain aspects of this sector still need high level policies and regulations that adequately address safety and liability concerns. The benefits of these technologies are not available in rural or undeserved 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

[52] https://www.digi.com/resources/customer-stories/digi-helps-septa-comply-with-federal-mandate

in this sector. The examples provided above reinforce that this technology is ready to go mainstream.

Finding 20: Healthcare. IoT is transforming healthcare and is poised to revolutionize it, but significant challenges need to be addressed.

Commented [GW14]: Ann and Maria will review and refine

Supports Recommendation(s) x.x, x.x

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:

Suggestions for Graphics Person:

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

1. 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).
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.

Some examples of top IoMT applications include:

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

IoMT enables the following benefits, including:

- **Enhanced Patient Outcomes**. By enabling continuous monitoring and personalized care, IoMT contributes to improved patient outcomes. Timely access to health data allows for early detection of potential issues, better management of chronic conditions, and more proactive interventions.
- **Efficiency and Cost Savings**. The implementation of IoT in healthcare streamlines workflows, reduces manual tasks, and enhances the efficiency of healthcare delivery. This not only improves the quality of care but also contributes to cost savings by minimizing unnecessary hospitalizations, optimizing resource utilization and minimizing administrative costs.

- **Patient Engagement and Empowerment**. IoMT empowers patients to actively participate in their healthcare journey. Access to real-time health data through wearable devices fosters a sense of ownership and encourages individuals to make informed decisions about their lifestyles and treatment plans.

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

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

Commented [GW15]: The Health group added "Edge AI Technologies" but not sure it fits

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

Finding 21: 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.

Commented [GW16]: Arman will review

Supports Recommendation(s) x.x, x.x

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

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

- **Monitor air quality.** Air quality sensors measure the concentration of pollutants in the air, including particulate matter (e.g., soot or black carbon), and gas pollutants (carbon monoxide, nitrogen dioxide, etc.). This information informs residents of a community whether to go outside exercise or not. The collected data may be used by city and health officials to identify areas of poor air quality, and to devise programs to mitigate its effects (such as planting trees in the area, restricting traffic at certain hours, banning idling cars at certain hours, providing residents with respiratory healthcare information, etc.).

- **Optimize water use.** Farming consumes a lot of water. Soil moisture sensors, integrated with automatic irrigation systems, measure moisture levels and activate the irrigation systems in those spots in the field where the water is needed. This helps save water (and the corresponding expenses) by precisely directing water to those spots where it is needed. This optimizes water usage by applying water it is most needed and reducing waste and conserving resources.

- **Reduce carbon emissions.** Intelligent traffic management systems, incorporating IoT sensors, detect heavy traffic conditions and automatically adjust traffic signals to reduce congestion. This increases the capacity of the street or freeway to handle more cars, while reducing the time cars are idling. The overall effect is a reduction in emissions and its impact on residents of the surrounding community.

- **Reduce energy use.** Buildings are one of the largest consumers of electricity. Room occupancy sensors turn off lights in empty rooms. Smart thermostats learn the behavior of building occupants and autonomously manage ambient temperatures based on those patterns. Automated demand response systems, connected to building automation and energy management systems, automatically reduce energy use by turning things off during peak demand periods while minimizing impact on building occupants.

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

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

- **Improved and more effective outcomes.** The use of IoT enables the direct monitoring of the environment at the precise locations needed. The data collected can be used to improve and validate simulation models, and to predict likely trends and patterns. This foresight leads to more informed policies and strategies, which can then be implemented and monitored.

- **Increased resource use efficiency.** Analysis of the collected data provides insights that lead to optimization strategies. For example, a study of energy usage data helps identify patterns that may be adjusted. Automation systems may be programmed with these insights to optimize energy utilization, minimizing waste and enhancing efficiency.

- **Agile and proactive response.** Real-time monitoring of environmental conditions, such as water contamination and air quality levels, allow the community to plan and respond swiftly. This enhances the effectiveness of the response, the number of resources applied, and minimizes the extent of the adverse impacts.

- **Informed and data-driven decision making.** The vast amount of data collected by IoT devices enables informed decision-making for policymakers, businesses, and individuals in the pursuit of sustainability goals. This leads to more effective policies and strategies, more productive use of resources, and sustainable outcomes.

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

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

- **Lack of supporting infrastructure.** Environmental monitoring devices may be deployed in remote or rural areas with limited or unreliable network connectivity, affecting the real-time transmission of data. For example, many wildfires start in remote areas and early detection is critical to containing the

impact. Many river monitoring stations are located upstream in remote areas. Ocean monitoring buoys are located in areas with no infrastructure. These remote areas have limited to no connectivity service, and hinders the ability to deploy IoT in these areas.

- **Initial Implementation Costs.** The upfront high costs of purchasing and deploying environmental monitoring sensors are a barrier for many agencies and communities. These costs are increased if a large network of sensors is needed. For example, in a city environment, air quality levels significantly. A street next to a freeway has poorer air quality than a street a mile away. In those applications where a dense network of sensors is needed, such as community air quality monitoring, the costs can 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.

Finding 22: Public Safety. IoT can enhance and improve public safety outcomes, but must overcome a wide variety of technical, community and policy challenges, before it can be deployed and used at scale.

Commented [GW17]: Ann and Nicole will review

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

- **Smart Surveillance.** IoT-enabled surveillance cameras and sensors are deployed in public spaces to monitor and detect unusual activities or potential threats in real-time. For example, connected audio sensors detect the sound of gunshots or breaking glass, identify the location and notify police so they can respond faster. Smart cameras detect and report suspicious and unpermitted behaviors, such as unattended luggage or packages, trespassing into secure areas, lack of social distancing, or fighting, display of a gun and other illegal activities. These smart applications enable and accurate monitoring and review of thousands of camera and sensor feeds autonomously with limited human involvement. In addition, when integrated with next-gen 911 systems, IoT systems provide dispatchers and first responders with relevant information and situational awareness for more effective deployment of resources and personnel.

- **Situational Awareness.** The use of IoT provides communities and responders with detailed information about existing and future events. For example, drones fly over active disaster areas to provide responders with a fast assessment of the scene to inform on deployment of resources and activities. Water level sensors monitor upstream river and stream levels to provide communities with knowledge of real-time conditions and enhance flood response, evacuation, and mitigation activities. Sensors that detect Wi-Fi signals from mobile phones allow first responders to know how many people are inside a building and where they are at. Air quality sensors monitor the pollution levels of communities, and inform public health officials of intervention programs to mitigate respiratory illnesses. The use of IoT for situation awareness facilitates where to focus initial resources to save human lives.

- **Responder Monitoring.** Wearable IoT devices, such as body cameras, biometric monitors, and communication devices, enhance the capabilities and safety of first responders during operations. These IoT devices inform operations

managers of responder stress levels, conditions of the surrounding environment and state of responder equipment. For example, sensors on oxygen tanks provide responders with a real-time estimate of the remaining time left, and takes into account responder exertion and stress levels. Body cameras on police provide a record of how officers respond to activities, document actions, hold officers accountable and provide a record of activities that is reviewed to improve future operations.

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

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

- **Improved Situational Awareness.** IoT devices provide real-time data, supplementing existing information. and enabling public safety agencies, first responders, disaster and resilience managers, and health officials to have a comprehensive and real time view of ongoing and developing situations. This improves decision-making and facilitates resource allocation during emergencies.

- **Increased Response Effectiveness.** Connected devices enable faster communication and response coordination. Emergency services can be dispatched more efficiently, reducing the time it takes to address critical situations.

- **Preventive and Predictive Capabilities.** IoT sensors enable the collection of data for predictive analytics. For example, information collected from gunshot detection sensors can be analyzed to predict when and where potential future incidents may occur. The police can anticipate potential risks and take preventive measures like stationing more officers at the predicted times and locations, to reduce the likelihood of incidents.

- **Data-Driven Decision-Making.** The data collected from IoT complements existing and historical information and knowledge to inform and enhance decision-making. For example, air quality monitors identify areas of a city where poor air quality consistently exists. Using this knowledge, along with the

correlation between increased death rates and air pollution,[53] 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

[53] 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/

funding vehicles, including grants, internal capital budgets, and capital improvement budgets. Other than grants, funding is based on agency priorities and availability, and can be subject to long procurement cycles.

Recommendations of the IoT Advisory Board

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

1.5. Establishing a National IoT Strategy and Leadership
2.6. Modernizing IoT Infrastructure
3.7. Establishing Trust in IoT
4.8. Fostering a IoT-ready Workforce
5.9. Facilitating Adoption
6.10. Incentivizing the IoT Economy including a Resilient IoT Supply Chain

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.

Recommendations Summary

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

Establishing a National IoT Strategy and Leadership

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

Key Recommendation KR1.1: Establish a strategic national approach 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, supercharge economic growth, increase public safety, create a more sustainable planet, individualize healthcare, and facilitate an equitable quality of life and well-being. This progress will be best facilitated by a strategic national approach for IoT.

In 2010, the President's Council of Advisors on Science and Technology (PCAST) recommended the Federal Government invest in a national, long-term, multi-agency, multi-faceted research initiative in these areas.[54] 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.[55] 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, and we might never get to where we need to be, and the recommended the creation of a long-range action plan.

[54] The 2010 PCAST report is available from: https://www.nitrd.gov/pubs/PCAST-NITRD-report-2010.pdf
[55] The OSTP/NSTC white paper is available from: https://www.nitrd.gov/pubs/CPS-OSTP-Response-Winning-The-Future.pdf

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

Likewise, a NITRD Report from 2012 that looked at opportunity in Agriculture, smart building, defense, emergency response, energy healthcare, manufacturing and transportation, advocated for a multi-agency, multi-sector comprehensive focus on the difficult crosscutting R&D challenges in CPS.[56]

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

We need a comprehensive national IoT strategy that:

- describes a comprehensive vision for the federal government's role in IoT;
- articulates the role that IOT can play across sectors and agencies, and within sectors, in advancing national priorities and solving social challenges – across health, transportation, manufacturing, energy etc.;
- ensures continued U.S. leadership in connected device technologies, a vibrant and innovative commercial sector, and U.S. leadership in the way the technologies are harnessed to address national challenges;
- comprehensively catalogues the game changing work the administration is already doing across many agencies in fundamental research, development, demonstration and deployments – and the important role agencies are playing in meeting our critical needs;
- 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 major grand challenges.

This undertaking is likely to be extremely large and complex. Successful execution will require the focus and dedication of an office that is staffed, and which has the authority to direct executive branch resources. The results of that work will be high-visibility and will highlight important federal work, so there should be a way to share

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

performance outcomes. Like nano.gov, ai.gov, and the Chips for America websites, stakeholders will benefit from central Internet presence that will share the strategy and vision, demonstrate the many ways the government is tackling these issues, and engage stakeholders in meaningful ways. By monitoring and tracking progress of various initiatives, federal leaders will be able to track achievement of key outcomes of the IoT strategic approach.

Enabling Recommendation ER1.1.1: Strongly consider including IoT in the federal critical and emerging technology 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.

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

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.[57] 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.[58] Still others like data ecosystems, automated machine learning, wireless battery-free sensors, neurosynaptic chips, QRNG chips, biodegradable sensors, 6G and quantum computing are still "years out" and require continued research investments.[59]

[57] "55+ emerging IoT technologies you should have on your radar (2022 update)," S. Sinha, IoT Analytics, April 6, 2022. Link
[58] ibid.
[59] ibid.

Enabling Recommendation ER1.1.2: Further improve and elevate inter-agency coordination.

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 there is an NSTC IoT committee that is properly named, elevated, and empowered, just like other NSTC committees focused on AI, Quantum and Nanotechnology. This is particularly important as formerly separate disciplines of AI, Quantum and IoT begin to converge. It's also critical that an approach must be inclusive of IoT and the many different names and enablers.

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

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

Congress should create and fund a new National Coordination Office for IoT/CPS for advancing this strategy, like it has in the areas of Nanotechnology, Quantum, and AI. 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, and AI.

Commented [WG(MT18]: For discussion at the May IoTAB meeting

Key Recommendation KR1.1.3: Study the impact of Quantum computing and post-quantum cryptography need further study by the Executive Branch and the Legislative Branch.

Supported by Finding x.x

Commented [HN(MT19]: Need to flesh out this recommendation on May 14/15 meeting.

Other recommendations:

- Incorporate quantum computing and post-quantum cryptography considerations in the development of the national IoT strategy

- Incorporate IoT considerations into the quantum strategy
- Promote industry awareness of post-quantum
- Develop plans to facilitate transition to post-quantum
- Need to plan and prepare industry and organizations to transition to post quantum cryptography
- 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

Key Recommendation KR1.1.4: The federal government 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

Commented [HN(MT20]: Need to flesh out this recommendation on May 14/15 meeting.

DAN provided recommendation. Need text to populate

Small Business Leadership

Key Recommendation KR1.2: 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.

Supported by Finding x.x

BENSON to provide text about making this more about Innovation

The federal government should accelerate IoT technology adoption and manufacturing for small business and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. Small businesses and startup organizations who are looking to adopt or manufacture IoT technologies may find it challenging to know where to start or have the resources and knowledge to do so. Federal funding mechanisms and procurements targeted to them can aid these companies by giving them a resource to help speed and incentivize their adoption.

Enabling Recommendation ER1.2.1: Accelerate adoption of IoT technologies manufactured by small business and startup organizations through targeted Federal Government programs, policies, procedures, and funding methods.

Supported by Finding x.x

The federal government should accelerate the adoption of IoT technologies manufacturers by small business and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. It is particularly challenging for small businesses and startup companies in this sector that have to provide upfront capital and full understanding in successfully navigating opportunities both within the federal government and with federal government support to market externally. The process for these projects can also take many years to bring them from proposal to commercial operation and these companies may not have patient resources.

Small businesses have the primary option of using a channel with existing relationships to cities to make sales which is also unpredictable and not very scalable. This makes it challenging for small businesses and startups. Federal funding mechanisms and procurements targeted to them can aid these companies so they can more effectively compete with larger organizations on RFPs relevant to their business. There are many existing Federal Government programs and policies that support small businesses and startup organizations. Rather than create from scratch, this recommendation advises tapping into these existing programs and have a dedicated IoT technologies track for related small businesses and startups in this space.

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 ER1.2.2: Accelerate the adoption of IoT technologies manufactured by small business and startup organizations.

Supported by Finding x.x

Through policies, procedures, and targeted funding methods, the federal government should accelerate the adoption of IoT technologies manufactured by small business and startup organizations. This can be done via policies, procedures, and funding methods that specifically target them. It is particularly challenging for these types of manufacturers in this sector that have to provide upfront capital, access, and knowhow, before hopefully being selected as a result of an RFP. The process for these projects can also take many years to bring them from proposal to commercial operation and these companies may lose both funding, ability, and interest in that time frame.

Small businesses IoT technology manufacturers have the primary option of using a channel with existing relationships to local governments to make sales which is also unpredictable and not very scalable. Federal funding mechanisms and procurements targeted to them can aid these companies so they can more effectively compete with larger organizations on RFPs relevant to their business.

Greater adoption of IoT technologies manufactured by small businesses and startups could help in the following examples:

- Incorporation of technologies enabled by IoT: Opportunities for IoT technologies are manufacturers by small business and startups across the IoT. For example, in smart, connected transportation these technologies include sensors, cameras, and edge computing devices that can improve safety in things such as vulnerable road users (i.e., pedestrians at crosswalks), traffic intersections, school, and work zones. Opportunities for IoT technologies in electrified transportation manufactured by small businesses and startups include in car systems or mobile apps that can locate charging stations, as well sensors that manage charging stations to gather data about usage and performance, to anticipate maintenance needs, and troubleshoot problems.
- Greater competition across IoT markets: Incentivizing small businesses and startups to bid on projects and deploy their technology will increase their

market penetration and provide end-users more technology options. This would lead to greater competition in selected markets providing end-users the ability to select manufacturers based on several factors such as cost, quality of products manufactured, service, and innovation.

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.

Enabling Recommendation ER1.2.3: Fully fund existing IoT research, development, deployment and demonstrations. (was 1.1.3)

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 allows them to operate, automate and sustain itself at scale.

In addition, the U.S. Government should fully fund science agencies that are doing work in these areas through important IoT-related programs such as those at ARPA, DOE, NSF, and DOT. It may also require a more significant role for OSTP in IoT-related research. Failure to do so will slow down government efforts and cut our IoT opportunity short.

Enabling Recommendation ER1.2.4: Specify and use, for federally-funded projects, IoT technologies and applications that are energy efficient, sustainable, and "smart". (WAS 1.1.6)

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.[60] 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

[60] 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/

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.

International Leadership

Key Recommendation KR1.3: Promote international collaboration in IoT adoption to share knowledge, best practices, and resources.

Supported by Finding x.x

Promoting international collaboration in the drive to adopt IoT technologies presents a unique opportunity to foster the sharing of knowledge, best practices, and resources among countries and regions. The goal is to spur innovation and accelerate the widespread adoption of IoT technologies. Stakeholders like the United States Federal Government, European Union Commission, and Asian Development Bank can form a global ecosystem that supports the development and deployment of IoT solutions, thereby tackling challenges related to interoperability, standardization, and regulatory compliance.

This international collaboration necessitates the creation of platforms and forums that allow policymakers, industry stakeholders, technology providers, and researchers from different countries to come together. Such platforms could include international bodies like the World Economic Forum, United Nations Industrial Development Organization, and International Telecommunication Union. These stakeholders can engage in a productive exchange of ideas, address common challenges, and explore opportunities for joint projects and initiatives. The outcome of these collaborations could be the development of harmonized regulations, standards, and guidelines that enable seamless integration of IoT systems across borders. This harmonization can foster efficient and resilient global supply chain networks.

International collaboration can facilitate the pooling of resources and expertise to support research and development efforts, pilot projects, and capacity-building initiatives aimed at promoting IoT adoption, such as in supply chain management. Organizations like the World Bank and World Trade Organization can help bridge the digital divide between developed and developing countries, ensuring that businesses worldwide have access to the tools and technologies needed to harness the potential of IoT in their operations. This collective effort, led by governments actively engaging with international partners and participating in relevant forums and organizations, can contribute to the development of a connected and resilient global supply chain ecosystem that benefits businesses and consumers alike.

Enabling Recommendation ER1.3.1: 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.

New Leading the Way Key Recommendation

Text to be provided by Benson at the May meeting

Enabling Recommendation ER1.4.1: Lead the way in facilitating IoT adoption promotion by adopting IoT technologies and systems for its own internal operations and needs. (was 1.1.4)

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, in asset

tracking using IoT helps agencies manage their assets, equipment and supplies more effectively, reduce equipment losses, facilitates distribution of equipment, and aids in recovery of missing and stolen equipment and supplies. Another common use of IoT is for condition monitoring. This application spans a variety of uses, from the operating condition of a vehicle, to critical infrastructure, and allows for the remote monitoring of an asset's status and performance. The data collected enables asset owners to detect issues early, and to apply corrective measures to minimize downtime, optimize asset performance, and meet service levels.

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

The federal government should promote its current use of IoT technologies, in order to drive broader visibility and awareness to the market and to other agencies. IoT applications and solutions should be piloted at a small scale initially to evaluate effectiveness and identify challenges. Notably, agency funding and budget allocations for this may not be a priority. 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: Upgrade legacy federally-owned or operated IoT infrastructure that is integrated into government facilities, assets, and operations. (was 1.1.5)

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: 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. (was 1.1.7)

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.** Processing of IoT workloads is increasingly moving to the edge to support requirements for low latency, high reliability and autonomous operations. Advancements in increasing device processing capabilities to support AI workloads, decreasing processor energy consumption, and low-cost sensors and processors are needed.
- **Enabling network infrastructure to support IoT at scale.** Network and communications infrastructure must support billions of heterogeneous IoT devices, distributed across the cloud, edge and mobile environments. Advancements in a number of areas, such as the management and operations of distributed networks, spectrum sharing and management, infrastructure to support AI and complex IoT application workloads, fault tolerant and resilient infrastructure, and context-aware computing are needed.
- **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.** The full value of IoT is realized when it is embedded and integrated transparently into all aspects of our economy, society and lives. Facilitating the realization of beneficial outcomes requires that IoT be human centric and usable. Advancements in a number of areas, such as the design of IoT systems for human-AI interaction and collaboration, development of trust in human-AI interactions, and user experience and user interactions.
- **Enabling trustworthy IoT.** Trust in IoT is paramount in a hyperconnected future with billions of IoT devices integrated into all aspects of the economy. Current research and industry efforts, centered around cybersecurity and

privacy, should continue. Additional research is needed to drive advancements in the development of trustworthy IoT systems in a wide variety of areas. Examples include confidential computing, lightweight quantum-safe cryptographic algorithms for resource constrained devices, and software defined networking and self-defending adaptive 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 continually evolving in response to a variety of adopter needs. Continuing research and development is needed to create the technological advancements needed to meet these needs and remove the barriers hindering its adoption. For example, the shifting of data processing from the cloud to the edge supports the need for low latency and autonomous operations. However, processing on the device and on edge servers add significant complexity to the design, operation and management of these systems and applications. New technologies must be developed to build the innovations necessary.

Industry efforts are focused on the development of nearer term innovations. These efforts typically support incremental improvements and nearer term goals. Federal research investments catalyze the development and acceleration of new innovations that have broad impact to the economy and transferred to industry, as well as those that industry may not necessarily focus on, and those that are high risk with uncertain outcomes.

Modernizing IoT Infrastructure

Objective 2: The U.S. should call upon and collaborate with industry to enhance and modernize the infrastructure that enables and supports IoT. Such collaboration should include the provision of clear direction and support for consistent and resilient communications among devices, update of legacy computing and networking systems, improved connectivity and interconnection among technologies.

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.

Promoting Existing Methods

Key Recommendation KR2.1: Promote collaborative development across industries to adopt existing industry standards and protocols.

Supported by Finding x.x

Industry collaboration will better advance existing communications and interoperability protocols that can rapidly be encouraged and adopted. The Board did not identify any single protocol that will solve the interoperability issues, since these models tend to application or domain specific, and does not recommend wholly new standards and models to be created “from scratch”. The Board highly recommends not to mandate any formal or informal standard or protocol, but rather to encourage voluntary cooperation in the interest of improved interoperability.

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

Enabling Recommendation ER2.1.1: Advocate for the implementation and adoption of interoperable data standards for public safety IoT.

The proliferation of IoT with interoperability challenges hampers future success. In public safety, IoT interoperability will enhance incident responses and coordination among responder teams, providing safety benefits that would encourage the adoption of IoT. Solutions might include facilitation of adoption by funding grants for jurisdictions/agencies for procurement of interoperable IoT solutions. Support could also include development of education/training materials to help jurisdictions/agencies apply best practices for interoperability.

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) will further aid progress. From a high level, the consideration of tax incentives that would encourage companies to implement public safety IoT with interoperable data standards and the education and promotion of interoperable data guidelines for public safety IoT across different jurisdictions (e.g., local and regional).

Enabling Recommendation ER2.1.2: Promote and, if necessary, develop a protocol for data exchange standards for IoMT (Internet of Medical Things) for interoperability, and promote the adoption of these standards.

Supported by Finding x.x

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

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

Enabling Recommendation ER2.1.3: Promote the development and use of standards for supply chain logistics, traceability, and assurance.

Supported by Finding x.x

The federal government should foster the development, adoption, and use of standards and protocols for supply chain logistics, traceability, and assurance. It should collaborate with Standards Development Organizations (SDOs) and international allies to promote assured & traceable products by manufacturers for efficient, reliable, and secure supply of goods. It should incentivize suppliers to establish unique corporate IDs, product IDs, asset IDs, and part IDs linked to a digital thread of information and data, that are used to track and trace goods while improving supply chain efficiency, transparency, resilience, and security. There is value in encouraging the use of Global Identifier Standards (such as GLS of GS1) in procurement contracts and regulatory frameworks and track goods and info related to assets and data, to optimize risk, cost, benefits, and value.

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

The government could Identify one or more federal agencies suited to convening a public-private partnership to establish a roadmap towards interoperability. The roadmap should be designed to enable interoperability for tools and data structures in supply chain logistics, traceability, and assurance. Towards that goal, they may apply some tactics such as encouraging inclusiveness from a diverse range of stakeholders, prioritizing critical areas of supply chain management where standardization can yield significant benefits, and developing mechanisms to monitor and enforce compliance to standards.

Enabling Recommendation ER2.1.4: Promote standards and protocols for IoT technology in supply chain management to provide assurance of interoperability, reliability, and security across various IoT systems and devices.

Supported by Finding x.x

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

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

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

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

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

Key Recommendation KR2.2: 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

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

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

A common theme from IoT users through the development of this report was their concerns about getting "locked-in" to a particular vendor's proprietary technology. These concerns currently act as an impediment to IoT adoption. No company or agency wants to invest in infrastructure that will rapidly become obsolete. Quite the opposite is true – in many cases, IoT infrastructure may need to operate for many decades. Parallel examples such as Wi-Fi (supported through IEEE 802 series technical standards) and cellular industry consortium standards demonstrate that interoperability and standardization do not reduce a vendor's ability to innovate. Quite the opposite seems to be true – the ability for products to work together has great possibilities for both established manufacturers and newcomers.

Before the government can foster specific standards, it may be helpful for one or more agencies to perform a survey of available and relevant standards, protocols, and models. Due to the differences in sub-sectors, each such effort must be constrained

to a specific application space, such as smart home or IoMT. Such a survey would be helpful, for example, if agencies wish to include open standards and consortium developed standards as part of the requirements for federal funded projects. Federal recommendations (or requirements) for a taxonomy or set of applicable models will promote industry adoption and foster standardization.

Enabling Recommendation ER2.2.1: Facilitate interoperability through the development of a consistent data taxonomy for the sharing and exchange of data collected from IoT and non-IoT sources.

Supported by Finding x.x

As an example, transportation and traffic agencies need 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 data exchanges may happen on a limited basis within each agency, but not across other agencies in other jurisdictions. This makes collaboration requiring multiple agencies difficult.

Once a taxonomy is established, government and industry can partner to develop conformance review criteria and methodology, further facilitating the reliable and consistent exchange of information. Projects involving multiple jurisdictions and requiring federal funding should specify the development of a data taxonomy that can be further used and developed by other jurisdictions. It's also important to engage with appropriate industry associations.

Enabling Recommendation ER2.2.3: Promote and adopt industry led standards, guidelines, and protocols for minimum baseline interoperability for IoT technologies to the greatest extent possible.

Supported by Finding x.x

Industry standards and protocols that have a minimum baseline interoperability can help to ensure that devices from different manufacturers can communicate and work together seamlessly. As an example, smart transportation systems focus on safety, so standardization (especially for security and interoperability needs) is vital to ensuring that devices can communicate basic safety information to other vehicles and to/from infrastructure. There are also cases where baseline standards, guidelines and protocols can address existing market fragmentation scenarios particularly in the global market.

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.

Connectivity

Key Recommendation KR2.3: Expand and improve programs that ensure sufficient availability, reliability and connectivity for IoT in all areas of the country.
Supported by Finding x.x

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

By ensuring the availability of suitable and sufficient spectrum resources, encouraging development of wide-area networking technologies, and enhancing interoperability the government can promote accelerated communications innovation. The rapid evolution of communications technology in recent history demonstrates the significant promise and opportunity for the nation to improve IoT connectivity. Current capabilities that were science fiction in the past are now routine in our daily lives. The U.S. must continue such advances to ensure that IoT can securely and reliably communicate and interoperate wherever devices are applied.

Improved communications will also support important sector-specific connectivity needs such as for smart agriculture applications and for sustainable environmental monitoring, especially in areas not services by traditional connectivity.

Enabling Recommendation ER2.3.1: 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

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.[61] The technology industry uses both licensed and unlicensed spectrum to enable this growth. Spectrum availability should not become a choke point in this growth.

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

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

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: 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: Actively promote and support the adoption of satellite narrowband IoT systems, with the aim of improving connectivity, data collection, and decision-making in rural and remote areas, resulting in economic growth.

Supported by Finding x.x

Existing and emerging satellite-based IoT systems provide a reliable and efficient means of connectivity and data transfer in remote agricultural areas where traditional terrestrial connectivity options may be limited or unavailable. Encouraging the adoption of satellite IoT systems will enable farmers to optimize their operations through real-time data management, resulting in benefits for various stakeholders, including farmers, policymakers, agricultural companies, and consumers.

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

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

The government could 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. The goal of this partnership would be to support the development, implementation, and adoption of satellite IoT systems in agriculture.

Other opportunities include defining specific agricultural applications, developing financial incentives and subsidies, and providing incentives or subsidies to facilitate the adoption and integration of satellite IoT systems by farmers and agricultural businesses.

The government should 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: 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 the security, reliability, integrity, and trust of data for the digital economy. By providing incentives for businesses to adopt digital tools, the federal government can help promote ecosystems that create opportunities for businesses and workers in any value chains which will drive economic growth. Furthermore, digitalization enables digital transformation whereby IoT device suppliers become connected to their customers which enables sustainability and circular economy.

The government can assist by working with industry stakeholders to develop and communicate clear guidelines and criteria for eligibility for the subsidies. Agencies could 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.

Enabling Recommendation ER2.4.1: 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 digital or data business ecosystems and trusted digital threads that will enable new business models. Digital networks of interconnected businesses, technologies, and platforms can leverage synergies to enhance existing products, enable digital twins and drive growth through XaaS[49] business models.

The federal government should 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.

This includes:

- Data-driven ecosystems that can create new revenue streams and enhance existing products and services among Interconnected businesses, technologies, and platforms that can leverage synergies in the value chain.
- Data analytics that can provide insights that drive innovation, improve decision-making, and enable data monetization strategies. This can lead to significant benefits across value chains and drive economic growth.
- Trusted digital marketplaces that can promote data sharing and collaboration while business ecosystems lead to better products, solutions, and services that enable new revenue streams.
- Platform-based ecosystems made of connected businesses that can collaborate and innovate more effectively. They can also scale rapidly through network effects and can drive sustainable growth for businesses.
- Data regulations that can provide a framework for businesses to manage and use data responsibly and using tools for monitoring and managing trusted digital marketplaces that ensure transparency and accountability.

Facilitation might include development of educational programs (e.g., through public campaigns, conferences, and workshops) for businesses and individuals to raise awareness about business ecosystems.

Enabling Recommendation ER2.4.2: Lead collaboration with international allies to develop, promote and adopt a Global Digital Identifier that can link to Local Identifiers of businesses, products, and data, to enable cross-border trade, supply chain resilience, and ultimately trusted digital marketplaces. ~~**Develop policies on IoT data confidentiality, management, and digital trust to reduce barriers to IoT adoption.**~~

Supported by Finding x.x

[Revised and proposed by TK] ~~[Need to update in collaboration with Mike and Debbie]~~

Commented [HN(MT21]: Updated with material from TomKat.

The U.S. should lead a collaboration with the EU, allied nations and USTR[62], to develop, promote and adopt a secure cross-border Global Digital Identifier facilitate trade of products, data and applications. A global standard like the Universally Unique Identifier[63] (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, and 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 Identifier standard capable of cryptographically linking to Local Identifiers of businesses, products, and data leveraging existing standards and infrastructure .

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

[62] The U.S.-EU TTC can lead with private public partnership initiatives to develop global standard.
[63] https://en.wikipedia.org/wiki/Universally_unique_identifier

Identifier may also be linked to Local Identifiers that may carry metadata pointing Businesses, Assets, and Data that can be shared at the producer's discretion.

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, end-user products and ultimately data, which the IoT ecosystem will need to operate. By incentivizing producers and consumers to use Identifiers and metadata that enables information exchange where producers determine the level of data sharing, this can foster trusted digital marketplaces and fuel the digital economies in the long run.

~~As IoT digital marketplaces evolve, the formulation of comprehensive data policies becomes imperative for modernizing IoT infrastructure. These policies will address critical aspects such as data privacy, confidentiality, ownership, control, access, licensing, and trust, thereby mitigating security risks and accelerating IoT adoption.~~

~~To capitalize on the monetization potential of data, a modern IoT infrastructure must be established. This infrastructure encompasses security, privacy, data sharing mechanisms, ownership and control frameworks, identity and access management (IAM), data protection protocols, licensing mechanisms, and advanced analytics and AI capabilities. These will help reduce adoption barriers, maximize the value of data, and establish a foundation for sustainable growth in the digital economy.~~

~~Effective data policies wield significant influence over various facets of the digital landscape, including privacy, security, interoperability, transparency, accountability, innovation, and monetization. Inconsistencies or inadequacies in these policies can introduce uncertainty, hampering the growth of digital economies. By modernizing data infrastructure, businesses can drive growth and foster synergistic ecosystems that propel future digital economies forward. Data infrastructure plays a pivotal role in unlocking the economic potential of data, protecting critical infrastructure, and optimizing the operation of smart cities, and transportation networks.~~

~~**Implementation Considerations:** Promote infrastructure for security and privacy, data sharing, ownership and control frameworks, identity, and access management (IAM), data protection, sharing and exchange, and data analytics. Establish policies related to trusted data that need to be created and enforced to ensure compliance with regulatory requirements. Promote essential requirements and guidelines for data privacy, confidentiality, and anonymization. Evolve policies in consultation with industry, academia, civil society, and government agencies and keep them up to date with changing technologies and business models.~~

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: 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: 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 chain networks aims to address the growing concerns around data privacy, security, and the potential risks associated with the increased connectivity and interdependence of IoT systems. While many manufacturers have adopted best

practices, many more have not. By implementing robust cybersecurity measures, the government can help ensure that businesses can confidently adopt IoT technologies in their supply chain operations without compromising the security and integrity of their networks and data.

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

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

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

Enabling Recommendation ER3.1.2: 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).

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.

Enabling Recommendation ER3.1.3: Accelerate the promotion and adoption of IoT technologies to make the electric grid more reliable and resilient.

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)).

Commented [GW22]: This recommendation was approved for inclusion; Steve offered to review and revise the supporting text.

Commented [GW23R22]: Updated information provided by Steve

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.

Enabling Recommendation ER3.1.4: 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 continuing 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: 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 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: 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 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.

Data and Privacy Policy

Key Recommendation KR3.3: The White House and Congress should facilitate/support the development of a Data and Privacy Policy Framework.
Supported by Finding x.x

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

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

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

Congress is identified as a possible participating body that could assist or champion this recommendation. For successful implementation, the U.S. Federal government should consider working closely with States that have already embraced privacy frameworks or are advancing regulations. This collaboration is vital for regulatory

alignment. The government is also encouraged to utilize strategies from the National Cybersecurity Strategy Implementation Plan of July 2013, particularly initiatives focused on cyber regulatory harmonization and increasing agency use of frameworks and international standards for regulatory alignment.

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

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

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

Enabling Recommendation ER3.3.1: 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 ER3.3.2: 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 ER3.3.3: 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 ER3.3.4: 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 ER3.3.5: 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 ER3.3.6: Require IoT Privacy information on new car automobile “Monroney Stickers”.

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 Stickers" for new and used cars. This recommendation aims to leverage the traditional role of Monroney Stickers – known for detailing fuel efficiency and safety ratings – to now also disclose vital information about IoT privacy. This encompasses data collection, retention, sale, and the availability of a universal opt-out feature.

This initiative is primarily driven by the need to enhance consumer protection and address growing concerns over personal data use and sharing by IoT devices in automobiles. The urgency of this issue is highlighted by findings from the Mozilla Foundation's Automobile Privacy Report in 2023, which reveals that all 25 car brands reviewed in this report collect personal data, with most sharing or selling this information. The report further indicates that most brands offer limited control over drivers' data, and many have concerning records regarding privacy breaches. Notably, the report notes that none of the car brands reviewed that participate under the Alliance for Automotive Innovation adhere to voluntary consumer protection principles focusing on data privacy.

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 Cybersecurity and Infrastructure Security Agency (CISA) could play critical roles. Their involvement would uphold the principles of the Automobile Information Disclosure

Act of 1958 and significantly bolster consumer rights in an era increasingly defined by connected technology.

Enabling Recommendation ER3.3.7: 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 ER3.3.8: 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 ER3.3.9: 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: 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

Supply chain and life-cycle-traceability are critical if we are to "trust any of the data in IoT". This means there must be "traceability to ensure trust" in all parts of IoT systems as well as platforms and systems they support and the overall IoT eco-system.

The government should support creation of cryptographically strong architectures and infrastructure that enable supply chain provenance, traceability, and lifecycle management by linking hardware and software bill of materials to the design and manufacturing processes delivering trusted assets and data.

This should incentivize suppliers to develop trusted architectures for supply chain provenance, traceability, assurance of supply and IoT product lifecycle management. By cryptographically linking trusted SBOM[64] to trusted HBOM[65] in any IoT device or system, industries can help mitigate the risks associated with supply chain security, compromised components, and ensure the security and reliability of critical systems.

This will strengthen national security, public safety, and economic stability, making it a valuable investment for the government and society such that the use of trusted architectures for supply chain provenance and traceability can help mitigate the risks associated with vulnerabilities or compromised components. Trusted architectures for supply chain provenance and traceability can increase the trustworthiness of critical IoT systems, which is key for national security, public safety, and economic stability. Foster collaboration between government agencies and industry stakeholders (Private-Public Partnerships) to develop and promote trusted architectures that support secure protocols for provisioning and market access.

[64] Software Bill of Materials for Electronic parts and Software modules used in the assembly of a device or complex system.
[65] Hardware Bill of Materials must include a Root of Trust with a source of Entropy such for security and unique ID (fingerprint).

Enabling Recommendation ER3.4.1: 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

The federal government should implement incentives to promote collaboration for trusted end to end solutions, including enterprise business processes and workflows cryptographically linking tasks, personas, and handoffs of IoT assets and data among participating stakeholders. Incentivizing enterprises IoT to adopt trusted digitalization solutions with cryptographic tracing is strategic to enhancing national security, stimulating economic growth, and positioning the US as a global leader in IoT. The term "trusted" indicates that IoT parts, systems, applications, and supply chains operate as intended and produce data that is not tampered or compromised.

Digitalization will allow industries to adopt capabilities for design, manufacturing, and enterprise workflows that cryptographically enterprises in IoT supply chains. The federal government's active role in promoting these capabilities can contribute to more resilient supply chains and valuable end-to-end solutions, that benefit societies and industry ecosystems. By encouraging industries to pursue trusted digitalization solutions, the government can strengthen national security and accelerate adoption and growth to:

- Ensure the confidentiality and integrity of IoT electronics to prevent attacks in critical infrastructure and protect against human and economic losses.
- Accelerate IT/OT convergence with adoption of trusted traceability methods for IoT electronics that enhance the effectiveness of critical infrastructure services.
- Enable businesses to foster innovation and create a competitive advantage using smart-connected IoT Systems to become smart-connected suppliers.
- Enable the creation of trusted ecosystems that accelerate end-to-end innovation, monetization, and growth of IoT-enabled digital economies.

Specific methods to implement could include:

- Offering tax credits, grants, or other financial incentives to companies that market electronics products with traceable parts Country of Diffusion and Country of Origin[66], provenance, and journey in the supply chain.
- Requiring suppliers to adhere to specific security and traceability standards when bidding on government contracts, particularly for critical infrastructure.

[66] Country of Diffusion where a part is fabricated and Country of Origin where the product made of parts is assembled.

- Establishing a certification process for electronics and IoT products linked to cybersecurity labels, security, and traceability standards to increase trust.
- Engage industry associations, businesses and tech hubs to develop best practices and guidelines for trusted IoT electronics and systems development and supply chain.

Enabling Recommendation ER3.4.2: 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 twins[67] and digital threads[68] 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.

Digital twins are virtual models of physical assets, which are proven to shorten the manufacturing process by using AI to improve efficiency. IoT platforms with sensors deployed in manufacturing produce data used for AI and analytics across supply chains[69]. The government should support the development of digital threads across supply chains by incentivizing companies to digitalize their workflows, starting from design and manufacturing.

The government should promote digitalization in supply chains by incentivizing companies to digitize workflows, starting with design and manufacturing. By integrating IoT Bills of Materials and data identifiers, certified digital threads can be created, facilitating trusted digital marketplaces and platform-based ecosystems. This approach enhances supply chain visibility, efficiency, security, and growth, extending from supply chains to IoT device usage.

Connecting digital threads across supply chains can safeguard proprietary IP while fostering new digital marketplaces, driving revenue streams and enhancing end-to-end visibility. This leads to reduced cyberattack risks, counterfeiting, and product recalls, while improving supply chain efficiency, cost management, vulnerability handling, differentiation, and innovation.

[67] 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.
[68] Digital flow of data connecting business processes products assets and bill of materials in a value chain. For the electronics value chain the digital threat includesof HBOM, SBOM and other Digital Bill of Materials (DBOM)
[69] McKinsey & Company - Reimagining fabs: Advanced analytics in semiconductor manufacturing

Fostering an IoT-Ready Workforce

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: 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.[70]

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.

[70] Highway Funding for Workforce Development. U.S. Department of Transportation. Link.

2. **Lifelong education and development of existing and new worker bases.** This can be done at a variety of levels and means - vocational training, community college and university training, and continuing professional education. Workforce development efforts include reskilling and new skills development, upskilling, and continuing professional education.

3. **Workforce Placement.** Once the workforce is trained or retrained, they need to be placed in industries across the economy. Specific areas of need include those industries that have not traditionally been digital or have hired digital talent (e.g. mining, construction, etc.) and in geographic areas of the country with significant shortages of digital workforce (e.g. rural areas, small towns, etc.). This includes new workers, as well as those reskilled from other industries.

4. **Workforce Retention.** Initiatives to retain workers who have been trained from leaving the industry or their roles.

The federal government should also consider "student loan forgiveness" programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies. These programs, analogous to the National Health Science Corps, provide expertise to municipalities, agencies and utilities, especially smaller ones, 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: Review the National Cyber Workforce and Education Strategy and align and integrate any special or unique needs and considerations of the IoT workforce. (Updated)

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: Collaborate with industry, academia, and state and local government to create an IoT trained workforce embedded in target high priority industry sectors. (Updated)

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: Collaborate with industry, academia, state and local governments and private investors to create and place workforce in industries and areas of opportunity. (Updated)

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.

Government Support to Facilitate 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: Consider new financial models for sustaining and supporting programs when considering 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: 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 consider models to help select adopting organizations sustain and support beyond the initial acquisition and building of new projects incorporating IoT technologies. While grants for projects help offset the initial cost of capital procurement, integration and development, the cost of operating the asset or system is left to the organization, municipality or agency. Some select organizations have the resources, funding models, or mechanisms to find the resources to sustain the operation and maintenance of this asset or system. However, many other organizations, especially the smaller ones, or those in rural and tribal

areas, that benefit from these technologies the most, do not have these mechanisms (budget, taxes, etc.), and may forgo these types of projects, or only operate the IoT applications short term until the funds run out. Similarly, current agency grant application evaluation criteria may screen out those that don't meet the financial requirements for sustaining operations.

For existing grant programs, consider extending funding for operations from one to two years for applicants that meet specific criteria of those that can benefit from IoT but could not otherwise sustain it (rural areas, tribal areas, small cities and towns, etc.) Regional models: Incorporate models that encourage regional partnerships. For example, one small community may not have the means to sustain a small IoT application. But if multiple adjacent communities apply for a grant together, they may be able to leverage some economies of scale to purchase and set up the application but may be able to employ synergies and cost sharing to maintain the application together. Innovative partnerships: Incorporate criteria that encourage and reward innovative approaches to sustaining operations. For example, one city was able to sustain operations by implementing a "support a AQ node" and getting corporate sponsors in the business community to support the maintenance and operation of the network.

Enabling Recommendation ER5.1.2: Develop programs and grants to help underserved and less developed communities benefit from IoT adoption.

Supported by Finding x.x

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

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

The government will need to identify appropriate tactics and methods, such as ADA-compliant EV Charging stations, adding EV-Ready language into building codes, opportunities for small- and disadvantaged businesses, or Department of Transportation (DOT) Grand challenges as programs/grants are developed. Clear eligibility criteria should be established to ensure that these grants/incentives are

targeted only at these types of communities and areas. The federal government should establish a system for monitoring and evaluating the effectiveness of these grants and incentives.

Leading the Way for IoT Adoption in Agriculture

Key Recommendation KR5.2: 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: 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

The proposed initiative advocates for the federal government to allocate sufficient funding to implement a "farm of the future" setup in a representative set of universities across the United States, providing a showcase for farmers in the region on how to collect and analyze data from their farms. In seeking candidates for the "representative" universities, consideration should be given to diversity of climate, soil, and other farming conditions. Land grant universities, including the several HBCU that fall under this category, are logical candidates.

The data collected by the IoT network could be used to develop and refine machine learning algorithms, which could help farmers predict future crop yields and identify potential issues before they occur.

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

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

It is difficult to specify what IoT technologies should be acceptable to be used. Some concrete and specific IoT applications should be defined for inclusion in the project and funding requirements, based on project types. "Farm of the Future" efforts should look to assist in determining what IoT technologies should be acceptable for use. This may require coordination with other federal agencies in alignment with their objectives. Different such universities might pose different challenges with respect to implementation, including connectivity, tech readiness, etc.

Enabling Recommendation ER5.2.2: 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: 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 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: 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: The government should implement specific actions to further promote IoT adoption through smart communities.

Supported by Finding x.x

Enabling Recommendation ER5.3.1: 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 and 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: 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: 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 build-outs.

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: 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 to no ability to communicate with each other and other city systems. This limits the ability of the city to monitor conditions, automate operations, respond quickly, effectively and efficiently.

Enabling Recommendation ER5.3.6: 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: 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: Promote IoT adoption that will improve public safety.

Supported by Finding x.x

Enabling Recommendation KR5.4.1: Create a stockpile of public safety IoT devices that is available for immediate access.

Supported by Finding x.x

[Note: Revision Pending.]

Enabling Recommendation ER5.4.2: **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 ER5.4.3: 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 ER5.4.4: Create a program that 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 serves 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, 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, etc.) and guidance of what IoT applications this grant would help procure. Grants offered should support or integrate into, as relevant and applicable, next gen 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 for 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: Promote IoT adoption in the health care industry.
Supported by Finding x.x

Enabling Recommendation ER5.5.1: 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: 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

[Update bullets to prose but otherwise ok]

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: 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 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).

Enabling Recommendation ER5.5.4: Facilitate the adoption of AI in IoT in healthcare through improved AI research, development and workforce improvement.

Supported by Finding x.x

While AI can help automate the analysis of massive amounts of IoMT data, and other data collected from health records, its ability to create explainable, beneficial and personalized outcomes specific to the patient that are clinically appropriate, reliable and accurate is a major challenge. For healthcare devices, it is important for Edge AI technologies to not require high bandwidth connectivity with backend cloud services to allow acceleration of adoption in many use cases, such as rural locations and healthcare facility lower levels. Edge AI devices are not accessed remotely, therefore, are not intercepted by malevolent actors.

AI algorithms review and analyze data, and make recommendations and in cases requiring autonomous operations, take action. Diagnosing people and identifying treatments for people is complex. Diseases such as cancer are complex, and there is still much to be learned. Furthermore, each person has a different reaction to treatments and what works for one person may not work for another. AI generated recommendations may yield treatment recommendations that lead to adverse outcomes, including injury and death. There are a variety of reasons AI may lead to negative or unintended outcomes, including data that may be outdated, contains bias, or incomplete. The source of the data may be unknown for privacy reasons. While the AI algorithms have been trained on this data, the reasons it led to a specific recommendation may not be explainable and transparent. This leads to a loss of confidence in the AI's ability to analyze the data accurately and reliably.

Along with cloud services and IoT specific requirements, provide equal, if not more focus, incentives, R&D grants and awards for edge networks and peer-to-peer capabilities. For the healthcare industry more specifically, rather than the general tendency to focus on IoT to cloud interfaces only, institutions require digital health data to be processed at the edge, minimizing the amount of information exchanged with central servers and the cloud. This approach will significantly increase the privacy of digital health data.

Enabling Recommendation ER5.5.5: 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: Promote IoT adoption that will improve sustainability and environmental monitoring.

Supported by Finding x.x

Enabling Recommendation ER5.6.1: 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. As described in other recommendations throughout this report, improved interoperability and competitiveness will help benefit all IoT adopters, and an open model for shared and consistent data will help take strides toward those objectives. 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.

Enabling Recommendation ER5.6.2: 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: 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 could also 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.

Enabling Recommendation ER5.6.4: 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.

Enabling Recommendation ER5.6.5: 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 critical to ecological health, public safety and disaster recovery. For example, a dense network of low cost IoT-enabled gas sensors can be used in conjunction with a network of cameras to detect and pinpoint wildfires. Early detection of wildfires in remote forests allows firefighters to direct resources to the initial location, increasing the odds of combating the fire before it becomes widespread. A network of IoT-enabled air quality, earthquake, and other sensors integrated together allow state and regional agencies to build real time situational awareness capabilities to support and plan activities that preserve ecologically sensitive areas, mitigate, respond and recover from natural and man-made hazards.

Smart Transportation

Key Recommendation KR5.7: 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: 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)

Facilitating 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: Monitor and evaluate progress of IoT adoption for supply chain logistics.

Supported by Finding x.x

The government should provide an intentional process to monitor and evaluate progress to provide assurance that IoT adoption efforts in supply chain logistics are on track, effectively addressing identified challenges and opportunities, and delivering

desired outcomes. The need to monitor and evaluate progress in IoT adoption for supply chain management stems from the need to ensure the effectiveness of implemented strategies, measure their impact, and identify areas for improvement.

By regularly monitoring and evaluating the progress of IoT implementation, the government can identify areas of improvement, assess the impact of its policies and initiatives, and make informed decisions to optimize its strategies and investments in the future. Monitoring and evaluating progress involves establishing a set of measurable indicators and targets that reflect the key objectives and desired outcomes of IoT adoption in supply chain management. These indicators may include the level of IoT technology adoption, efficiency gains, cost reductions, improvements in transparency and traceability, and advancements in cybersecurity, among others.

Regular assessments should be conducted to track the progress of IoT adoption against the established targets, identify any gaps or challenges, and evaluate the effectiveness of the implemented policies and initiatives. Based on the findings of these assessments, the government should adapt its strategies and actions to address the identified issues, optimize resource allocation, and maximize the impact of its efforts. By monitoring and evaluating progress, the government can ensure that its approach to driving IoT adoption in supply chain management remains agile, responsive, and results-oriented, ultimately contributing to the long-term success and competitiveness of the industry.

Implementation Considerations:

- Establish clear goals and objectives: Define specific, measurable, and time-bound goals and objectives for IoT adoption in supply chain management to enable effective monitoring and evaluation.
- Develop relevant performance indicators: Identify key performance indicators (KPIs) that reflect the desired outcomes of IoT adoption and can be used to measure progress and impact.
- Implement data collection and reporting mechanisms: Set up systems and processes for collecting, storing, and analyzing data related to IoT adoption and supply chain performance.
- Conduct periodic assessments: Schedule regular evaluations of progress and impact, using the collected data and KPIs to assess the effectiveness of IoT initiatives in supply chain management.
- Foster a culture of continuous improvement: Encourage feedback and learning from monitoring and evaluation results, using the insights to improve and refine policies and initiatives.
- Collaborate with stakeholders: Engage with industry, academia, and other relevant stakeholders to gather their insights and perspectives, ensuring a comprehensive understanding of progress and challenges.

- Assign responsibility: Designate a lead federal agency or interagency group responsible for overseeing the monitoring and evaluation process for IoT adoption in supply chain management.
- Develop a monitoring and evaluation plan: Create a detailed plan outlining the goals, objectives, KPIs, data collection methods, and evaluation schedule.
- Allocate resources: Ensure adequate financial, human, and technical resources are allocated to support monitoring and evaluation activities.

Enabling Recommendation ER6.1.1: 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: 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 build new manufacturing capacity, develop new 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.

The government should review federal domestic preference requirements that may be time consuming and costly, particularly when it comes to the country of origin of components and subcomponents. This burden will increase as subcomponents become smaller and more integrated, so this review is urgently needed.

Public and Private Partnership

Key Recommendation KR6.2: 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. The resultant platform would foster collaboration and knowledge exchange, stimulating the development, deployment, and wider adoption of IoT technologies in supply chain management.

PPPs can address common barriers to IoT adoption, including infrastructure gaps, limited technical knowledge, and financial constraints. By aligning efforts and pooling resources, these partnerships can drive the innovation of IoT solutions, initiate pilot projects, and roll out proof-of-concept initiatives that demonstrate the value and benefits of IoT in supply chain operations. Additionally, they can contribute to workforce development by creating and supporting training programs, potentially in collaboration with technical colleges and universities.

They also play a role in establishing industry standards and regulatory frameworks conducive to IoT adoption across the supply chain industry. This would involve close collaboration with regulatory bodies like the Federal Communications Commission (FCC) and standard-setting institutions like the National Institute of Standards and Technology (NIST). By fostering such partnerships, the government can nurture a thriving ecosystem that drives innovation and competitiveness in the supply chain sector, maximizing the potential of IoT technologies.

Implementation Considerations:

- Identifying key stakeholders: The federal government should identify relevant private sector stakeholders, including businesses, industry associations, research institutions, and technology providers, who can contribute to the development and implementation of IoT solutions in supply chain management.
- Establishing a collaborative framework: A formal framework should be established to facilitate collaboration between the public and private sectors. This may include creating joint working groups, industry forums, or innovation hubs, where stakeholders can share ideas, knowledge, and resources.
- Defining clear goals and objectives: Public-private partnerships should have well-defined goals and objectives that align with the overall strategy for promoting IoT adoption in supply chain management. This will help ensure that all stakeholders are working towards a common vision and can measure their progress.
- Developing joint projects and initiatives: The federal government and private sector stakeholders should collaborate on joint projects and initiatives that address specific challenges or opportunities in supply chain management. These could include pilot projects, research and development programs, or the development of new IoT standards and protocols.
- Ensuring effective communication and coordination: Open and transparent communication between the public and private sectors is critical for successful collaboration. Regular meetings, progress reports, and information sharing mechanisms should be established to facilitate coordination and maintain momentum.
- Monitoring and evaluation: The federal government should establish a system for monitoring and evaluating the effectiveness of public-private partnerships in promoting IoT adoption in supply chain management. This may involve tracking key performance indicators, such as the number of joint projects implemented, the amount of private investment leveraged, and the impact on supply chain efficiency and resilience.

Enabling Recommendation ER6.2.1: 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

The government should support collaborative IoT platforms that align the business incentives of stakeholders to foster innovation, enable orchestration and while harnessing the power of network effects to enhance security, user experience and drive economic growth. These platforms serve as hubs where various stakeholders,

including device manufacturers, service providers, developers, and end-users, come together to share data, insights, and resources to achieve common goals and benefits.

Collaborative IoT platforms encourage industry-wide innovation, leading to the development of cutting-edge technologies and solutions. These platforms streamline device management, data exchange, and interoperability, reducing operational complexities. By aligning business incentives, stakeholders are motivated to prioritize shared goals, establish mutual interests, and align their incentives to drive collective success. Collaborative IoT platforms help reduce conflicts of interest, foster trust and improve collaboration. IoT-driven industries will experience substantial growth, create jobs, and contribute to economic prosperity.

Implementation considerations include:

- Standardization: Define industry standards to ensure compatibility and interoperability across IoT platforms.
- Public Private Partnerships: Foster collaboration between government agencies, businesses, and academia to drive innovation.
- Data Privacy and Confidentiality: Establish robust data protection regulations to build trust and protect user data.
- Incentive Mechanisms: Create incentives like tax benefits and grants to motivate businesses to align their incentives with IoT platform goals.
- Monitoring and Evaluation: Implement a monitoring system to track progress, security, and the impact on economic growth.

Enabling Recommendation ER6.2.2: Promote the enablement and use of IoT trusted digital marketplaces and platform-based business ecosystems.

Supported by Finding x.x

As digital threads and digital platforms emerge, the government should promote the enablement and use of these tools to drive economic growth with trusted data exchange and licensing while protecting the proprietary IP of enterprises in the value chain.

In the most general case, digital threads are the flow of data that connects business processes, products, and assets across supply chains, networks, or applications. In a narrower sense within the supply chain, each component (chip, software, module, device) has associated information regarding provenance, integrity, version and more. As components are associated with modules and the modules with assembled devices running software, this flow of data through the supply chain has the potential to inform security, product integrity and availability. Ideally, all of this information—

this “digital thread”—is and remains available throughout stages of the supply chain, from original materials through installed systems.

A trusted digital thread benefits from cryptographic protection in each stage and throughout the flow. This information is valuable and can be exchanged in digital marketplaces. The government should incentivize the enablement and use of trusted digital marketplaces where producers and consumers query and share information about assets and related data, enabling better visibility, traceability, and monetization while protecting proprietary IP and PII.

Trusted digital marketplaces can be promoted through pilot programs, best practices and guidelines. Platforms that facilitate adoption of digital marketplaces can enable producers and consumers to reduce costs and improve efficiency. Efficiencies come from streamlining processes and eliminating redundancies, especially in complex supply chains where information flows are often fragmented or disconnected. Furthermore, trusted digital marketplaces driven by digital threads enable participating stakeholders to evolve new business models and revenue streams. When these are combined with business platforms that maximize network effects, it will fuel the growth of ecosystems and future digital economies.

Implementation Considerations:

- Identify standards, taxonomies, and best practices to define supply chain trusted digital threads and marketplaces.
- Identify suitable marketplaces to incentivize and support (e.g., EV charging and monetization). Develop guidelines and incentives for access and use of data.
- Promote the benefits of data marketplaces to potential participants and provide tax credits and subsidies to encourage participation.
- Ensure data security and confidentiality measures are in place. Monitor and evaluate the effectiveness of the data marketplaces. Use analytics to improve visibility, traceability, efficiency, and cost.

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.

Enabling Recommendation ER6.3.1: The government 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. Circular supply chain ecosystems are those sustainable cycles where resources remain as much as possible in the loop of collection and processing, production and purchasing, consumption and use. Key is that resources can be cycled back again in these stages by use of sustainable processes of, e.g., remanufacture or recycling. Use of AIoT can enhance transparency, sustainability, and economic growth by fostering innovation and efficiency which will benefit businesses, the environment and digital economy.

Promoting trusted AIoT platforms within circular supply chain ecosystems is imperative for ensuring transparency, sustainability, and economic growth. This initiative not only fosters innovation but also enhances efficiency, benefiting businesses, the environment, and the future digital economy. By strategically integrating AIoT into circular supply chains, the government can create a foundation for responsible and sustainable technological advancement, positioning the nation as a leader for the global digital economies.

Examples include:

- Innovation Hubs: Promoting AIoT platforms will drive innovation, enabling the development of cutting-edge technologies and solutions.
- Efficiency Boost: AIoT can optimize resource utilization, reducing waste and energy consumption within circular supply chains.
- Environmental Benefits: Sustainable practices fostered by this initiative can help combat climate change and promote eco-friendliness.
- Economic Growth: The growth of AIoT-driven industries will create jobs and stimulate economic development.
- Competitive Advantage: By embracing AIoT, the nation can establish itself as a pioneer in the digital economy, attracting global investments.

Key Recommendation ER6.4: Provide overarching regulatory guidance for the drone industry.

Supported by Finding x.x

Drones integrated with IoT technologies can leverage real time data and automation capabilities to further enhance their functionality and efficiency. The adoption of drone technology can have substantial impacts on the nation's key sectors. In agriculture, for instance, drones equipped with advanced sensors can help in efficient farm scouting, pinpointing areas of pest infestations, disease, or poor irrigation. This not only enhances productivity but also promotes precision farming by reducing the excessive use of chemicals. For the energy sector, drones can monitor electric grids and detect faults or required maintenance, helping to prevent power outages, and ensuring a stable power supply. Similarly, drones can be utilized for environmental monitoring of forests, aiding in early detection of wildfires, and thus mitigating their devastating effects. Drones can also be actuated to perform tasks such as spraying pesticides or fertilizers in farming, reducing human exposure to harmful chemicals, and ensuring that the process is accomplished with greater precision and less waste.

The Internet of Things (IoT) is instrumental in accelerating the adoption of drone technology, including the use of drones in Non-Line-of-Sight (NLOS) operations. IoT facilitates seamless communication and data exchange over the Internet, enabling real-time data collection and analysis, remote control of drone operations, and automation of tasks. This is particularly beneficial for NLOS drone operations, which require sophisticated data communication and handling capabilities. Drones operating beyond visual line of sight can cover larger areas and perform tasks in remote or inaccessible locations, expanding their utility in sectors such as agriculture, energy, and environmental monitoring.

However, leveraging the potential of NLOS drone operations hinges on the establishment of appropriate regulatory guidance for IoT in the drone industry. Such regulations can address critical aspects such as data security and privacy, airspace usage, safety, and accountability for NLOS operations. By providing clarity and assurance, these regulations can stimulate innovation and investment in drone technology, contributing significantly to the economy and society at large. Additionally, there are conflicting regulations that govern drones for recreational pilots versus those that govern drones for commercial pilots. The regulations that govern drones for commercial pilots are put forth by the Federal Aviation Administration (FAA) as they regulate that section of the airspace. Sometimes these regulations are mistakenly applied to recreational pilots. In some jurisdictions there is uncertainty over who regulates the airspace for recreational pilots (FAA versus Local Police).

In addition, there are commercial drone pilots that fly large aircraft in sections of the airspace that fall under Advanced Air Mobility (AAM) jurisdiction. Another issue facing the drone industry is Remote ID — a requirement for a drone to have an internal signal broadcasting the drone's location, latitude, longitude, and heading. Not all drones currently meet this requirement. It will be necessary to involve all stakeholders: such as drone equipment manufacturers, communications providers, among others in developing any type of regulatory guidance. This should be accompanied by expanding access to education and training: particularly on safety aspects related to drones.

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~~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~~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

ML	Machine learning
MVA	Manufacture value added
NAAQS	
NDAA	
NEMA	
NESHAP	
NEVI	
NHTSA	National Highway Traffic Safety Administration
NICE	National Initiative for Cybersecurity Education
NIETC	National Interest Electric Transmission Corridors
NIST	National Institute of Standards and Technology
NITRD	
NOAA	
NSF	National Science Foundation
NSTC	National Science and Technology 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	
SCADA	
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	

Formatted: Space After: 0 pt