IoT Advisory Board

April 2023 Meeting

Draft – For Discussion Purposes

IoT AB Cybersecurity Subgroup

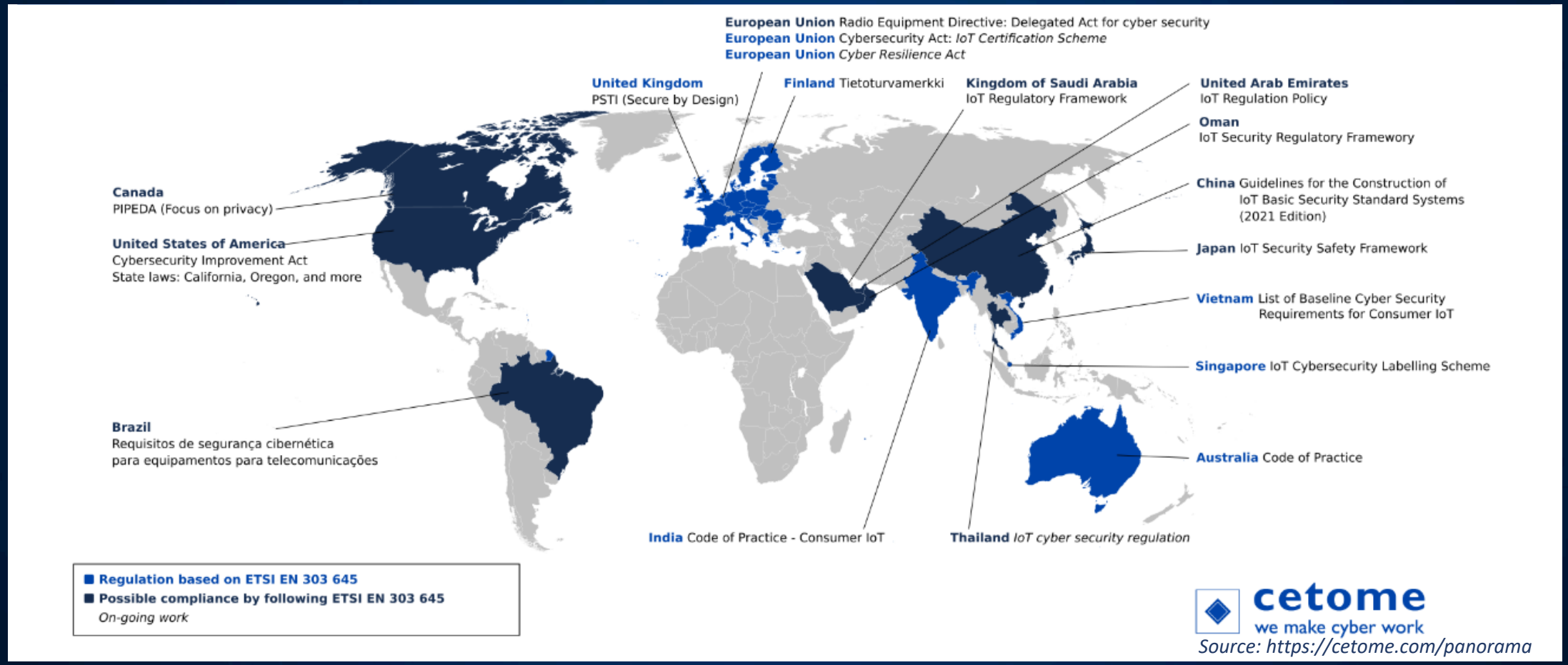
Subgroup Members:

- Mike Bergman
- Ranveer Chandra
- Steve Griffith
- Tom Katsioulas
- Kevin Kornegay
- Pete Tseronis

Consumer Technology Association™

Introduction to the U.S. National Cybersecurity Label Program for Consumer IoT

Ongoing Development of Global Requirements / Labels / Initiatives



Source: https://cetome.com/panorama

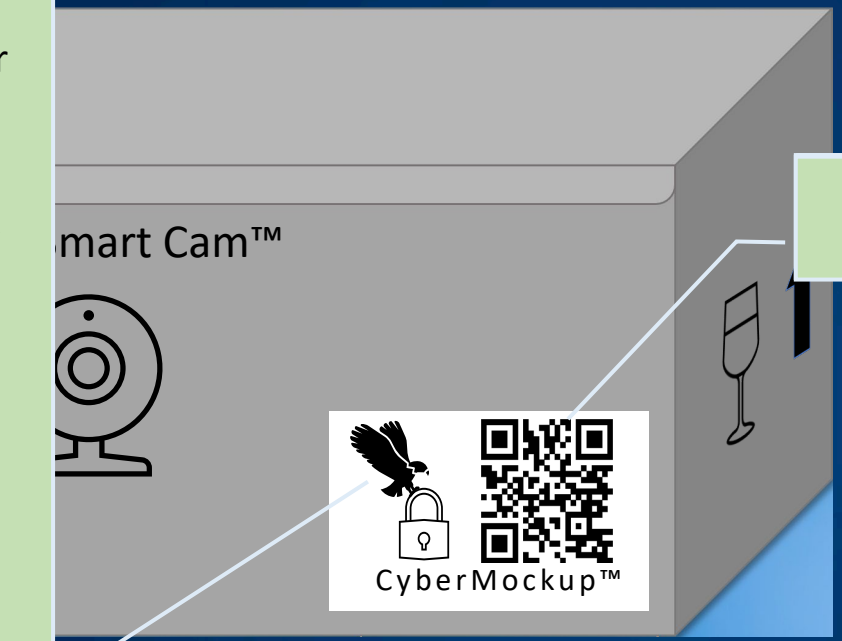
The U.S. National Label Effort – the plan:

1. Create a single common U.S. label (mark).
2. Set criteria for use of the mark.
3. License existing voluntary industry label programs to issue the mark and establish self-attestation path for qualified manufacturers.
4. Promote & advertise domestically / Negotiate internationally for recognition

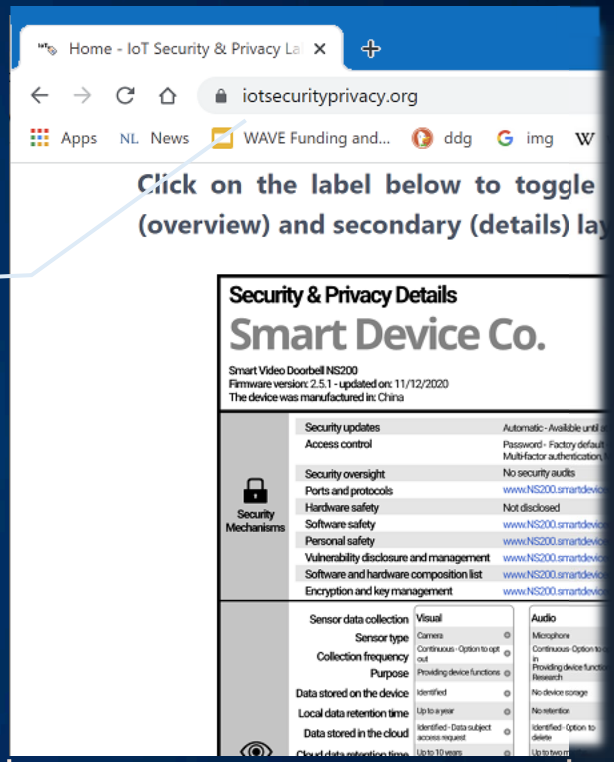
- *This is a voluntary program—not a regulatory requirement.*

“1. Create a single common U.S. label”

- Limited on-package “footprint” to allow for small products
- Comprehensive online info available from link
- Trademarked element enables legal protections
- Follows industry practice for safety or compliance “certification” marks



Link to information



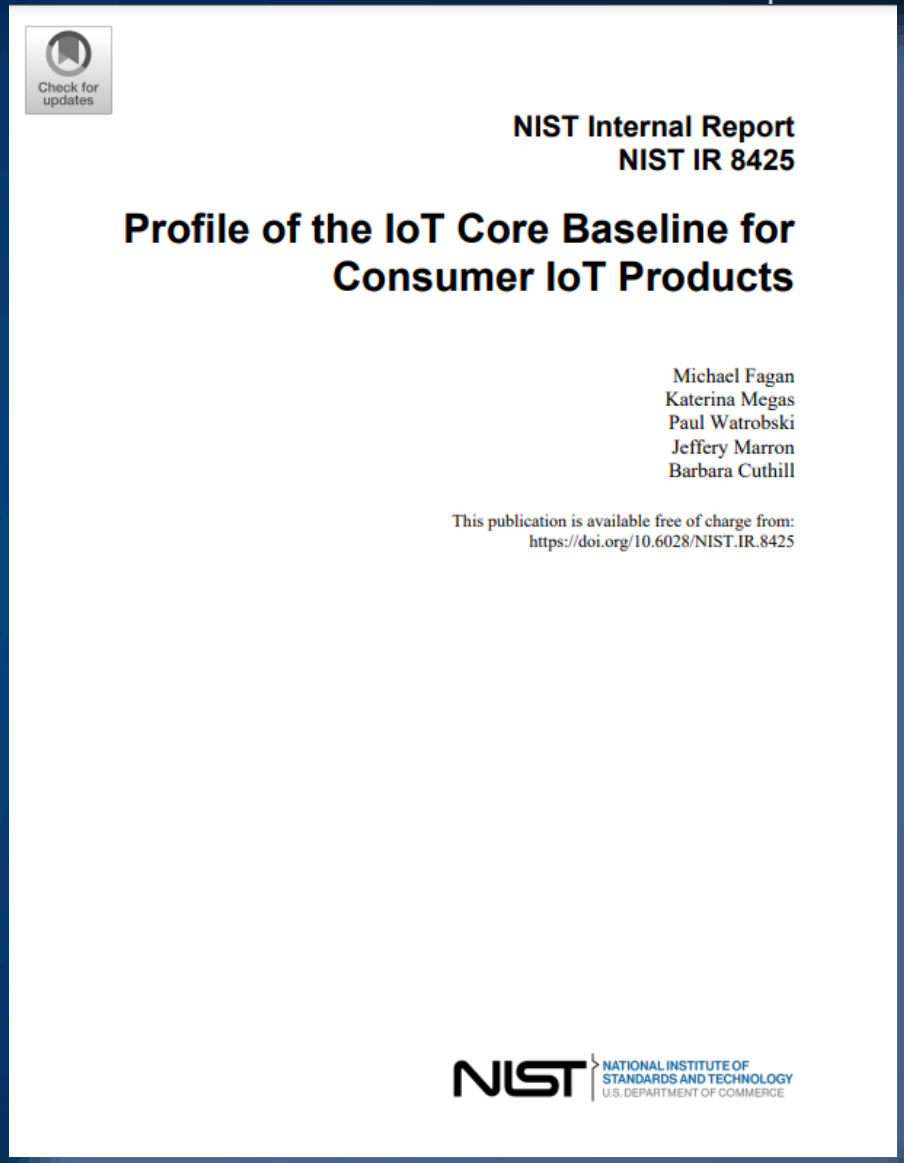
Trademarked element

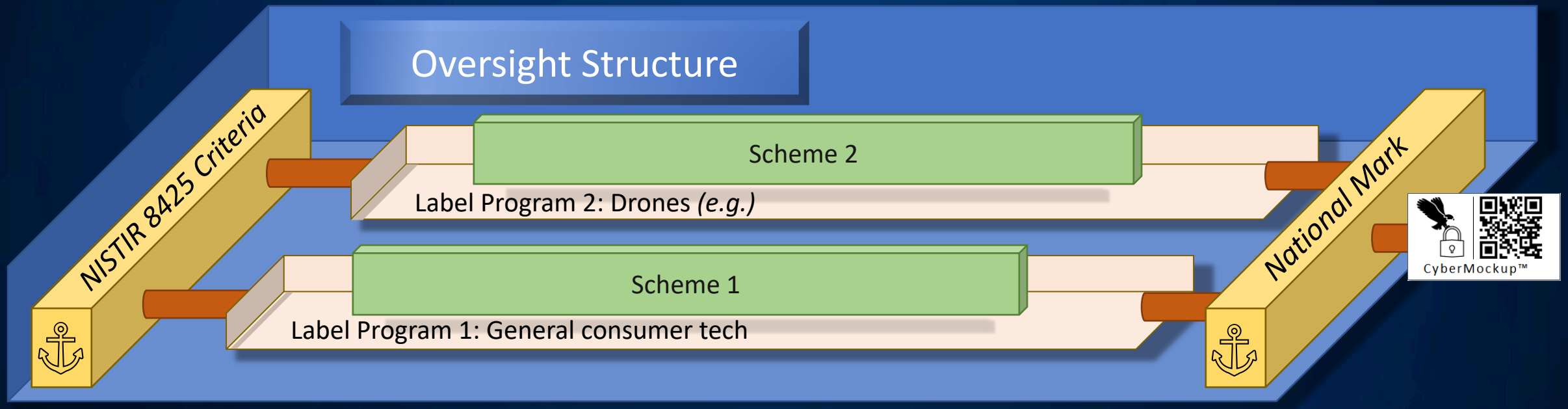
On-package label

Online details:
1) Landing page is consumer-friendly
2) Secondary page is more technical

“2. Set Criteria for Use of the Mark”

NISTIR 8425 is generally accepted by the US government and by industry as the US requirements for consumer IoT cybersecurity label programs.





"3. License existing voluntary industry label programs to issue the mark and establish self-attestation for qualified manufacturers."

Consumer Technology Association™

April 2023 Subgroup Update

Proposed Cybersecurity Section Content – General

- Major sectors of IoT—cybersecurity considerations
- Legacy IoT devices (e.g., OT space, smart buildings, consumer)
- Role of chip-based security (incl. TPM and secure device architectures)
- Attack vectors in an IoT Context
- Linkage between security and privacy
- Security and Traceability
- National Cybersecurity Label for Consumer Connected Devices
- Policy Topics
- Issues
- Solutions, Activities and Opportunities

From March 2023 Meeting

Proposed Cybersecurity Section Content – General

April 2023 Meeting

- More emphasis is needed on the linkage between security of devices and user privacy.
  - How do we address the privacy concerns around the data collected by the devices, especially consumer privacy in confined spaces - e.g., home, car? When a connected device is in close proximity to a user, data is collected.
  - We are looking for information on initiatives like NSF's SPLICE collaborative research; enhancing collection of performance information while also placing a focus on security and privacy of consumer IoT devices.
  - How to address the disconnect between hardware and privacy? It is sometimes unclear who is responsible for addressing privacy concerns (e.g., device or application).
  - Privacy must be dealt with across the ecosystem, but the concern starts at the edge as the data is collected by the IoT device. There are policy issues but also design concerns to make devices more privacy aware.
  - Generally, this group will deal with privacy as a cyber topic in the context of device data collection. The broader privacy topic will continue to be the purview of the Privacy subgroup.
- We are reviewing the National Cybersecurity Label for Consumer Connected Devices (White House Initiative).
  - This is a foundational element for IoT and can be extended beyond consumer. Some of our priorities can be addressed, at least partially, via such a structure. In other words, more will need to be done, but this program can help in multiple areas.

Proposed Cybersecurity Section Content – General

- The subgroup will distinguish between major sectors of IoT.
  - E.g., industrial control /operational technology has unique concerns for security which are different from consumer devices; some sectors (e.g., health care/medical) are heavily regulated.
  - These distinctions are important when considering policy topics.
- Security should be from the chip inside.
  - After dealing with 'baseline' security (as in the U.S. National Cyber Label program), we consider stronger security opportunities.
  - Hardware computing components (microprocessors/controllers/memory) are making progress but are not the same across the board. There are relevant standards for security at the chip level which may be promoted. We need to distinguish use cases / market segments, but hardware components are at the root of advanced security opportunities.
  - The sensor level currently (typically) has no security. This may be due to cost.
  - Traceability is needed for full security (avoid counterfeits, especially malicious ones).
  - Use cases will lead to a different level of security depending on power, performance, market sector, risk assessment, etc. Security frameworks should appreciate differences in types of devices. How do you address the risks associated with devices and incorporate into your ecosystem ?

Proposed Cybersecurity Section Content – General

- Legacy IOT devices must be addressed. The large installed base of susceptible devices will be a problem for years and some incentives to trade out should be considered.
- In the OT space, smart buildings, manufacturing, are systems that are open systems with no security.
- We will highlight TPM (Trusted Platform Module) technology and secure device architectures, esp. for critical infrastructure.
- We will seek more information on secure elements that can enter at the low end.
- We will be defining certain new attack vectors, e.g., battery attacks (Battery draining attacks against edge computing nodes in IoT networks).
- There is interconnection between security and traceability; we are likely to address this in a supply chain-linkage paragraph.

Barriers

- Lack of trust in connected devices support for consumer privacy and security
- A large installed base developed under existing norms
- Fragmentation in the global ecosystem with regard to a growing patchwork of requirements domestically and internationally
- Evolving capabilities of malicious actors

Potential Opportunities

1. Address device collection and storage of data locally.
   - Once the data is exposed beyond the device, it is more clearly a topic for the Privacy subgroup.
2. Study the challenge of legacy IoT devices, the “installed base” issue
   - E.g., SCADA systems that interface with process sensors
3. Promote resolution of fragmentation in the global ecosystem
   - Organizations increasingly must comply with multiple regulatory regimes
4. Improve transparency
   - Required for building trust
5. Improve traceability
   - Trusted devices v. secure devices
6. Look to address evolving attacks
   - E.g., battery draining attacks

Potential Solutions and Activities

1. Consumer IoT (national consumer cybersecurity label effort) and e-Labeling
2. Security by Design (Secure Development Life Cycle)
3. Built-in security in products and systems (co-design: HW/FW hardware and firmware, and SW/OS software operating system/apps)
4. Harmonization to address global fragmentation.
5. Market incentives for implementing cybersecurity
6. Other technologies being deployed in industry (TPM, e.g.)
7. Training and workforce development- things that are specific to cybersecurity with a linkage back to the workforce subgroup.

Draft Recommendations – National Cybersecurity Label

Recommendation 1: Engage with Industry

Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of this program.

Recommendation 2: Keep Voluntary

Conformance to any specific set of requirements should be voluntary.

Recommendation 3: Support Current Roles

Continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.

Recommendation 4: Create Further Incentives

The Administration should encourage Congressional support to deploy this program, including establishing incentives for manufacturers to participate.

- Congress should support earned safe harbors for participants, as protection from civil actions that may occur despite good-faith efforts by compliant industry participants. *(Define "industry participants in body text.)*
- Congress should support preemption of the emerging patchwork of state laws on IoT cybersecurity, which will be critical to encouraging industry participation.
- Clearly establish that the mark is sufficient to meet government procurement requirements as appropriate to the risk assessment of the application.
- The U.S. government agency overseeing the program, with assistance from other U.S. agencies and offices, should engage in negotiations with counterparts in allied nations regarding equivalence or mutual recognition.
- Promote coordinated agency efforts with regard to consumer education and awareness, to avoid mixed messages coming from different parts of the U.S. government.

Draft – For Discussion Purposes

Recommendation #1 (details)

Recommendation 1

Engage with Industry

Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of this program.

Justification

As the NSC-hosted workshop (Oct. 2022) demonstrated, it is possible to establish a national label program quickly and at scale, provided existing ecosystem mechanisms are used.

Efficiently using these processes requires taking advantage of industry expertise. Continued industry engagement as the program is scoped, planned, and executed will be critical to the program's success.

Recommendation #2 (details)

Recommendation 2

Keep Voluntary

Conformance to any specific set of requirements should be voluntary.

Justification

At this time, there is general consensus that conformance to any specific set of requirements should be voluntary. Market incentives continue to grow, and there is increasing interest in this program based on the participation by industry, consumer advocates and academia. Further incentives from the USG will drive more participation.

Recommendation #3 (details)

Recommendation 3

Support Current Roles

Continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.

Justification

Until now, NIST's role has been to develop for the entire IoT ecosystem. Industry subject-matter experts have participated in further developing NIST requirements for their specific sectors. 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.

Recommendation #4 (details)

Recommendation 4

Create Further Incentives

The Administration should encourage Congressional support to deploy this program, including establishing incentives for manufacturers to participate.

Justification

Increasing market incentives will be enhanced by introduction of the label program, but only if manufacturers participate. There is strong interest now but the Administration and Congress can accelerate adoption with earned safe harbors, preemption of mismatched state laws for program participants, negotiation of mutual recognition or “equivalence” opportunity across borders, and coordinate agency efforts with regard to consumer education.

Discussion