



Software and Supply Chain Assurance Forum

NIST's Approach to IoT Cybersecurity Baselines

January 15, 2020

Outline

- Background on how we got here....
- Overview of 8259v2
 - Highlights
 - Changes from first version
- Next: Federal Baseline
 - Approach
 - Timeline
- Q&A



The NIST Cybersecurity for IoT Program coordinates across NIST on IoT cybersecurity

Research/Reports

- **Mitigating IoT-Based DDoS/Botnet Report**
- Cybersecurity for Cyber Physical Systems
- Cybersecurity Framework
- Cybersecurity Framework Manufacturing Profile
- Cybersecurity for Smart Grid Systems
- Cyber Threat Information Sharing
- Lightweight Encryption
- Low Power Wide Area IoT
- Network of Things
- Report on State of International Cybersecurity Standards for IoT
- Security and privacy concerns of intelligent virtual assistances
- Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- Considerations for Managing IoT Cybersecurity and Privacy Risks
- Core Cybersecurity Baseline for Securable IoT Devices
- Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

Special Publications

- BLE Bluetooth
- Cloud security
- Digital Identity Guidelines
- Guide to Industrial Control Systems (ICS) Security
- RFID Security Guidelines
- Software Assessment Management Standards and Guidelines
- Supply Chain Risk Management
- Security Content Automation Protocol (SCAP) Standards and Guidelines
- Security Systems Engineering
- ABCs of Conformity Assessment
- Conformity Assessment Considerations for Federal Agencies

Applied

- Galois IoT Authentication & PDS Pilot
- GSMA Trusted Identities Pilot
- National Vulnerability Database
- Projects at National Cybersecurity Center of Excellence (NCCoE), some examples:
 - IoT-Based Automated Distributed Threats
 - Capabilities Assessment for Securing Manufacturing Industrial Control Systems
 - Security Review of Consumer Home IoT Products
 - Security for IoT Sensor Networks
 - Healthcare Sector Projects
 - Wireless Infusion Pumps, etc.
- Privacy Engineering Program



Cybersecurity for IoT Program Principles

Risk-Based Understanding

IoT capabilities, behaviors, deployment environments, and other characteristics can affect cybersecurity risk. Our approach to managing this risk is rooted in an understanding of how IoT can affect it.

Ecosystem of Things

Recognizing that no device exists in a vacuum, NIST takes an ecosystem approach to IoT cybersecurity. For many devices, much of the functionality happens outside the device—not all the security is on the device itself. As such, we look at the entire ecosystem, not just endpoints.

Outcome-Based Approach

Embrace the Cybersecurity Framework's outcome-based approach. Specify desired cybersecurity outcomes, not necessarily how to achieve those outcomes, which allows organizations to choose the best solution for each IoT device and/or their enterprise environment.



No One Size Fits All

Each organization has its own risk tolerance and mission needs, and no one set of controls will address the wide range of cross-industry and cross-vertical needs and use cases. There is no one-size-fits-all approach to managing IoT cybersecurity risk.

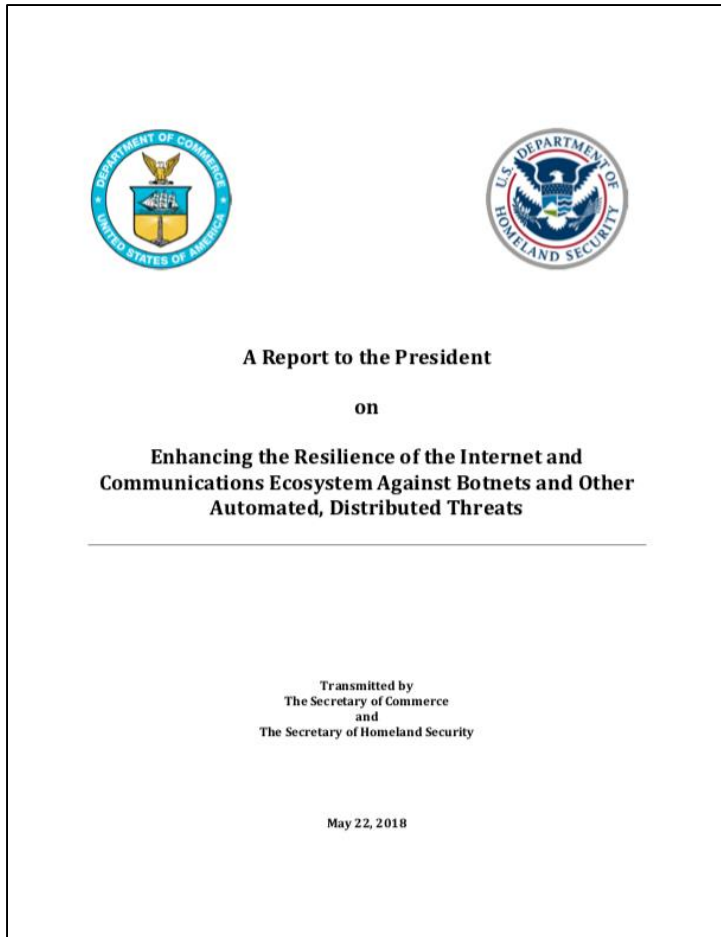


Stakeholder Engagement

NIST works with diverse stakeholders to advance IoT cybersecurity. This includes collaborating with stakeholders to provide the necessary tools, guidance, standards, and resources.



Our national strategy for securing IoT comes from President Trump's 2017 EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*

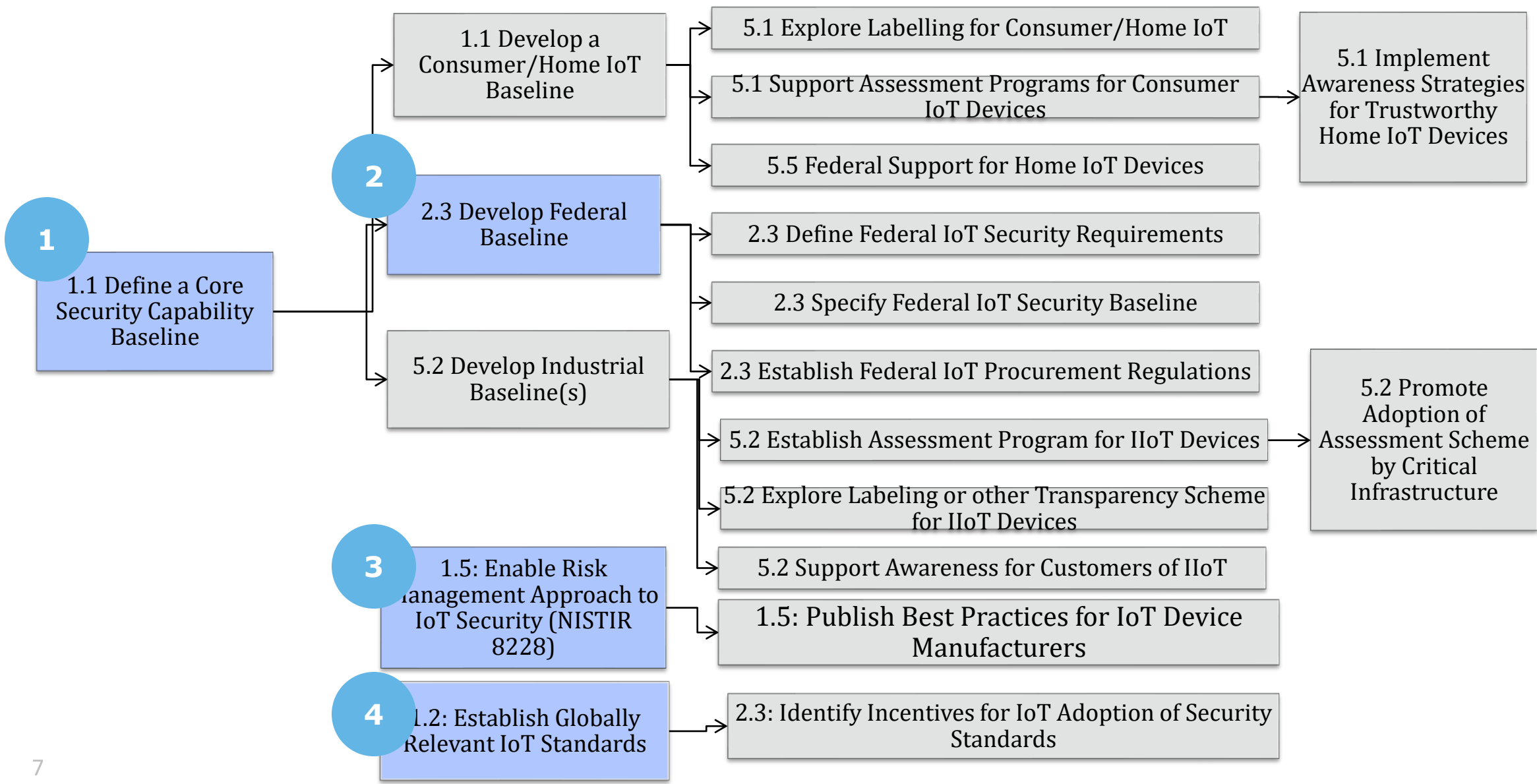


That EO tasked the Department's of Commerce and Homeland Security to "identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks"

The Departments completed this report in May 2018 and the subsequent roadmap lays out a series of actions for both private sector and government for securing the IoT ecosystem.



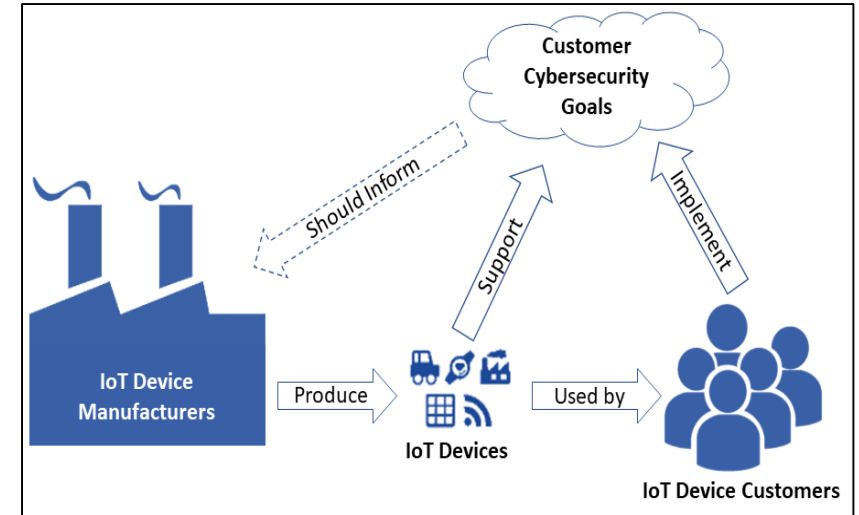
The November 2018 Roadmap lays out a plan that relies on both private industry and government partnerships and actions



Background on the concepts and core capabilities proposed in NIST IR 8259

- Pursuant to Roadmap action 1.5: Enable Risk Management Approach to IoT Security NIST published NIST IR 8228
- Focuses on IoT cybersecurity and privacy risk not addressed in existing IT guidance and provides considerations for applying existing guidance.
- Existing Risk Management Frameworks framed the analysis: Cybersecurity Framework; NIST Risk Management Framework; Special Publication 800-53
- We received over 250 public comments received during the public comment period
- The draft released **September 2018** included **15 possible security and privacy capabilities for IoT devices** **were based on:**
 - 13 existing IoT recommendations \ domestic and international (e.g. BITAG; CSA; CTIA; ENISA; GSMA; IIC; IoTSF; OTA; UKDDCMS)

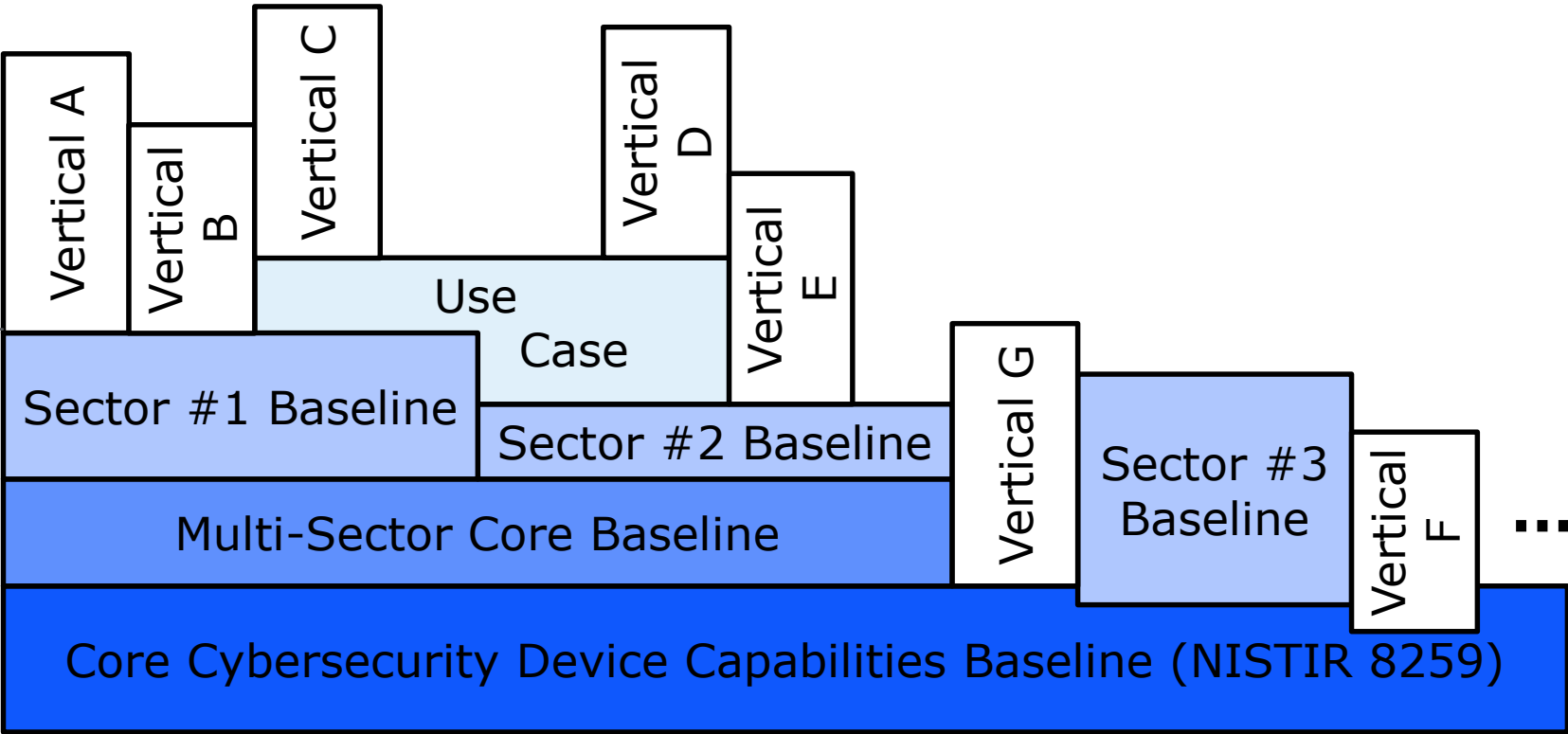
Comments on the IoT device capabilities, public workshops and roundtables served as the input for the starting point in 8259



The core baseline serves as a foundation across verticals to promote harmonization while allowing for customization

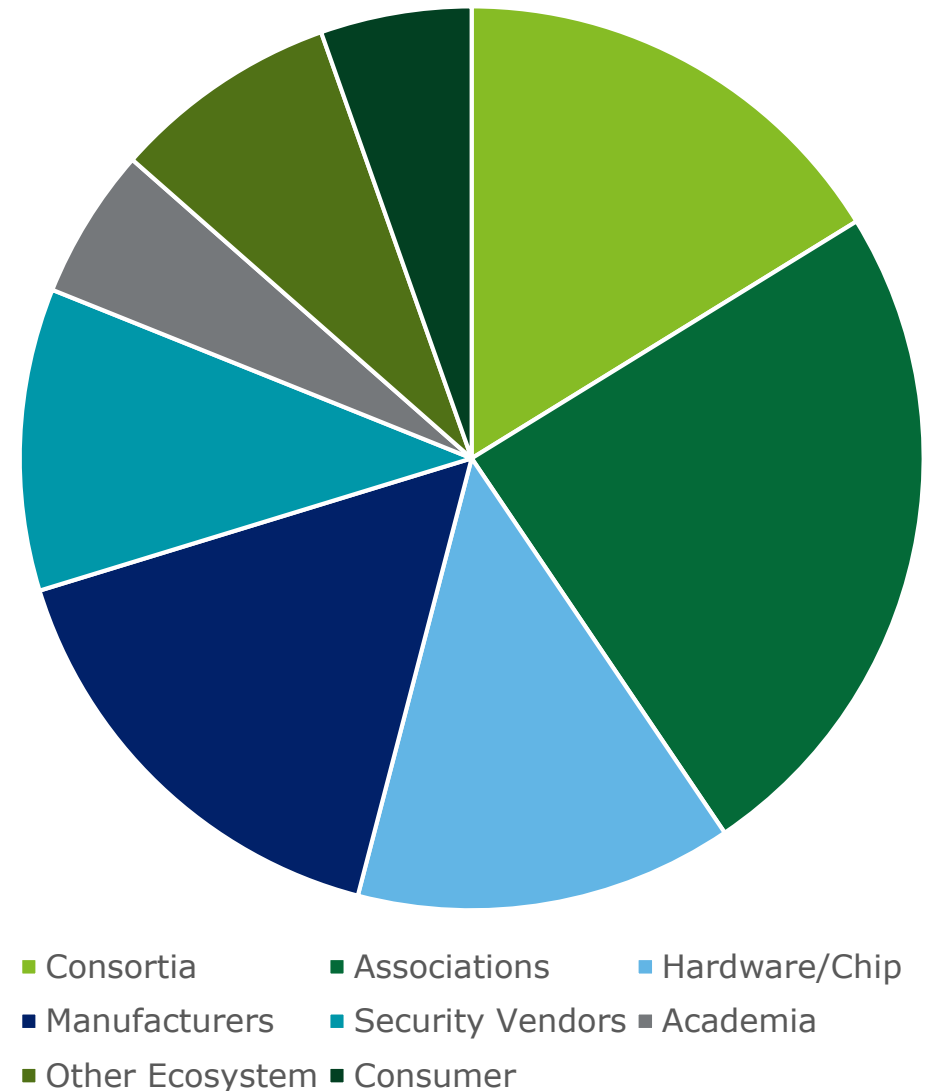
Sector/Vertical specific baseline approach follows IoT Principles:

- Risk Based Understanding
- No One Size Fits All
- Ecosystem of Things
- Outcome-based approach



First Draft NISTIR 8259 released in June 2019

- Public comment period on first draft closed September 30
- We received more than 450 comments from individuals and organizations across a variety of industries and sectors
- Updated NISTIR 8259 to reflect stakeholder feedback
- Released updated NIST IR 8259: *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline*



Updated 8259 highlights activities for manufacturer to consider framed within product development process



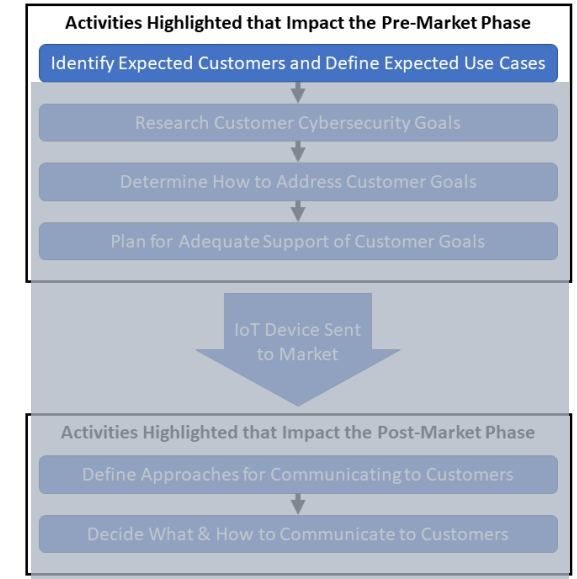
- Activities organized by phase most impacted by execution of the activity
- Two phases:
 - Pre-market – *before* an IoT device is sent to market
 - Post-market – *as and after* an IoT device is sold
- Content from first draft was reformatted as question to inform these activities
 - Meant to show through examples how a user of 8259 would plan and engage in the highlighted activities

Activity 1: Identify Expected Customers and Define Expected Use Cases

Identifying the expected customers and use cases for an IoT device early in its design is vital for determining which device cybersecurity capabilities the device should implement and how it should implement them.

Guiding questions for identifying expected customers:

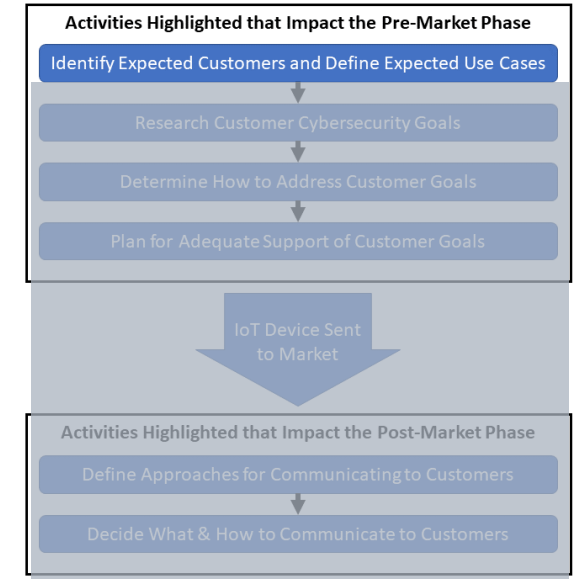
1. Which types of people are expected customers for this device? (e.g., musicians, small business owners, cyclists, police officers, chefs, home builders, preschoolers, electrical engineers)
2. Which types of organizations are expected customers for this device? (e.g., small retail businesses, large hospitals, energy companies with solar farms, educational institutions with buses)



Activity 1: Identify Expected Customers and Define Expected Use Cases

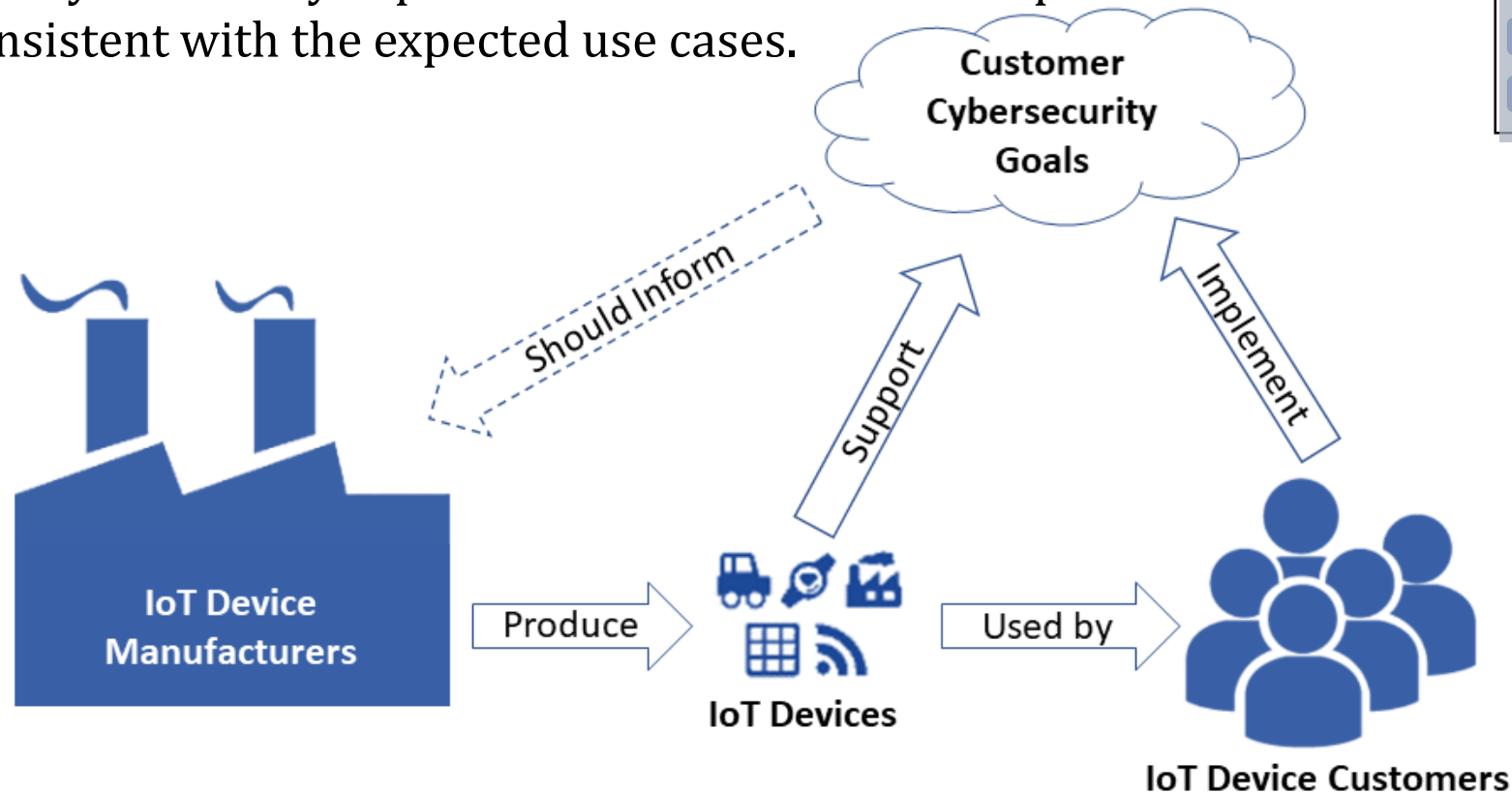
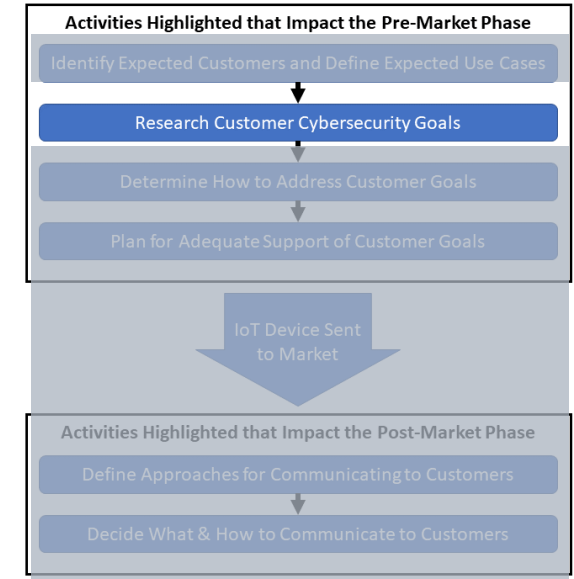
Guiding questions for exploring expected use cases:

1. How will the device be used? (e.g., for a single purpose or for multiple purposes; embedded within another device or not embedded)
2. Where geographically will the device be used? (e.g., countries, jurisdictions within countries)
3. What physical environments will the device be used in? (e.g., inside or outside; stationary or moving; public or private; movable or immovable)
4. What dependencies on other systems will the device likely have? (e.g., requires use of a particular IoT hub; uses cloud-based third-party services for some functionality)
5. How might attackers misuse and compromise the device within the context of the use case? (i.e., potential pairings of threats and vulnerabilities, such as in a threat model)
6. What other aspects of device use might be relevant to the device's cybersecurity risk?



Activity 2: Research customer cybersecurity goals

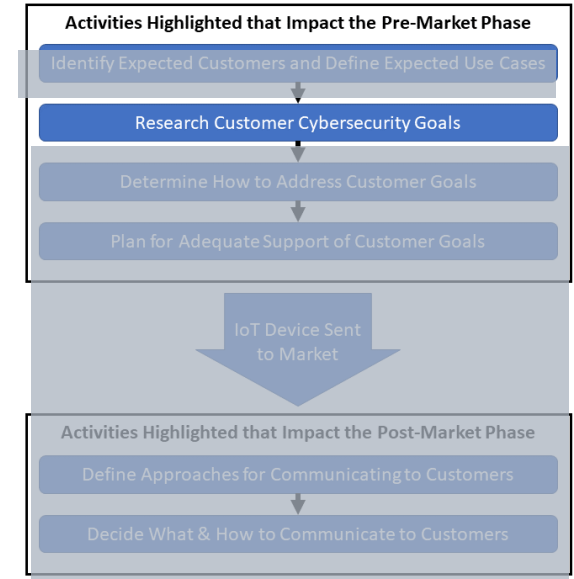
Manufacturers cannot completely understand all of their customers' risk because every customer faces unique risks based on many factors. However, manufacturers can make their devices at least minimally securable by those they expect to be customers of their product who use them consistent with the expected use cases.



Activity 2: Research customer cybersecurity goals

To gather information on customer goals related to safeguarding device integrity and data confidentiality, integrity, and availability, manufacturers can answer the following questions for each of the expected use cases:

1. How will the IoT device interact with the physical world?
2. How will the IoT device need to be accessed, managed, and monitored by authorized people, processes, and other devices?
3. How will the IoT device's use of device cybersecurity capabilities be affected in terms of the device's availability, efficiency, and effectiveness?
4. What will the nature of the IoT device's data be?
5. What are the known cybersecurity requirements for the IoT device?
6. What complexities will be introduced by the IoT device interacting with other devices, systems, and environments?

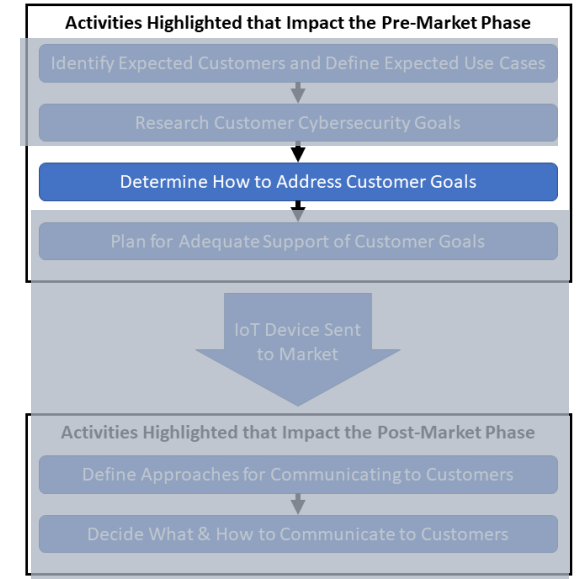


Activity 3: Determine how to address customer goals

Manufacturers can determine how to address those goals by having their IoT devices provide particular device cybersecurity capabilities in order to help customers mitigate their cybersecurity risks. For each cybersecurity goal, the manufacturer can answer this question:

Which one or more of the following is a suitable means (or combination of means) to achieve the goal?

- The IoT device can provide the technical means through its device cybersecurity capabilities
- Another device related to the IoT device (e.g., an IoT gateway or hub also from the manufacturer or a third-party) can provide the technical means on behalf of the IoT device
- Other systems and services acting on behalf of the manufacturer can provide the technical means (e.g., a cloud-based service that securely stores data for each IoT device)
- The customer can select and implement other technical and non-technical means for mitigating cybersecurity risk. (including accepting or transferring the risk)



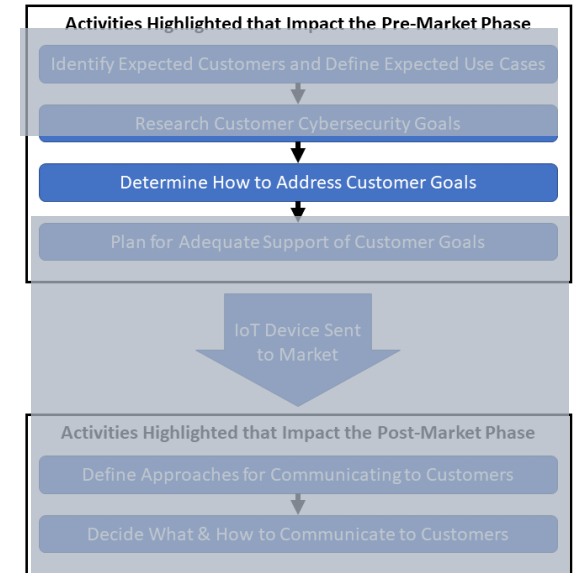
Activity 3: Determine how to address customer goals

In addition to identifying suitable means for addressing each cybersecurity goal, manufacturers can also answer this question:

How robustly must each technical means be implemented in order to achieve the cybersecurity goal?

Here are some examples of potential robustness considerations:

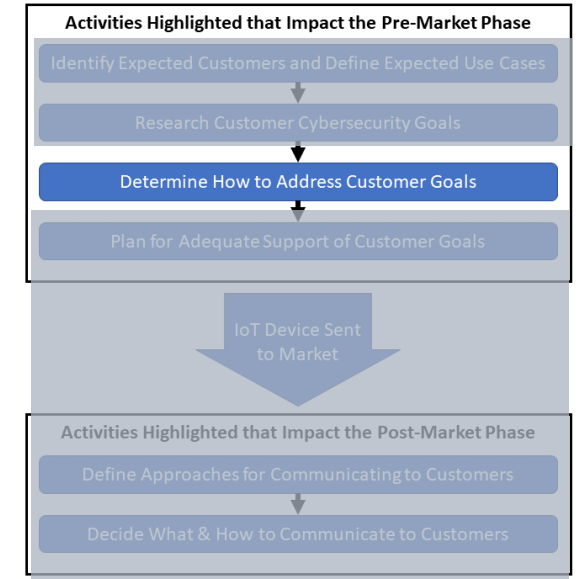
1. Whether it needs to be implemented in hardware or can be implemented in software instead
2. Which data needs to be protected, what types of protection each instance of data needs (e.g., confidentiality, integrity), and how strong that protection needs to be
3. How strongly an entity's identity needs to be authenticated before granting access (e.g., PIN, password, passphrase, two-factor authentication)
4. How readily software and firmware updates can be reverted if a problem occurs (e.g., a rollback capability, an anti-rollback capability)



Activity 3: Determine how to address customer goals

Ultimately, manufacturers can aggregate the technical means identified for all the goals to answer the following question:

Which technical means will be provided by the IoT device itself, other devices related to the IoT device, other systems and services acting on behalf of the manufacturer, and the customer, and how robust should each of those means be?



Activity 3: Determine how to address customer goals

To provide manufacturers a starting point to use in identifying the necessary device cybersecurity capabilities, this document identified a **Core IoT Device Cybersecurity Capability Baseline**, which is a set of device cybersecurity capabilities that customers are likely to need:

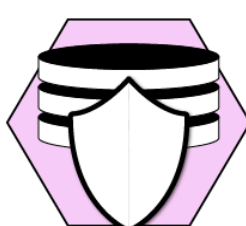
- **Device Identification:** The IoT device can be uniquely identified logically and physically.
- **Device Configuration:** The configuration of the IoT device's software and firmware can be changed, and such changes can be performed by authorized entities only.
- **Data Protection:** The IoT device can protect the data it stores and transmits from unauthorized access and modification.
- **Logical Access to Interfaces:** The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
- **Software and Firmware Update:** The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
- **Cybersecurity State Awareness:** The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.



Device
Identification



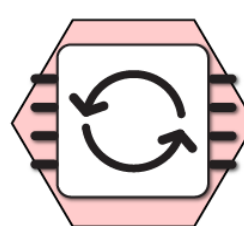
Device
Configuration



Data
Protection



Logical Access
to Interfaces



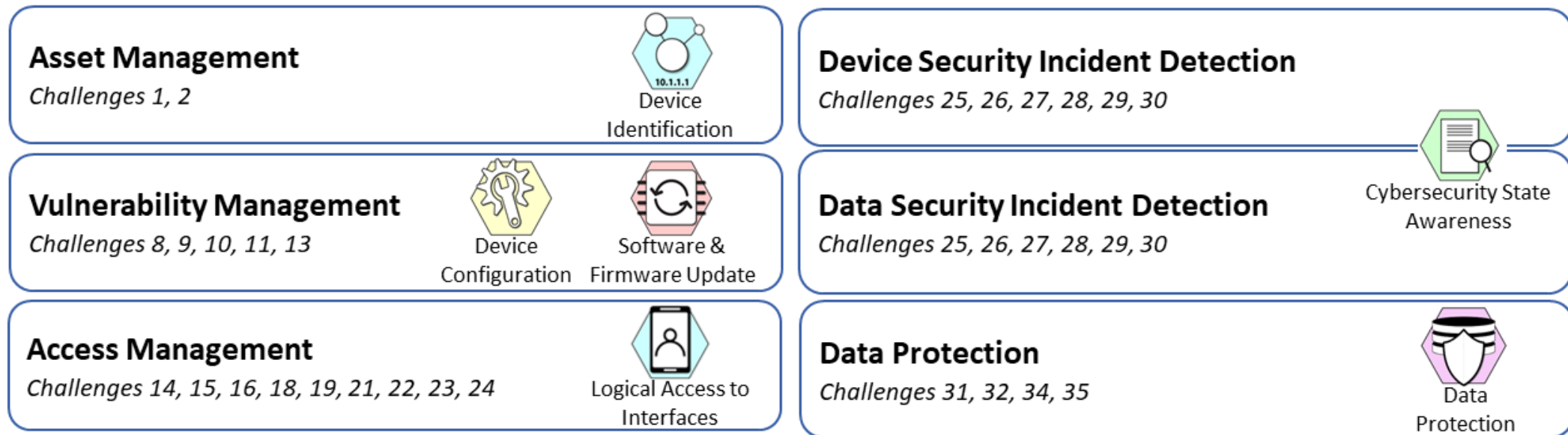
Software &
Firmware Update



Cybersecurity State
Awareness

Activity 3: Determine how to address customer goals

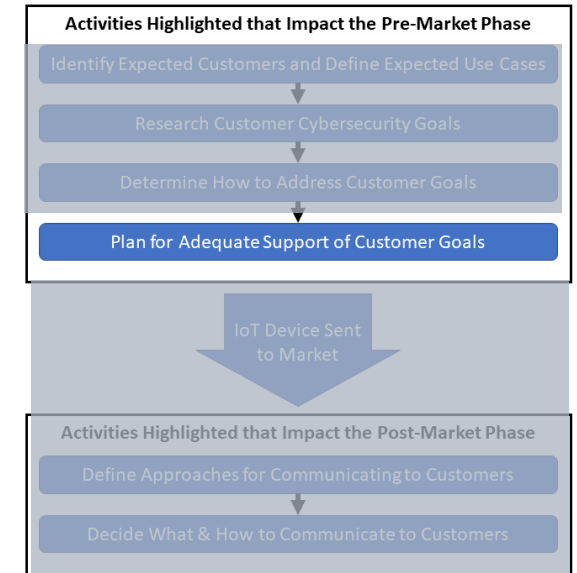
- The core baseline has been derived from common cybersecurity risk management approaches
- NIST IR 8228 had identified key challenges in risk mitigation areas for security
- The risk mitigation areas that are supported by each device capability are:



Activity 4: Plan for adequate support of customer goals

Manufacturers can help make their IoT devices more securable by appropriately provisioning device hardware, firmware, software, and business resources to support the desired device cybersecurity capabilities. When designing or selecting device hardware, firmware, and software resources, manufacturers can answer the following questions for the expected customers and use cases to help identify provisioning needs and potential issues:

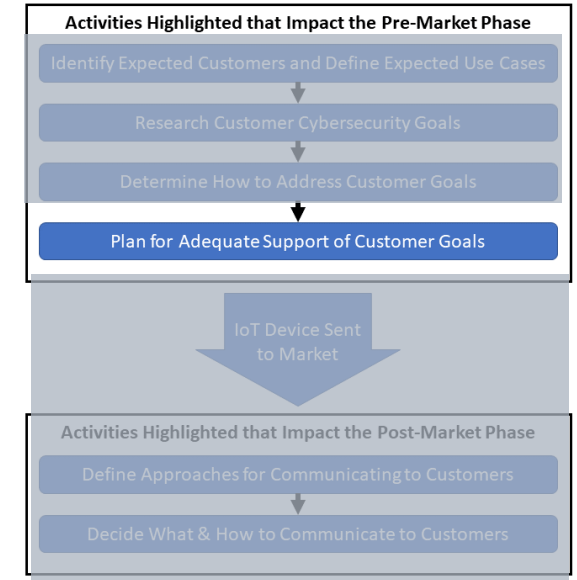
1. What potential future use needs to be taken into account?
2. Should an established IoT platform be used instead of acquiring and integrating individual hardware, firmware, and software components?
3. Should any of the device cybersecurity capabilities be hardware-based?
4. Does the hardware, firmware, or software (including the operating system) include unneeded device capabilities with cybersecurity implications? If so, can they be disabled to prevent misuse and exploitation?



Activity 4: Plan for adequate support of customer goals

Manufacturers should consider which, if any, secure development practices are most appropriate for them and their customers as they further plan how to adequately support customer goals. Manufacturers can answer questions like the following based on expected customers and uses cases to help identify additional action to take towards cybersecurity:

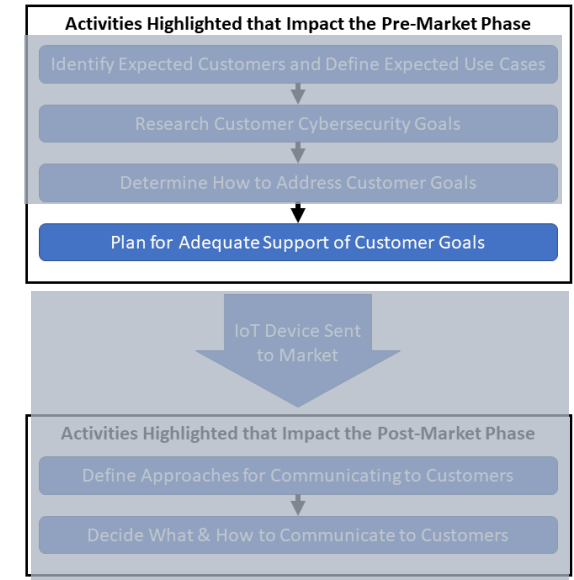
1. How is IoT device code protected from unauthorized access and tampering? (e.g., well-secured code repository, version control features, code signing)
2. How can customers verify software integrity for the IoT device? (e.g., code signature validation, cryptographic hash comparison)
3. What verification is done to confirm that the security of third-party software used within the IoT device meets the customers' needs? (e.g., check for known vulnerabilities that are not yet fixed, review or analyze human-readable code, test executable code)



Activity 4: Plan for adequate support of customer goals

Manufacturers should consider which, if any, secure development practices are most appropriate for them and their customers as they further plan how to adequately support customer goals. Manufacturers can answer questions like the following based on expected customers and uses cases to help identify additional action to take towards cybersecurity:

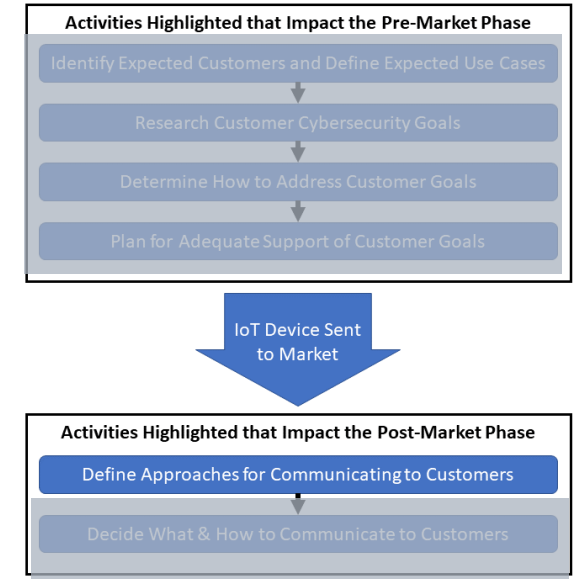
4. What measures are taken to minimize the vulnerabilities in released IoT device software? (e.g., follow secure coding practices, review and analyze human-readable code, test executable code, configure software to have secure settings by default)
5. What measures are taken to accept reports of possible IoT device software vulnerabilities and respond to them? (e.g., vulnerability response program, vulnerability database monitoring, threat intelligence service use)
6. What processes are in place to assess and prioritize the remediation of all vulnerabilities in IoT device software? (e.g., estimate remediation effort, estimate potential impact of exploitation, estimate attacker resources needed to weaponize the vulnerability)



Activity 5: Define approaches for communicating with customers

Many customers will benefit from manufacturers communicating to them more clearly about cybersecurity risks involving the IoT devices the manufacturers are currently selling or have already sold. Manufacturers can answer questions like the following to help define communication approaches:

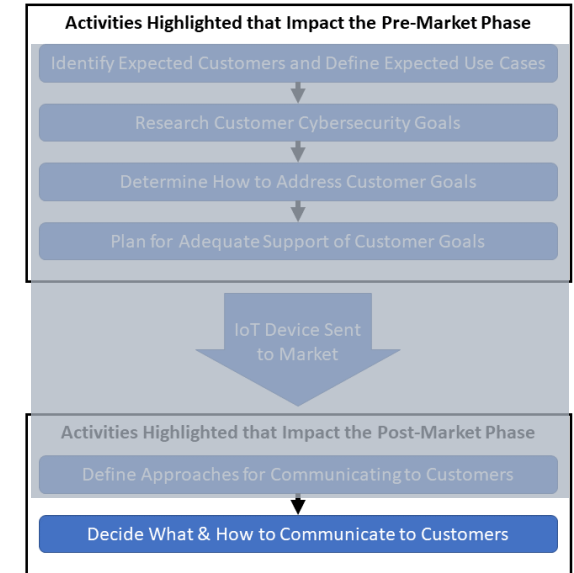
1. What terminology will the customer understand? For example, a home user will likely have less technical knowledge than points of contact at a large business
2. How much information will the customer need? Giving a customer too much information may overwhelm them and make it harder for them to find the information they need, but not providing enough information is generally undesirable as well.
3. How/where will the information be provided? Information can be provided in one or more logical and/or physical locations.
4. How can the integrity of the information be verified? For some methods of providing information, such as emails, customers may want a way to determine if the information is legitimate (e.g., not a social engineering attempt).



Activity 6: Decide what to communicate to customers and how to communicate it

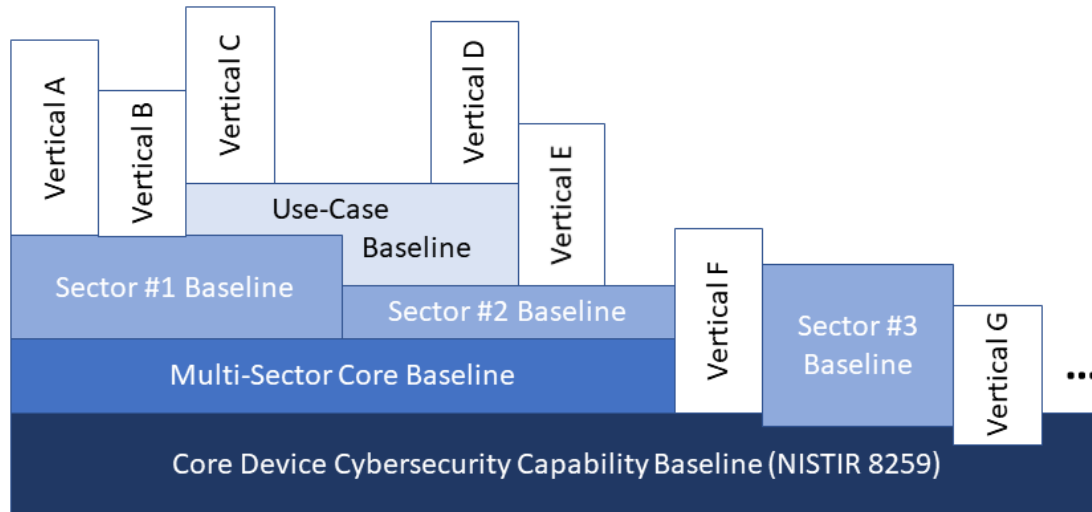
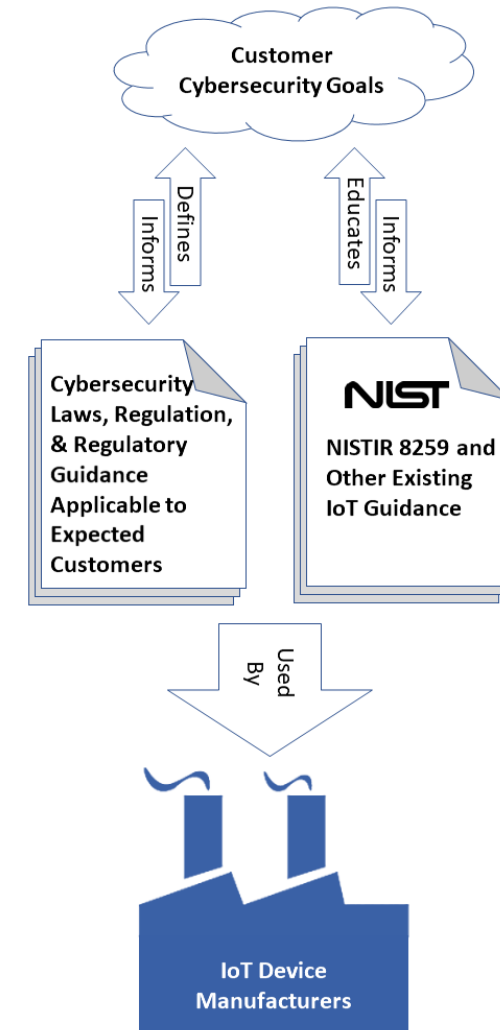
There are many potential considerations for what information a manufacturer communicates to customers for a particular IoT product and how that information will be communicated. Examples of topics are:

- Cybersecurity risk-related assumptions that the manufacturer made when designing and developing the device
- Support and lifespan expectations
- Device cybersecurity capabilities that the device provides, as well as cybersecurity functions that can be provided by a related device or a manufacturer service or system
- Device composition and capabilities, such as information about the device's software, firmware, hardware, services, functions, and data types
- Software and firmware updates
- Device retirement options



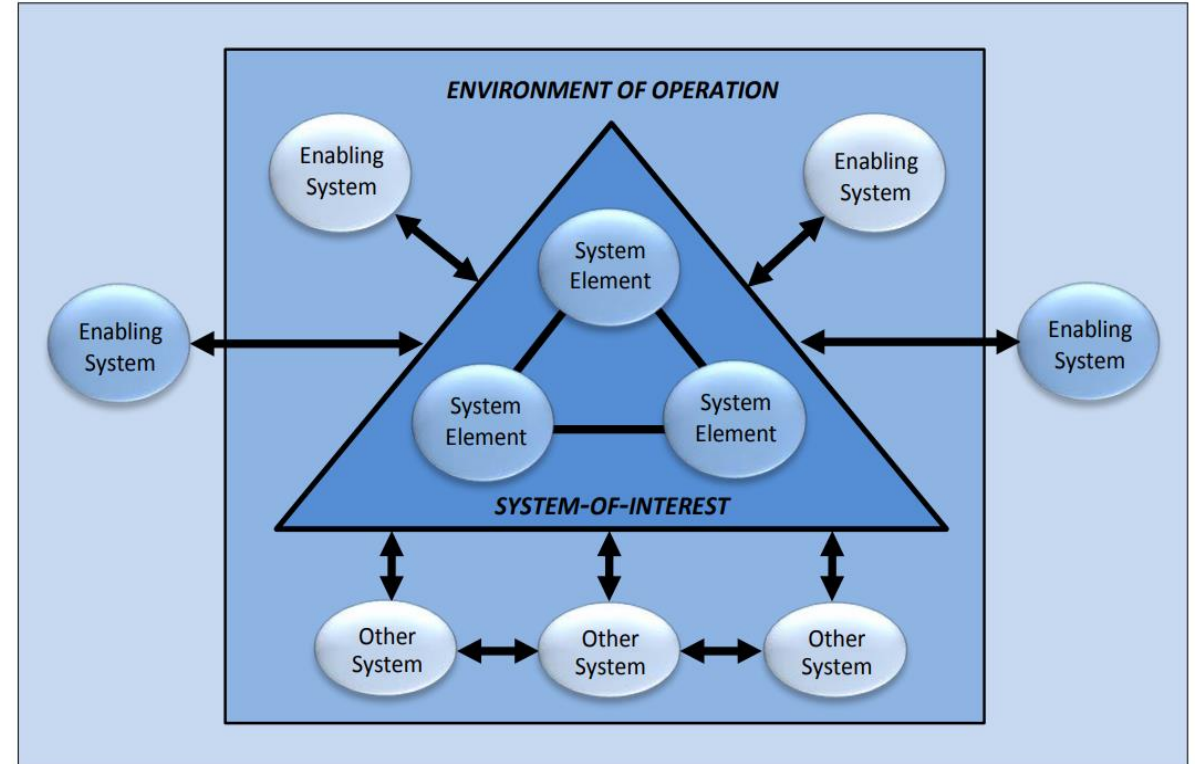
Using the Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline

- Guided by expected customers and use cases, existing and future guidance can be used to further identify and define device cybersecurity capabilities
- Not all customers and use cases will have such explicit guidance
 - Complicating the task for manufacturers
- The Core Device Cybersecurity Capability Baseline can be extended for sectors and use cases to give further guidance on needed device cybersecurity capabilities



Next: Develop the Federal IoT Device Baseline

- NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal systems
- Pursuant to Roadmap Action 2.3: Develop Federal Baseline NIST has started working on a Federal Baseline for IoT Devices
- Recognizing that agencies acquire IoT devices that are an element of a federal system that operates in a Federal Government environment, the goal is to provide Federal Agencies with guidance on Baseline Security Capabilities for IoT devices used within a federal system



For the Federal Government as a customer there is extensive guidance for Federal IT systems that can be used to identify customer goals

- While the customer is “known” the use cases are many a customer can use a generic baseline and tailor it, similar to the tailoring of NIST SP 800-53 baselines
- Ongoing analysis of existing guidance include:
 - Risk Management Framework
 - Cybersecurity Framework
 - FIPS Standards for Security Categorization of Federal Information and Information Systems
 - Cybersecurity Framework
 - NIST SP 800-53 Security and Privacy Controls
 - Guidance needed on applying existing body of knowledge to IoT and IoT devices
 - Surfacing cybersecurity assumptions of IT (NISTIR 8228)
 - Special considerations for different risk levels of Federal systems
 - Special tailoring of implementing controls may be needed



Federal Baseline development steps

- Kicked off the effort with Federal Stakeholders – Nov. 19, 2019 at Federal Computer Security Managers Forum
- Planning workshops and essays to invite feedback
- Plan to release draft in 3QFY2020 for public comment



Q & A



*Have a question or an idea? We want to hear from you!
We're always accepting thoughtful feedback at
iotsecurity@nist.gov*



@NISTcyber
#IoTSecurityNIST



iotsecurity@nist.gov



<https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>

We welcome **your** written
feedback at:
iotsecurity@nist.gov



Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

