Recommendation 6: The federal government should promote and support the development of an overarching guideline developed in a multi-stakeholder process that more clearly distinguishes the major sectors of the IoT for use when dealing with concerns such as cybersecurity.

Description:

The purpose of this recommendation is to create and promote a distinction between IoT, IIoT and Process Sensors and to address the lack of cyber security and trust in legacy process sensors and IIoT devices among multiple stakeholders.

As an example, in December 2022 the Government Accountability Office (GAO) issued Critical Infrastructure Actions Needed to Better Secure Internet-Connected Devices (GAO-23-105327). But the GAO report does not address over 17 million control system cyber incidents despite the importance of actual control system cyber incidents. Agencies and legislators need to clarify that cyber security issues specific to Consumer IoT (and cyber-trust labeling) are not necessarily applicable to Industrial IoT (IIoT) and Process Sensors, nor are they necessarily complete with respect to the IIoT sector. As the US government works with industry on solutions, it is necessary to have common agreement on where these solutions are applicable.

There are 16 sectors under CISA which oversee cybersecurity, some are more regulated than others. Each sector manages their own risks and set of criteria. NIST can provide an overarching guideline that each sector can adapt to their specific profile. This overarching guideline would serve as a reference tool to distinguish the operating environments for the major sectors of the IoT and how cybersecurity concerns or issues would be addressed in a particular sector. For the guideline to be relevant it needs to be developed in a multi-stakeholder process that is open and includes industry participation across the various sectors (i.e., consumer, industrial, healthcare, finance, transportation). This guideline would not necessarily define the major IoT sectors, it is better used as guidance when cybersecurity legislation or regulations are being considered.

An example of a high level writeup that would be included in this guideline that targets the industrial IoT sector is provided below: The Industrial IoT or OT sector leverages existing cybersecurity standards such as the IEC 62443 series of international standards that define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems. Industrial automation and control systems are used in nearly every industrial sector such as manufacturing, transportation, energy, and water treatment industries. There are also several conformity assessment and certification programs that exist for these standards. When legislative or regulatory language is developed targeting this sector, ideally it should reference these standards.

Justification:

The justification an overarching guideline that distinguishes the major sectors of the IoT with respect to cybersecurity concerns is provided below.

- **Use/Scope:** Consumer IoT devices are typically used for personal and home use, whereas Industrial IIoT (IIoT) devices are used in industrial settings for manufacturing, transportation, energy, and other critical infrastructure.

- **Utility:** Consumer IoT devices are generally used for convenience and entertainment purposes, whereas IIoT devices are used for enhancing productivity, improving efficiency, and reducing costs in industrial processes

- **Applications:** Consumer IoT devices are used for a range of applications such as home automation, health monitoring, and entertainment, whereas IIoT devices are used for industrial applications such as monitoring and control of machinery, inventory management, and supply chain optimization.

- **Impact:** Cybersecurity breaches in consumer IoT devices may result in loss of personal data and privacy violations, whereas security breaches in IIoT devices can cause significant damage to critical infrastructure, including production downtime, supply chain disruptions, and safety risks.

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

- **Automation:** IIoT devices are often automated and may interact with other machines and systems, whereas consumer IoT devices are interact primarily with their human users and other consumer IoT devices.

- **Reliability:** IIoT devices must operate reliably and continuously in harsh environments, whereas consumer IoT devices typically operate in more controlled environments.

- **Privacy:** Consumer IoT devices may collect and transmit personal data, and protecting user privacy is a critical cybersecurity concern. IIoT devices may also collect sensitive data, but the privacy concerns may differ based on the application.

- **Interoperability:** IIoT devices are often part of larger systems and must be interoperable with other devices and systems, whereas consumer IoT devices are often standalone and may not require interoperability (although there is a trend towards increased interoperability in certain scenarios)

- **Scalability:** IIoT systems often involve a large number of devices and must be scalable to accommodate growth, whereas Consumer IoT systems may be smaller in scale

- **Regulation:** Legislation or regulations that are developed targeting a particular sector do not necessarily apply across all sectors. IIoT devices may be subject to industry-specific regulations or are already heavily regulated (i.e., healthcare). Consumer IoT devices may be subject to general data privacy regulations.
- **Attack Surface:** IIoT devices 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. Consumer IoT devices may also be vulnerable to similar threats, but the attack surface may be smaller.

- **Criticality:** The cybersecurity of IIoT devices is critical for the operation of critical infrastructure, whereas consumer IoT devices may not be as critical

- **Distinction:** IIoT devices are starting to incorporate Consumer IoT devices (i.e., sensors, cameras) and the distinction between IIoT and Consumer IoT is blurring.

Implementation Considerations:

- **Multi-Stakeholder process:** It’s critical that this guideline development has participation and representation across the relevant IoT Sectors. NIST could convene workshops similar to the process they use with respect to the Cybersecurity Framework (CSF).

- **Utilize the Cybersecurity Framework (CSF):** The CSF guidelines could be extended to distinguish these major IoT Sectors.

- **Use Cases and Examples:** For each Sector that the guideline addresses it needs to rely on existing information from the corresponding sectors (i.e., National Label Program for Consumer Devices-Consumer Sector, FDA requirements for new internet-connected medical devices-Healthcare Sector). The guideline could also include examples from each sector of how they utilize best practices/industry standards to mitigate cybersecurity threats. Harmonization: The guideline could help to promote international harmonization.

Potential implementation barriers:

- **Resource constraints**: Staff resources would be needed to put this together are likely significant.

- **Coordination across government agencies:** Having government agencies reference or point to this guideline could be challenging. Education and outreach would definitely be needed.

- **Existing regulations/legislation/frameworks:** Some states like CA and other nations like Europe already have existing material and there would be a question of how this guideline would align with them.

- **Evolving threat landscape:** As the threat landscape is constantly evolving there are concerns with this becoming outdated and in need of updating.

Possible participating agencies:

The National Institute of Standards and Technology has a role in this recommendation. (Need to consider other agencies: FDA, NHTSA, DOT, DOE, CISA)

References

IoT, IIoT, and supply chain implications in OT and process sensor cyber security
Joe Weiss, PE, CISM, CRISC, ISA Fellow
Presentation to the IoT Advisory Board, April 19, 2023

Recommendation 7: The government should consider additional ways to highlight those vulnerabilities most likely to be applicable to IoT product developers.

Description:

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.

Justification:

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 mentions “identified security vulnerabilities” @58 and “critical patches” @40.

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

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

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

Implementation Considerations:

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

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

Potential implementation barriers:

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

Possible participating agencies:

CISA, NIST