Cover Sheet / Front Matter

- List of Board Members / Disclaimers / Note to Readers

Contents

1. Executive Summary

2. Summary of Recommendations of the Advisory Board

2.1. Recommendation #1

A brief paragraph about each recommendation or recommendation topic.

3. Introduction

3.1. Background

Background and brief description (DIGIT Act, FWG, IoTAB)

3.2. Charter and Scope

FACA description, charter and scope

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

4. Methodology

4.1. Approach

- Key assumptions and caveats
- Guiding principles
- Description of approach (and any visuals)

This report reviews sector and cross-sector aspects of the Internet of Things. It is the product of the Department of Commerce National Institute of Standards and Technology's Internet of Things Advisory Board. [More history can be added here]

This report is intended to advise on policy topics for the Internet of Things. It makes sense to stay within a generally common understanding of what that term means. As a group chartered under the Department of Commerce, reference to a NIST technical definition as a starting point is also common sense. However, this report needed to adapt to certain limitations of the NIST definition as explained below. Consequently, this IoT Advisory Board determined early on to define the scope of IoT, and therefore the limits of this work, as follows.

4.2. IoT Definition

IoT Products and Devices: For the purposes of this report, an IoT device is defined as follows.

> *An IoT device is computing equipment with at least one transducer (i.e., sensor or actuator) and at least one network interface. As sold, the full IoT product may be the IoT device bundled with companion applications and backend services that enable essential features. This more complete "product" aspect is generally assumed but discussed explicitly where appropriate. General purpose computing equipment (such as personal computers and smartphones) and general internet and networking infrastructure devices (such as servers, switches and routers) are excluded. Hubs, gateways and protocol translation devices may be part of a system that enables IoT products. Where it is necessary to discuss devices that do not precisely fit these parameters in order to appropriately frame discussion and make recommendations, this report will explicitly note the inclusion of such "non-IoT" device categories.*

This definition was built taking into account the needs of this Board while assembling information and forming recommendations in the context of this effort. There is no intent to define or redefine the Internet of Things outside the scope of these recommendations.

To expand on this definition, the term "Internet of Things" ("IoT") is familiar to those working in, or in connection with, the technology industry. A simple definition of "IoT device" is available from various sources, including well-respected international technical standards. The consensus in the standards community is that an IoT device is essentially a networked computing device that "*interacts and communicates with the physical world through sensing or actuating*." [Editor's note: Cite source: ISO/IEC 20924:2018, 3.2.4] For this definition, the sensing-or-actuating property (or "transducer property") is what distinguishes an IoT device from other networked computing devices (Information Technology or IT devices).

NIST has an equivalent definition,

> "NIST describes an IoT device as computing equipment with at least one transducer (i.e., sensor or actuator) and at least one network interface."

This definition is from a recently published NIST standard, "*Profile of the IoT Core Baseline for Consumer IoT Products*" [Editor's note: Source NISTIR 8425] and derives from earlier work by the IoT Cybersecurity Program team at NIST [Editor's note: Cite source: NISTIR 8259]. Both documents are the product of public-private stakeholder work conducted by NIST and heavily subscribed to by industry. Therefore this transducer criterion is both long-standing and up-to-date, is supported by NIST, and is well-known to industry.

However, this bright-line transducer distinction has limitations. For example,

- A computer server may have a thermal sensor for system shutdown to prevent overheating. The presence of the thermal sensor should not put a server into the IoT category.
- Smartphones are filled with sensors and actuators. Smartphones can be argued as either IoT or IT, but often fall under IT.
- An agency or legislator may group a category of transducer-less connected devices with "IoT devices" to achieve some policy goal.

NIST comments on these limitations in their February 4th 2022 *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* [editor's note: cite https://doi.org/10.6028/NIST.CSWP.02042022-2], where the same definition is paired with a footnote 3 that reads,

> "This description excludes common general purpose computing equipment (e.g., personal computers, smartphones) as well as general internet and networking infrastructure (e.g., internet routers and switches)." [Editor's note: ibid]

Finally, NIST expands on the "IoT device" concept by considering the "IoT product", which includes

> "In many cases, the IoT product may be purchased as one piece of equipment (i.e., the IoT device) but still requires other components to operate, such as a backend (i.e., cloud server) or companion user application on a personal computer or smartphone." [Editor's note: Cite NISTIR 8425]

Therefore, the definition used in this report builds on the NIST definition, which is well-grounded in other technical standards, and adapted to take into account the above factors.

4.3. Examples of IoT Products and Devices

Example	**Is this IoT? *(proposed)***
Connected baby monitor, smart refrigerator	Yes

Internet connected industrial control system (suggest Steve expand on this)	(depends on the component and connectivity, some ICS elements are IoT)
Soil humidity sensor connected by proprietary, non-Internet Protocol radio, to a WiFi-enabled hub	No (suggest we do not look at things without IP capability that bridge to some IP-connected hub)
A WiFi-enabled hub for soil humidity sensors as in the above example	Yes (unlike the item above, this *is* connected to the internet)
Smartphone or laptop	No (IT exclusion)
Consumer router	(Needs discussion – NSC proposes routers be "high risk IoT", yet they have no sensor/actuator and are more commonly IT devices)
Electronic vehicle with 4G/5G connectivity	Yes (but it's a regulated space)
Wearable step tracker that connects via Bluetooth to a smartphone app	No (again, this device goes through a smartphone, like the soil sensor above)

4.4. IoT personas

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

4.5. Analysis Model and Framework

Graphic that organizes the content, including the verticals, horizontal topic areas

5. IoT Technology

5.1. What is the current state

- Discussion of free open source designs (goes to ease of implementation, but "wild wild west" of cyber, IP, etc.)

- Discussion of microcontrollers and microprocessors (goes to complexity, supply chain)
- Discussion of connectivity (WiFi, BT, 5G, LoRa, Matter, etc.)
- Discussion of applications

5.2. What is the future state

- Something regarding AI?
- Emerging trends
- Mid term state/predictions
- Long term state/predictions/projects

6. Detailed Findings of the Advisory Board (Market and application topic areas)

6.1. Smart traffic and transit technologies

6.1.1. Overview

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

6.1.2. Opportunities and benefits (for personas)

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

6.1.3. Barriers (faced by personas to IoT implementation)

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

6.2. Augmented logistics and supply chains

6.3. Sustainable and critical infrastructure

6.4. Precision agriculture

6.5. Environmental monitoring

6.6. Public safety

6.7. Healthcare

6.8. Smart homes (HVAC, security, lighting, etc.)

6.9. Consumer (appliances, TVs, wearables, etc.)

7. Cross market and development topic areas

7.1. Cybersecurity

7.1.1. Overview

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

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

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

7.1.3. Barriers (faced by personas)

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

7.2. Privacy and data ownership

- Data categories (data with PII, data without PII but sensitive, etc.)
    - Privacy considerations and issues
    - Cybersecurity considerations and issues
    - Ownership considerations and issues

7.3. Standards and interoperability

- Local/national/international?
- Enforcement
- Planned or already in place?
- Key activities or organizations involved (representative table?)

7.4. Skills, education, workforce development

7.5. Regulations and commerce

7.6. Policies

7.7. International engagement

8. Recommendations

8.1. Prioritization approach

8.2. General recommendations (recommendations applicable to all areas)

8.3. Market/application topic specific recommendations

8.3.1. Smart traffic and transit

- Recommendation 1
    - Recommendation summary (brief description, agency impacted, priority)
    - Recommendation details
        - Description and objective
        - Example of representative recommendation actions and mechanisms (e.g., contracts, grants, policies, regulations, standards, workforce considerations, research, model agreements, federal collaboration)

- Agencies impacted and what areas
- Timeframe consideration (near, mid, long term)
- Priority (high/medium/low)
- Sector/special considerations
- IoT personas?
- Other recommendation components

8.3.2. Augmented logistics and supply chains

8.3.3. Sustainable and critical infrastructure

8.3.4. Precision agriculture

8.3.5. Environmental monitoring

8.3.6. Public safety

8.3.7. Healthcare

8.3.8. Smart homes (HVAC, security, lighting, etc.)

8.3.9. Consumer (appliances, TVs, wearables, etc.)

8.4. Cross market and development topic recommendations

8.4.1. Cybersecurity

- Recommendation 1
  - Recommendation summary (brief description, agency impacted, priority)
  - Recommendation details
    - Description and objective
    - Example of representative recommendation actions and mechanisms (e.g., contracts, grants, policies, regulations, standards, workforce considerations, research, model agreements, federal collaboration)
    - Agencies impacted and what areas
    - Timeframe consideration (near, mid, long term)
    - Priority (high/medium/low)
    - Sector/special considerations
    - IoT personas?
    - Other recommendation components

8.4.2. Privacy and data ownership

8.4.3. Skills, education, workforce development

8.4.4. Standards and interoperability

8.4.5. Regulations and commerce

8.4.6. Policies

8.4.7. International engagement

9. 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.

10. References

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

11. Acknowledgements

- Include people who spoke to us during meetings
- NIST team

12. Appendices

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

- Glossary of Selected Terms
- Abbreviations / Acronyms
- Other ideas?