Recommendation 1: Prioritize broad and active industry engagement when developing and maintaining the government-sponsored portion of the U.S. national cybersecurity label for connected devices.

Description:

The initial U.S. cybersecurity label program focused on consumer product with expectations of growth into other sectors. The federal government should continue to engage industry in determining operational aspects of this program. Many aspects will require detailed business processes, license agreements, and compliance actions on the part of ecosystem participants; these have been and should continue to be developed using industry expertise in this topic.

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.

Implementation Considerations:

- Existing label programs vary; the more flexible the government can be in qualifying the process rather than dictating it, the better.
- Process qualification should be outcome-based rather than centrally determined. These outcomes determine the need for trust mechanisms such as meeting the NISTIR 8425 Criteria and having industry-accredited processes.

Potential implementation barriers:

- There may be a perceived advantage in defining a uniform U.S. government scheme rather than defining the necessary outcomes from various industry schemes.

Possible participating agencies:

The "Program Owner" is yet to be announced as of this writing. Update this section after May 31st 2023.

-

Federal considerations:

- Update after May 31st 2023.

Recommendation 2: Conformance to any specific set of requirements should be voluntary.

Description:

The U.S. national label for connected devices was conceived of as a voluntary program. The National Cybersecurity Strategy discusses the program in Pillar 3 without mention of regulation *per se*, but also calls strongly for regulation and mandatory requirements in most other areas.

Justification:

- At this time, there is general consensus that conformance to any specific set of requirements should continue to 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.

- Depending on the Program Owner, a pivot from voluntary to mandatory risks changing the focus in industry from developing and supporting this program, to debate over authority. Such a debate will likely stall progress despite current momentum in industry.

Implementation considerations:

- Depending on the Program Owner,

Potential implementation barriers:

- Depending on the Program Owner,
-

Possible participating agencies

- All federal agencies that have enforcement authority in this space (e.g., FCC, FTC, CPSC, others).

Federal considerations:

- Depending on the Program Owner,
-

Recommendation 3: The federal government should continue to support NIST as the developer of outcome-based requirements that inform industry consensus standards, and industry as the developer of those standards.

Description:

The roles defined…

Justification:

- 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.

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- tbd

Federal considerations:

- tbd

Recommendation 4: The Administration should encourage Congressional support to deploy this program, including establishing incentives for manufacturers to participate.

Description:

Participation in the U.S. cybersecurity label program began 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. Other potential incentives include relief from a patchwork of state requirements via a federal preempt and a successful negotiation of mutual recognition of U.S. marks with other nations and the EU. Coordinating agency messaging to ensure “one voice” on these label and certification programs to the private sector is also important.

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.

Implementation considerations:

- Incentives may require legislation. However, there are a range of other options. For example, … *[Edit: Mike to provide text. It is being checked at this time.]*

  In the context of FTC authority, here are several options for such a statement, in a general descending order of strength/clarity:

  [Edit: Mike to provide list (it is being checked as of this writing)]

  In the same vein, other agency authority contexts will have similar options.

Potential implementation barriers:

-

Possible participating agencies:

- CPSC, DOE, FAA, FCC, FTC, FDA, NHTSA

Federal considerations:

Recommendation 5: The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems.

Description:

The federal government should consider upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems. By upgrading these buildings, they can set an example for private industry to follow. They could then promote conversion in other market segments such as industrial factories or power plants.

Justification:

The justification for upgrading legacy federal owned or operated buildings that have inadequate security in their connected systems is provided below:

- These buildings are reliant on building 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.

Implementation Considerations

- The EPA has a program for Energy Star Building Certifications. 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 explored such as the National Cyber Labeling Program for Consumer IoT versus Energy Star on appliances.
- The GSA Federal Acquisition Regulation (FAR) could have base level cybersecurity requirements for connected systems in building infrastructure. (See https://www.gsa.gov/cdnstatic/Real_Estate_Acquisitions/FSL_I_Security_Requirements_82021.pdf)
- The Defense Federal Acquisition Regulation (DFAR) has requirements (https://www.nist.gov/mep/cybersecurity-resources-manufacturers/compliance-cybersecurity-and-privacy-laws-and-regulations).
- Building owners can utilize basic cyber hygiene best practices (i.e., changing default passwords, segmentation of networks by using items such as firewalls, installing patches)

Potential implementation barriers:

- Funding: Funding to upgrade the existing legacy base could be considerable. Also, if additional validation/certifications are needed for a particular building there is an additional upfront cost.
- Lack of knowledge and training: Building owners and managers may have limited knowledge of how to protect against cyber-attacks.
- Cybersecurity addresses a variety of requirements across the building infrastructure, as an example a medical building may have different needs and associated risks from a commercial office building. There is no-one size fits all.
- Evolving threat landscape: As the threat landscape is constantly evolving- concerns exist if a building has been updated/retrofitted with cybersecurity systems and malicious actors can still gain access to it.

Possible participating agencies:

GSA, NIST, DHS, DoD, among others.