IoT Advisory Board

May 2023 Meeting

Draft – For Discussion Purposes

IoT AB Cybersecurity Subgroup

Subgroup Members:

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

May 2023
Subgroup Update

Draft Recommendations – National Cybersecurity Label

Recommendation 1: Engage with Industry On IoT Product Certification Programs

Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices ~~this program~~.

Recommendation 2: Keep IoT Product Certification Programs **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 For IoT Product Certification Programs

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

Draft Recommendations – (new)

Recommendation 5: Upgrade Federal Buildings

The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

Draft – For Discussion Purposes

Recommendation #1 (details)

Recommendation 1

Engage with Industry On IoT Product Certification Programs

Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices

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.

Note that the consumer version should be launched as of this Report publication, but that other categories will be under development.

Draft – For Discussion Purposes

Recommendation #2 (details)

Recommendation 2

Keep IoT Product Certification Programs **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.

Draft – For Discussion Purposes

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.

Draft – For Discussion Purposes

Recommendation #4 (details)

Recommendation 4

Create Further Incentives

For IoT Product Certification Programs

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.

Draft – For Discussion Purposes

Recommendation #5 (details) (new since April)

Recommendation 5

Upgrade Federal Buildings

The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

Justification

- These buildings are reliant on control systems which provide the functional, operational, and safety needs of a building. These can serve as gateways for malicious actors who can take control of critical lifesaving applications with a building (i.e., heating, air conditioning, physical access).
- Data that resides on an unprotected building control system that contains personal and confidential information could be used against an individual.
- Credibility and assurance can be provided to the private sector when the Federal Government leads by example.
- Buildings that have their connected systems upgraded could save money on cyber insurance premiums.

Draft – For Discussion Purposes

Discussion