February 26, 2021

Via IoTSecurity@nist.gov

Katerina Megas
Program Manager, NIST Cybersecurity for IoT Program
National Institute of Standards and Technology
Gaithersburg, MD 20899

Subject: NIST Releases Draft Guidance on Federal Internet of Things (IoT) Device Cybersecurity

Dear Ms. Megas:

The U.S. Chamber of Commerce commends the National Institute of Standards and Technology's (NIST's) efforts in writing the four draft publications to help coordinate the manufacture and federal procurement of more secure IoT devices.[1] We appreciate NIST's extensive outreach to the Chamber and other business groups, as well as the additional time to provide feedback.

Key Points

- The National Institute of Standards and Technology's (NIST's) four drafts—NIST Special Publication (SP) 800-213 and NIST Interagency Reports (NISTIRs) 8259B, 8259C, and 8259D—are a good starting point to address aspects of recently enacted Internet of Things (IoT) cybersecurity legislation, as well as ensure that the federal officials and IoT device manufacturers are on the same page with regard to security for IoT devices procured by agencies.

- The Chamber wants to work with NIST to get these guidance and requirements documents correct. Over the past few years, industry has successfully worked with NIST to develop a *core security baseline* for all new IoT devices, which is a positive development.

- While it's not NIST's objective, the four drafts have resurfaced concerns about policy fragmentation that was largely addressed by IoT security stakeholders this past summer. IoT device stakeholders are also concerned about the apparently high ceiling that agencies could have to inconsistently stack security requirements atop the core baseline for devices and/or managed service providers.

- The Chamber recognizes that only Congress can address the IoT security policy fragmentation problem through federal preemption legislation.

FOUR DRAFTS ARE A GOOD STARTING POINT

According to NIST, the four drafts—NIST Special Publication (SP) 800-213 (SP 800-213) and NIST Interagency Reports (NISTIRs) 8259B, 8259C, and 8259D—form a unit intended to help ensure that the government and IoT device makers are on the same page with regard to cybersecurity for IoT devices used by federal agencies.[2] NIST notes that the publications are a "starting point," and that they're expected to address some of the requirements called for under the recently enacted IoT Cybersecurity Improvement Act of 2020 (the IoT Act).[3]

NIST deserves praise for producing the documents under relatively challenging conditions. Each draft, whose primary audience includes IoT device manufacturers and agency officials, combines both similarities and differences. At the time of this writing, many in industry are working to comprehend the four drafts (e.g., what they require of device makers and federal officials, how they fit together, and how they would be used by both practitioners and policymakers). The Chamber wants to help NIST get these guidance and requirements documents right. We urge NIST to complete them based on public- and private-sector consensus, which agency officials appear to support.

KEY CONCERNS INCLUDE POLICY FRAGMENTATION AND AGENCY REQUIREMENTS ABOVE THE CORE BASELINE

The four drafts have generated a mix of comments, concerns, and requests for clarification from several business groups. It would be easy to focus on the minutiae of the four drafts and miss the forest for the trees. The Chamber's principal concerns with the four drafts relate to arguments that we've emphasized in the past. The Chamber believes that stakeholders should increasingly direct their energies toward pushing public officials at home and internationally to align their policies to the core IoT security baseline and fostering market demand for strong devices.[4]

The Chamber is confident that NIST principals will do their best to develop the preliminary drafts in partnership with the business community. Yet NIST and industry actors are constrained by the law. Only Congress can address the IoT security policy fragmentation problem—which was largely dealt with following the release of NISTIR 8259A but resurfaced with the passage of the IoT Act—through truly preemptive legislation.[5]

Policy fragmentation. While it's not NIST's intention, the four drafts have resurfaced the *Which NISTIR(s) do we point to?* problem that was largely addressed by IoT security stakeholders this past summer. In June 2020, NIST published the core IoT security baseline as a stand-alone document,[6] commensurate with the Chamber's September 2019 and February 2020 letters to the agency. We applaud NIST for its positive decision.[7] At the time, the Chamber concluded that this outcome would likely be felt domestically and overseas through reduced legal and regulatory fragmentation.

In December 2020, however, the IoT Act became law after some three years of development. Among other things, the new law establishes minimum security requirements for IoT devices purchased by the U.S. government. According to the bill writers, the IoT Act seeks to leverage the purchasing power of the federal government to move the market for IoT devices

toward greater cybersecurity. Notwithstanding industry urgings, Congress stopped short of developing a national, protective bill that addressed the underlying costs of increasing domestic policy fragmentation, which the IoT Act contributes to.

Requirements above the core baseline. It is worth highlighting that policy fragmentation is a key challenge, but it's not the only one. IoT device stakeholders are concerned about the seemingly high ceiling that agency officers could have to inconsistently stack security requirements atop the core baseline for devices and/or managed service providers. High ceilings in a dwelling can be freeing, but in this regulatory environment they become onerous, leading to multiple requirements and much irregularity among agencies' profiles. Agencies' profiles are likely to begin with the core baseline; then, officials will add cybersecurity capabilities and non-technical supporting capabilities on top. "If agencies take the [core] baseline and stack up device requirements without guardrails," the thickness and variability of requirements could prove difficult to manage well, noted a Chamber member.

Which NISTIR(s) do manufacturers and policymakers point to?

Over the past few years, industry has successfully worked with NIST to develop a core security baseline for all new IoT devices. This past June, NIST published the core baseline as a stand-alone document meant for all new devices.

However, the preliminary drafts, which are called for by the IoT Act, are geared toward establishing requirements for federally purchased devices. These documents will likely command much attention by cybersecurity stakeholders and could increase business confusion and policy fragmentation.

It's not a stretch to see how IoT device makers or managed service providers could review the security guidance/requirements landscape and wonder which special publication or NISTIR should drive their decision making and risk management activities. Further, not all IoT device makers will build for the U.S. government in accordance with SP 800-213 and the NISTIR 8259 series. Whether they do or do not, it could be unclear to them and others what using the core baseline means.

Released in January 2020:	Released in June 2020:	Released in December 2020:
• Draft (2nd) NISTIR 8259 NISTIR 8259 contained the core baseline within one of six foundational activities. This arrangement clouded the distinction between the foundational activities and the core baseline that many in industry seek to elevate. The Chamber urged NIST to make the separation between the foundational activities and the core baseline obvious to readers of NISTIR 8259, which the agency constructively did.	• NISTIR 8259 (foundational activities) • NISTIR 8259A (core baseline) The core baseline is grounded in public-private consensus.	• Draft SP 800-213 (federal guidance and requirements) • Draft NISTIR 8259B (non-technical baseline) • Draft NISIR 8259C (federal profile creation and documentation) • Draft NISTIR 8259D (federal profile) A separation between the foundational activities and the core baseline was achieved until passage of the IoT Act, which calls for the development of IoT security standards and guidelines (i.e., the four drafts)[8] specific to the federal government.

***

COMMENTS ON THE FOUR DRAFTS

The remainder of this letter consists of business community feedback, which ranges from high level to specific, that the Chamber has received on draft SP 800-213 and the preliminary NISTIRs. The Chamber does not necessarily endorse each view, but we believe that NIST should consider each in the context of cybersecurity stakeholders' comments.

Draft NISTIR 8259D

Table 1—Device Cybersecurity Capabilities in the Federal Profile	
Capability: Device Configuration	
Sub-capability No. 1: Display Configuration (pp. 5–6). • Ability to configure content to be displayed on a device.	Comment: The Chamber received feedback from a company principal who noted that the wording "Ability to configure content to be displayed on a device" implies that there is an expectation that IoT devices must possess an interactive display. "Most IoT devices do not have a screen on which to display content, so this sub-capability could be unrealistic in many, if not most, situations."
Capability: Logical Access to Interfaces	
Sub-capability No. 3: System Use Notification Support (pp. 6–7). Related to the comment above on device displays, this sub-capability also seems to call for devices to come equipped with a display function or a screen. • Ability to create an organizationally defined system use notification message or banner to be displayed *on the IoT device*. • Ability to keep the notification message or banner *on the device* screen until the device user actively acknowledges and agrees to the usage conditions [italics added].	Comment: A businesses official told the Chamber that even though the capability is titled "Logical Access to Interfaces," he thinks this sub-capability is meant to apply to any interactive session. But the language "on the IoT device" and "on the device screen" can be interpreted as a requirement that devices must be outfitted with a screen. "This is exceedingly rare," the official noted.

Sub-capability No. 5: Authentication & Identity Management (p. 7). • Ability to establish access to the IoT device to perform organizationally defined user actions *without* identification or authentication [italics added].	Comment: A business cyber expert told the Chamber he is uncertain about the intent of this sub-capability. "It seems to contradict previous sub-capabilities" (see sub-capability No. 4: Authorization Support, p. 7). Without identification or authentication, it's unclear how this sub-capability, which calls for "identify[ing] authorized users and processes" and differentiat[ing] between authorized and unauthorized users (physical and remote)" can be accomplished.
Sub-capability No. 7: Interface Control (p. 7). • Ability to support wireless technologies needed by the organization (e.g., Microwave, Packet radio [UHF/VHF], Bluetooth, Manufacturer defined).	Comment: A business commenter expressed concern to the Chamber about an aspect of sub-capability No. 7: Interface Control (p. 7). It calls for the "Ability to *support wireless technologie*s needed by the organization (e.g., Microwave, Packet radio [UHF/VHF], Bluetooth, Manufacturer defined)" [italics added]. "This ability is a design constraint and dictates an operational feature, not a cybersecurity feature. I presume the devices will support or not support wireless technologies as dictated by their design and expected use case. Granted, most IoT devices will have a wireless component, as it is a typical use case, but this should not be a mandated cybersecurity requirement."
Capability: Cybersecurity State Awareness	
Sub-capability No. 1: Access to Event Information (p. 8). • Ability to access information about the IoT device's cybersecurity state and other necessary data.	Comment: A business principal told the Chamber that the sub-capability "Access to Event Information" references the "Ability to access information about the IoT device's *cybersecurity state* and other necessary data [italics added]." He added, "While the NISTIR 8259D glossary defines 'cybersecurity state,' [p. 21] and it is referenced elsewhere in the document, the term is vague enough that vendors have leeway to interpret it in any way they desire. More clarity on 'cybersecurity state' would be helpful."

Sub-capability No. 2: Event Identification and Monitoring (p. 8). • Ability to identify organizationally defined cybersecurity events (e.g., expected state change) that may occur *on or involving* the IoT device. • Ability to monitor for organizationally defined cybersecurity events (e.g., expected state change) that may occur *on or involving* the IoT device [italics added].	Comment: A company official remarked to the Chamber, "In this capability, the usage is less specific and more appropriate. However, it is still too vague a concept. "The language '[…] that may occur on or involving the IoT device' is both broad and vague. Vendors should, as indicated throughout this profile, provide the ability to monitor for cybersecurity events *on* the device. But 'on involving the IoT device' lacks specificity."
Sub-capability No. 2: Event Identification and Monitoring (p. 8). • Ability to scan files for *unapproved* content [italics added].	Comment: A business expert questioned the "Ability to scan files for unapproved content" (p. 8). He said, "I don't quite understand how a vendor will accomplish this. While innocuous sounding, this [bullet] seems to indicate the ability to [undertake] whitelisting. If this means scanning the internal [unapproved] content of files, it becomes a markedly more difficult proposition. Perhaps it would make more sense if this were a sub-capability referring to anti-malware abilities, but that does not appear to be the case."[1]
Sub-capability No. 4: Logging Capture & Trigger Support (pp. 8–9).	Comment: A business principal noted to the Chamber that some of the logging-capture requirements are "potentially unattainable." He added, "Depending on the organization's retention period—something the vendor cannot know beforehand—this could require an almost limitless amount of storage. For example, an organization may require unlimited retention, in which case the requirement calls for unlimited storage. In that situation, it would be incumbent upon the customer to design a mechanism to offline storage to accommodate the limited storage on the device."

[1] Similarly, sub-capability No. 3 under Cybersecurity State Awareness, Event Response, in NISTIR 8259D calls for the "Ability to prevent download of unapproved content" and the "Ability to delete unapproved content." (p. 8).

Capability: Device Security	
Sub-capability: Secure Communication (p. 10). • Ability to enforce traffic flow policies. • Ability to interface with DNS/DNSSEC.	Comment: A business respondent said there are situations where devices are deployed in a static configuration for which these two points would be an unnecessary requirement. The respondent was referring to both points, although he added, "I was thinking more about DNS when I wrote. What I was getting at was the idea that [the NISTIR] shouldn't necessarily require DNS/DNSSEC or traffic flow if a device is not meant to be implemented in a non-static environment. I can see the need for traffic flow because devices will generally require some connectivity that generically involves 'traffic.' But not all decides will rely on DNS to resolve names. They'll just be statically configured. It's a burden for a manufacturer to include that capability if the device is never designed to use it. However, of course if name lookups are part of the design, then sure DNS/DNSSEC makes sense. I just want to throw a flag on requiring it 'no matter what.'"

Draft NISTIR 8259D

Table 2—Non-technical Supporting Capabilities in the Federal Profile	
Capability: Documentation	
Sub-capability: Legal & Regulatory Compliance Support (p. 11). • "Document all security standards requirements, such as SP 800-53 Rev 5 controls, ISO security and/or privacy standards controls, etc., that are used to support security and privacy regulatory requirements with which the IoT device capabilities must comply within the IoT device customer's information systems."	Comment: A company official said, "I don't understand this requirement. How would the vendor know the regulatory environment that the device(s) is being deployed into? … I would accept this requirement if it were framed in terms of 'documenting the capabilities of the device,' including which NIST SP 800-53 controls are supported by such capabilities. But this capability reads more like 'develop a compliance plan for the organization.' I don't think that this would work for many vendors. The second bullet in

• "Document the legal security and privacy controls requirements (Federal regulations, international regulations, state and local laws) for which the IoT device has capabilities that support compliance. Some examples: Health Insurance Portability and Accountability Act (HIPAA), California Consumer Privacy Act (CCPA), EU General Data Protection Regulation (GDPR)."	this sub-capability reads more like I assume the first bullet would read."
Capability: Information Dissemination	
Sub-capability: Cybersecurity and Vulnerability Alerts (p. 13–14).	Comment: A company professional said to the Chamber, "This [capability] seems to skirt the requirement that vendors actively and proactively notify customers of discovered vulnerabilities and provide timely remediation. It gets very close [to proactive notifications] but tends to deviate into a 'document' statement rather than explicitly stating that vendors should be required to notify [their customers]. … We run into this often where vendors have a stated obligation to notify the asset owner of discovered vulnerabilities. When there has been a long period with no notifications, how is the customer assured that the process is still working? I recommend positive assurance in which the vendor notify on a regular basis even if there are no newly discovered vulnerabilities."

The four drafts should emphasize they're not regulatory for the non-federal market

Several business organizations urge NIST to—

- Clarify whether and how the four drafts fulfill congressional mandates under the IoT Act.
    - While NISTIR 8259D and SP 800-213 seem relevant to the provision of the IoT Act that requires NIST to "develop and publish … standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to

information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices," the drafts are silent about their relation to the law.[9]

  - It would be helpful for NIST to clarify where each draft document fits into the law's mandates and describe any additional workstreams related to the IoT Act.

- Continue meaningful collaboration with the private sector.

  - Collaboration with industry is important to NIST's success. The four drafts could benefit from additional, extended input. One possible approach, for example, would feature NIST and business groups considering conformity assessments for devices. Businesses are interested in collaboration that focuses on implementing the IoT Act and ensuring high levels of device cybersecurity at federal agencies.

  - The four drafts could benefit from highlighting industry best practices and industry-driven informative references, which are forthcoming.

- Make explicit that the four drafts are nonregulatory (voluntary) for the private sector and flexible for public- and private-sector users. NISTIRs 8259B and 8259D and SP 800-213 are recommendations only for the federal government and use of 8259C is voluntary.

  - SP 800-213 and NISTIR 8259D focus on federal agencies' risk profiles. NISTIR 8259B says it is essential to understand that the non-technical supporting capabilities are not considered mandatory.

  - NISTIR 8259C should help agencies create a profile based on technical and non-technical core baselines. NIST is not trying to establish private sector risk profiles.

  - While NIST recognizes the importance of flexibility to varying degrees throughout the four drafts, it should be stated even more explicitly.

- Differentiate public- and private-sector risk profiles.

  - While NIST's guidance will affect the IoT ecosystem, the four drafts should acknowledge the different risk profiles of the federal government and the private sector.

  - NIST should make it clear that its federally specific documents are plainly delineated as such, with appropriate disclaimers and language to ensure that private users understand that these publications do not necessarily apply to them.

- Revise the non-technical capabilities baseline document (i.e., NISTIR 8259B) so that it is applicable to all IoT devices and targeted toward manufacturers, consistent with the existing technical capabilities baseline document. NIST needs to clarify that NISTIR

8259B is for federal use. The document (p. 4, line 304) says that each row in Table 1 covers one of the device non-technical supporting capabilities in the federal core baseline.

  - Consistent with NISTIR 8259A, NIST should ensure that NISTIR 8259B is a true baseline for manufacturers and flexible enough to be applicable to all IoT devices.

  - To accomplish this goal, NIST should make targeted edits to clarify that NISTIR 8259B is broadly applicable to all types of devices—from low- to high-complexity, managed to unmanaged, and home use to federal government use. Remove non-technical capabilities that are not broadly applicable to the diverse universe of IoT devices.

  - NIST should clarify that NISTIR 8259B's guidance is designed for manufacturers, consistent with the rest of the NISTIR 8259 series and remove references to non-manufacturer third parties to help achieve this objective.

- Explain how the four drafts work with one another and develop resources to promote voluntary use—that is, the IoT device capability requirements in the documents are for federal government use only.

  - Because the NISTIR 8259 series involves many publications tackling different aspects of a larger goal—with some guidance directed at manufacturers and some directed at federal users—it may be difficult for a cybersecurity practitioner to understand where to start or how all the documents fit together.

  - The Chamber recommends that NIST publish a standalone document that explains the relationship of its four drafts with one another, as well as other NIST guidance. Improving the utility of the documents will help ensure that NIST's important work can be voluntarily and securely adopted across the IoT ecosystem.

More clarity is urged regarding NISTIR 8259D requirements and supporting features

- NIST took a structured approach to derive the federal profile (NISTIR 8259D) by applying the process for creating a specific profile (NISTIR 8259C) to the technical and non-technical baselines (NISTIRs 8259A and B). The agency wants to support the needs and goals of federal agencies and provide guidance to federal agencies in determining the applicable device cybersecurity requirements (i.e., the set of device cybersecurity capabilities and non-technical supporting capabilities) for an IoT device (SP 800-213).

- Industry wants to collaborate with NIST to achieve high and effective IoT cybersecurity standards for federal agencies. Increasing mutual understanding between

NIST, customers (federal agencies), and IoT device manufacturers is necessary to mitigate increasing burdens on the stakeholders.

Further guidance is needed on NISTIR 8259D requirements

- SP 800-213 refers to two types of IoT device integration with federal information systems: (1) as its own system (minimum interaction with the system(s)) and (2) as an element within an authorization boundary (close interaction with the system(s)). NIST is asked to clarify how each of the crucial abilities and actions defined in NISTIR 8259D is applicable to deployment scenarios with different level of integrations (e.g., a gateway that may provide interworking functions between IoT devices and the information systems).

- More guidance would help federal agencies develop procurement requirements for IoT devices. Such guidance articulates minimum capabilities and actions in further detail for typical cases of IoT device integration(s) to the low-impact information systems.

Supplementary clearness is needed on supporting features

- NIST defines "Device Cybersecurity Capability" as "Cybersecurity features or functions that computing devices provide through their own technical means …," and Non-Technical Supporting Capability Core Baseline" as … "a set of non-technical supporting capabilities generally needed from manufacturers or other third parties to support common cybersecurity controls that protect an organization's devices as well as device data, system, and ecosystems." It is noted that some key capabilities defined in table 1 of NISTIR 8259D (p. 5) require support from IoT platforms and tools. NIST is urged to clarify the supporting feature in the table.

- Considering resource constraint IoT devices in the market, [commentators] highlight the importance of the supporting features for securing the federal information systems with IoT devices, including device discovery, monitoring, configuration management, vulnerability handling, and anomaly detection. To help secure supply chains, continuous monitoring and verifying of device cybersecurity posture are essential. Automated tools to scan binary files, create software inventory, and assess vulnerabilities should be a supporting feature.

- NIST is urged to provide supplementary clarification on requirements for supporting features in the four drafts or via an additional guidance document.

Feedback is requested on 'should versus shall' considerations, zero trust, and catalog updates

Requirements

- SP 800-213 is a guidance publication. Yet is the plan to set requirements ("shall" statements) for federal agencies?

Federal information system and environment

- Section 2.1 of SP 800-213 (p. 4) explains the scope of a generic federal information system and its surround operational environment. Because of shifts to zero trust architectures, the authorization boundary becomes less clear. Additional clarification about the boundary is needed.

Cybersecurity capability catalog

- How will NIST update the catalog of IoT device cybersecurity capabilities and support non-technical capabilities for manufacturers and IoT device customers?

IT cybersecurity requirements on IoT require further examination

- NISTIR 8259C defines how to get to NISTIR 8259D; one essential step is to assemble all applicable requirements for cybersecurity for the agency.

- The FISMA Implementation Project[10] chose the strategy that IT and IoT are equivalent from a network security perspective. In other words, agencies are expected to treat IoT no differently than IT components. As such, requirements for servers, printers, and routers would apply to IoT devices like soil humidity detectors and single-use package tracking fobs.

- This IT-is-equivalent-to-IoT decision shows up in the latest version of SP 800-53 (rev. 5, September 2020). Thus, SP 800-53 treats IT and IoT as equivalent for cybersecurity discussions in the federal government. Also, Federal Information Processing Standards and other cybersecurity requirements for IT systems are automatically pulled into NISTIR 8259D by processes called for in NISTIR 8259C.

- The combination of SP 800-53 and NISTIR 8259C ensures that NISTIR 8259D is a list of IT-centric requirements that would be applied to IoT, despite the practically differences with respect to IoT devices. It is important to find ways to adjust NISTIR 8259D, while recognizing that it is not written in a vacuum.

- NIST is urged to clarify that all device capabilities do not have to be on the physical device, and that some capabilities could be delivered via the cloud.

Scope the guidance for effectively managed device life cycles, and so forth

NISTIR 8259C

- Call for IoT to comply, implement, and develop functionality, including application program interfaces through published open standards.
    - Interoperability between IoT devices and solutions should be based on published open standards.

NISTIR 8259B

- Scope guidance for a *well-managed life cycle* for all parts of any IoT device or a solution.
    - This effort should include embracing standards for technology life cycle management.
    - A reasonable duration of *in-support life expectancy* should be consistent with the anticipated lifecycle of the product when deployed.

- Allow for special classes of IoT devices where other regulations or unique requirements may apply.
    - Specific example—
        - Fire alarms need to meet burn survival times. These devices may use network interconnects with proprietary solutions and consider themselves *internal components to the outcome they offer*. Clarity is urged on whether IoT regulations apply to internal components vis-a-vis the expected outcomes.

Four drafts (general)

- To the extent that NIST's current work focuses on security vulnerabilities and related topics, it should also consider the following:
    - Additional guidance related to the treatment of data collected and shared, typically to public cloud-hosted solutions.
    - Recommendations for adherence to existing privacy and data protection regulations.

***

The Chamber appreciates the opportunity to provide NIST with comments on the draft guidance and requirements on federal IoT device cybersecurity. If you have any questions or need more information, please do not hesitate to contact Christopher Roberti (croberti@uschamber.com, 202-463-3100) or Matthew Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Christopher D. Roberti
Chief of Staff
Senior Vice President, Cyber, Intelligence, and Security

Matthew J. Eggers
Vice President, Cybersecurity Policy

Endnotes

[1] NIST, "NIST Releases Draft Guidance on Internet of Things Device Cybersecurity," December 15, 2020.
https://content.govdelivery.com/accounts/USNIST/bulletins/2b1446d
https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity

[2] https://csrc.nist.gov/publications/detail/sp/800-213/draft
https://csrc.nist.gov/publications/detail/nistir/8259b/draft
https://csrc.nist.gov/publications/detail/nistir/8259c/draft
https://csrc.nist.gov/publications/detail/nistir/8259d/draft

[3] The IoT Cybersecurity Improvement Act of 2020 (the IoT Act) (H.R. 1668—P.L. 116-207).
https://www.congress.gov/bill/116th-congress/house-bill/1668

[4] https://www.uschamber.com/sites/default/files/09-30-19_uscc_comment_letter_nistir_8259_final_v1.0.pdf

[5] The Chamber urges Congress to develop legislation that would both spur device makers to build to the core baseline and grant legal liability and regulatory safeguards to the makers and sellers of strong IoT equipment. Legislation of this kind would be a win-win for government and industry.

[6] https://content.govdelivery.com/accounts/USNIST/bulletins/28ea048

[7] https://www.uschamber.com/sites/default/files/200211_uscc_comments_nistir_8259_second_draft_final.pdf

[8] See § 4 of the IoT Act.

[9] IoT Act, § 4(a)(1). NIST is also required to develop, publish, and implement vulnerability disclosure guidelines for information systems, including IoT devices. See §§ 5–6 of the act.

[10] https://csrc.nist.gov/projects/risk-management