Manufacturing and IoT

September 15, 2019

Why does IoT cybersecurity matter to manufacturers?

- Connected devices at higher risk
- Even small manufacturers are probably using connected devices in current operations
- Some may not realize that non-ICS connected devices leave systems, data and more at high risk
- IoT devices have a wide range of vulnerabilities
- Securing IoT requires different methods than traditional devices
- Connected devices have a wide range of vulnerabilities
- Cost of breaches high

How can I help manufacturers protect themselves from IoT security risks?

- NIST's Cybersecurity for IoT Program is making progress with voluntary guidelines to help manufacturers secure operations
- Even if currently not manufacturing connected devices, learning cybersecurity and privacy risks for IoT devices compared with conventional IT devices can help them prepare for future
- Understanding considerations that affect IoT device security can help inform procurement of most secure, effective solutions for current and future operations

About the NIST Cybersecurity for IoT Program

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

The Program supports the development & application of standards, guidelines, and related tools to improve the cybersecurity of connected devices & the environments in which they are deployed.

By collaborating with stakeholders across government, industry, international bodies and academia, the program aims to cultivate trust & foster an environment that enables innovation on a global scale.

Cybersecurity for IoT Program Principles

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.

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.

Outcome-Based Approach

Embrace an 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.

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.

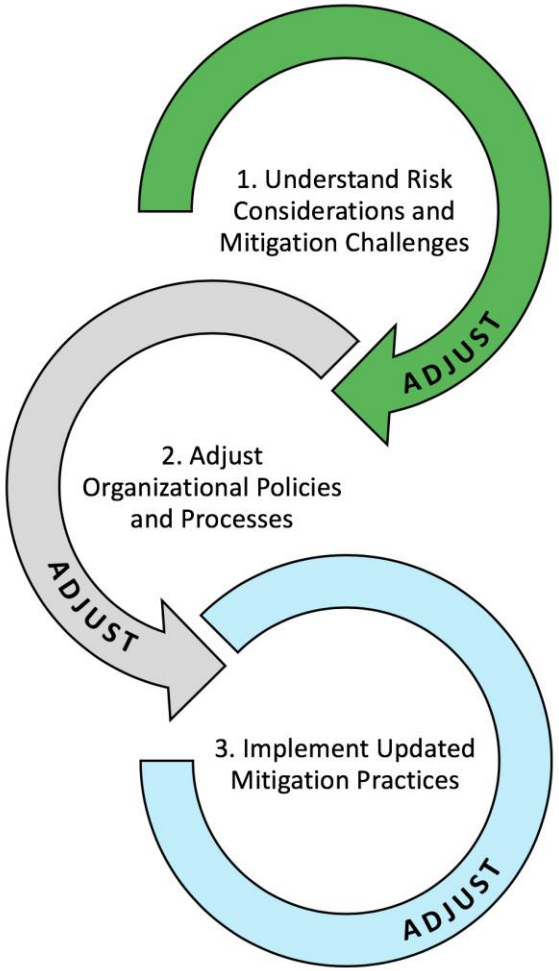
Stakeholder Engagement

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

NISTIR 8228: Navigating the Process of Identifying and Addressing IoT Cybersecurity and Privacy Risks

The publication walks readers through the process of considering IoT cybersecurity and privacy risks, by:

1. Defining capabilities IoT devices can provide, particularly those with most potential to affect cybersecurity and privacy risk.
2. Describing considerations that may affect the management of cybersecurity and privacy risks for IoT devices.
3. Exploring how the risk considerations may affect mitigating cybersecurity and privacy risk for an organization's IoT devices.
4. Providing organizations recommendations on how to address the risk considerations for their IoT devices.



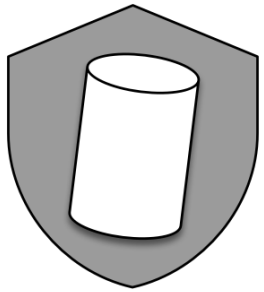
Cybersecurity and Privacy Risk Considerations

Risk Consideration	Cybersecurity Perspective	Privacy Perspective
1. Device Interactions with the Physical World	Cybersecurity incident could result in physical harm.	Ubiquity of sensors can contribute to the aggregation and analysis of enormous amounts of data about individuals.
2. Device Access, Management, and Monitoring Features	Lack of a user interface could result in inability to patch or update the device.	Lack of a user interface could make it difficult for individuals to know what PII devices are collecting and how the PII will be processed.
3. Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness	Many IoT devices do not or cannot support a range of cybersecurity and privacy capabilities.	

IoT Risk Mitigation Goals

Protect Device Security

Prevent a device from being used to conduct attacks, including participating in distributed denial of service (DDoS) attacks against other organizations, and eavesdropping on network traffic or compromising other devices on the same network segment. This goal applies to all IoT devices.



Protect Data Security

Protect the confidentiality, integrity, and/or availability of data (including PII) collected by, stored on, processed by, or transmitted to or from the IoT device. This goal applies to each IoT device with one or more data capabilities unless it is determined that none of the device's data needs its security protected.

Protect Individuals' Privacy

Protect individuals' privacy impacted by PII processing beyond risks managed through device and data security protection. This goal applies to all IoT devices that process PII or directly impact individuals.

Mitigation Goals and Areas

Goal 1: Protect Device Security	Goal 2: Protect Data Security	Goal 3: Protect Individuals' Privacy
Asset Management: Maintain a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices' lifecycles in order to use that information for cybersecurity and privacy risk management purposes. **Vulnerability Management**: Identify and eliminate known vulnerabilities in IoT device software and firmware in order to reduce the likelihood and ease of exploitation and compromise. **Access Management**: Prevent unauthorized and improper physical and logical access to, usage of, and administration of IoT devices by people, processes, and other computing devices. **Device Security Incident Detection**: Monitor and analyze IoT device activity for signs of incidents involving device security.	**Data Protection**: Prevent access to and tampering with data at rest or in transit that might expose sensitive information or allow manipulation or disruption of IoT device operations. **Data Security Incident Detection**: Monitor and analyze IoT device activity for signs of incidents involving data security.	**Information Flow Management**: Maintain a current, accurate mapping of the information lifecycle of PII, including the type of data action, the elements of PII being processed by the data action, the party doing the processing, and any additional relevant contextual factors about the processing to use for privacy risk management purposes. **PII Processing Permissions Management**: Maintain permissions for PII processing to prevent unpermitted PII processing. **Informed Decision Making**: Enable individuals to understand the effects of PII processing and interactions with the device, participate in decision-making about the PII processing or interactions, and resolve problems. **Disassociated Data Management**: Identify authorized PII processing and determine how PII may be minimized or disassociated from individuals and IoT devices. **Privacy Breach Detection**: Monitor and analyze IoT device activity for signs of breaches involving individuals' privacy.

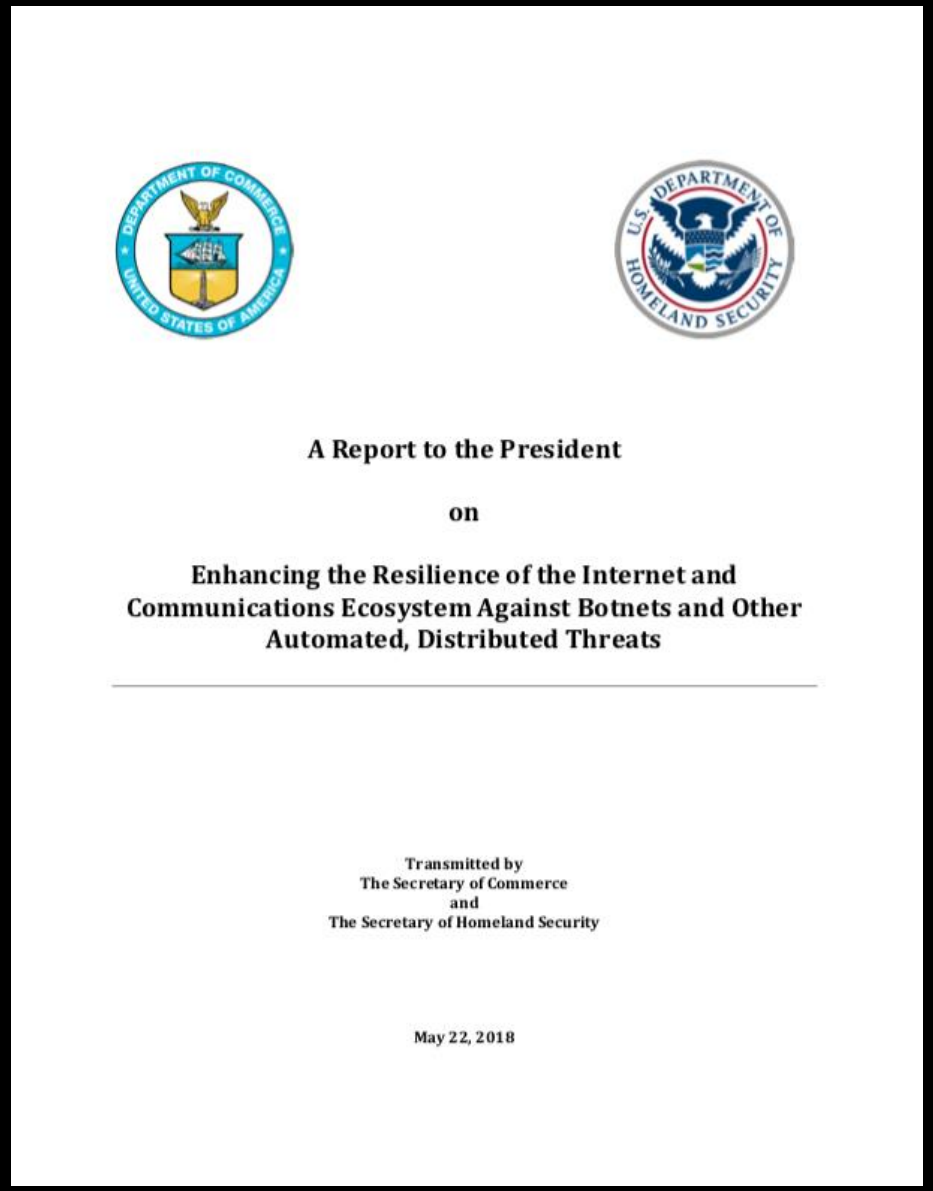
NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks

NISTIR 8228 - Final version was published on July 31, 2019

- NIST received more than 25 sets of comments from orgs including Amazon, Boeing, Chamber of Commerce, CTA, CTIA, ITI, Microsoft, Raytheon, Symantec, and many more on previous draft release.

Approaches risk management from the organizational use of IoT, but what about the **manufacturers of devices**?

- Multiple existing efforts, domestic and international were analyzed, and 15 common features identified included in draft Appendix.
- **Key takeaway and follow-on**: continued engagement to develop stand-alone cybersecurity baseline for IoT devices.



A Report to the President

on

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

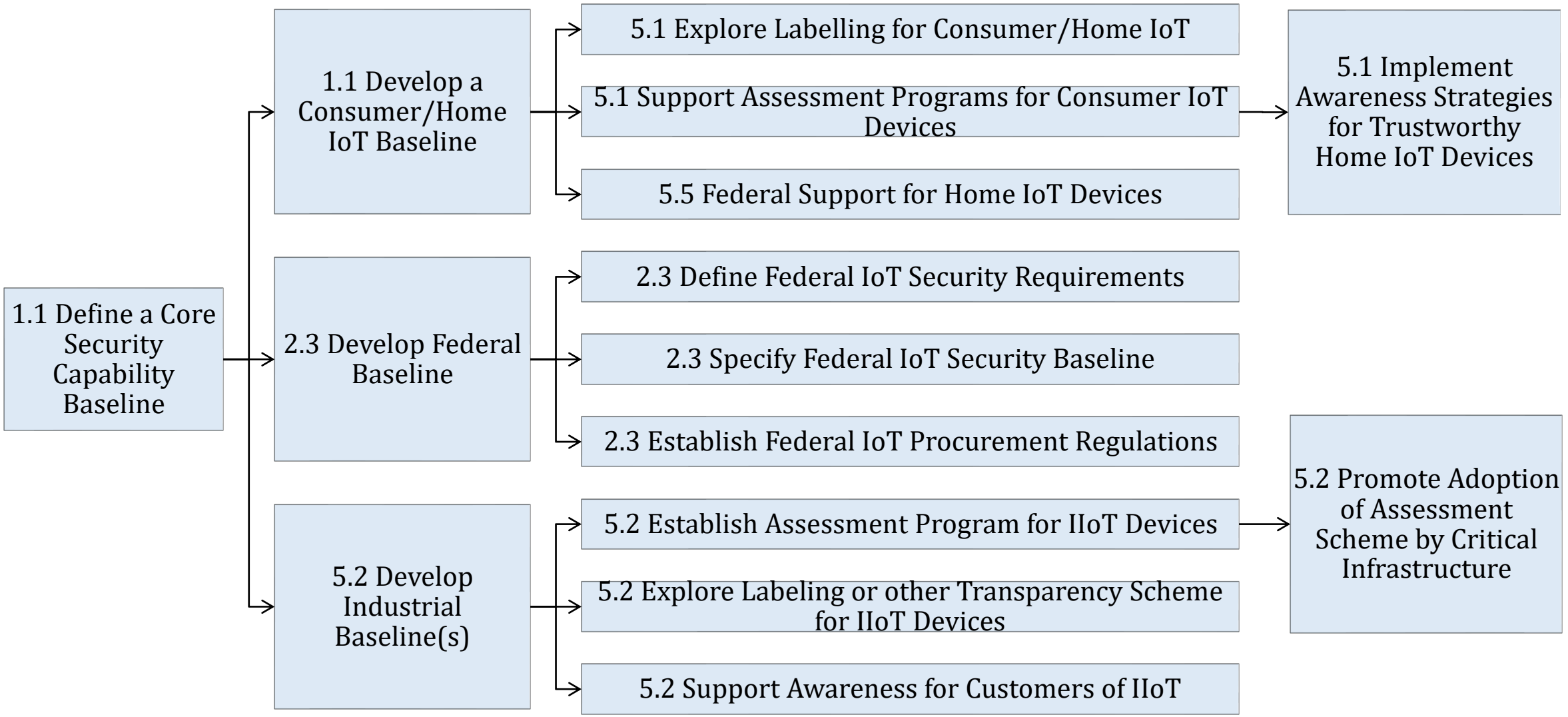
A Roadmap Toward IoT Security

- In response to Executive Order 13800 issued by the President on May 11, 2017, DoC and DHS delivered a report to the President in May, 2018 on the Resilience of the Internet against Botnet and other threats
- IoT security identified as a key unpinning component
- The Roadmap **charts a path** forward and **sets out a series of tasks** and deadlines laid out in the Report to the President
- The roadmap is a **plan for coordinating efforts among government, civil society, technologists, academics, and industry** sectors to develop a comprehensive strategy for fighting these threats.
- The roadmap is a **starting point**, and will likely identify new tasks as the work evolves.

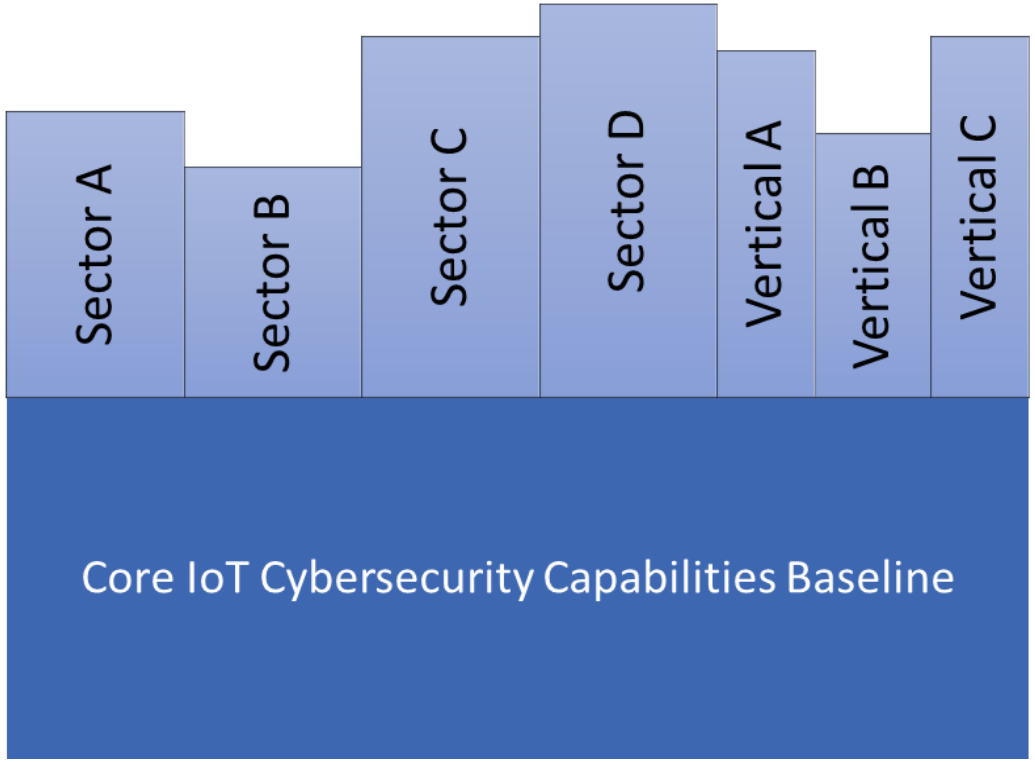
The Roadmap's IoT Line of Effort lays out an action plan to establish a robust market for trustworthy IoT devices

- The **Baseline document is a foundation** to the follow on actions
- Two workstreams under IoT line of effort:
    - IoT Workstream 1: Developing Robust Markets for Trustworthy IoT Devices
        - Focuses on the development of robust market for devices that offer appropriate security capabilities for three sectors: **consumer/home users, industrial users and the federal government**
    - IoT Workstream 2: Adoption and Sustainability for IoT Security
        - Focuses on the **development of the global ecosystem for IoT devices in general**

IoT Line of Effort



Identifying a core baseline of security features for devices



NIST published an essay inviting stakeholder feedback to inform development of the Core IoT Baseline

Criteria to Assess Core Baseline Candidates

- **Utility:** How critical is the feature towards improving security?
- **Verifiability:** Can the manufacturer easily verify implementation of feature in an IoT device?
- **Feasibility:** Are there roadblocks to implementing the feature: cost, complexity, interoperability?

1. **Elaboration of features and informative references to further inform the meaning of the features.** In the essay, they were too high-level.
2. **Optional features for consideration**: although some technology may not be currently available – e.g., stakeholders noted standards expected in near future.
3. **Other considerations for manufacturers of devices beyond the baseline items:**. This includes but is not limited to: device development and other pre-market business practices/processes; post-market business practices/processes.
4. **Considerations in the baseline for device constraints when adaption may be appropriate.** Some features, even at the high-level, are not appropriate for all cases; devices that will/must be managed are also different than "unmanaged" devices.

Feedback on Draft Essay

1. **Elaboration of capabilities and informative references to further inform the meaning of the capabilities.** In the essay, they are too high-level.
2. **Optional capabilities for consideration**: although some technology may not be currently available – e.g., stakeholders noted standards expected in near future.
3. **Other considerations for manufacturers of devices beyond the baseline items.** This includes but is not limited to: device development and other pre-market business practices/processes; post-market business practices/processes.
4. **Considerations in the baseline for device constraints when adaption may be appropriate.** Some capabilities, even at the high-level, are not appropriate for all cases—e.g. supporting full crypto may cause an over-provisioning of computing resources; devices that will/must be managed are also different than "unmanaged" devices..

PUBLICATIONS

NISTIR 8259 (DRAFT)

Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers

Date Published: July 2019
Comments Due: September 30, 2019
Email Comments to: iotsecurity@nist.gov

Author(s)

Michael Fagan (NIST), Katerina Megas (NIST), Karen Scarfone (Scarfone Cybersecurity), Matthew Smith (G2)

Announcement

Manufacturers are creating an incredible variety and volume of Internet of Things (IoT) devices. Manufacturers need to understand the cybersecurity risks their customers face so IoT devices can provide cybersecurity features that make them at least minimally securable by the individuals and organizations who acquire and use them. This approach can help lessen the

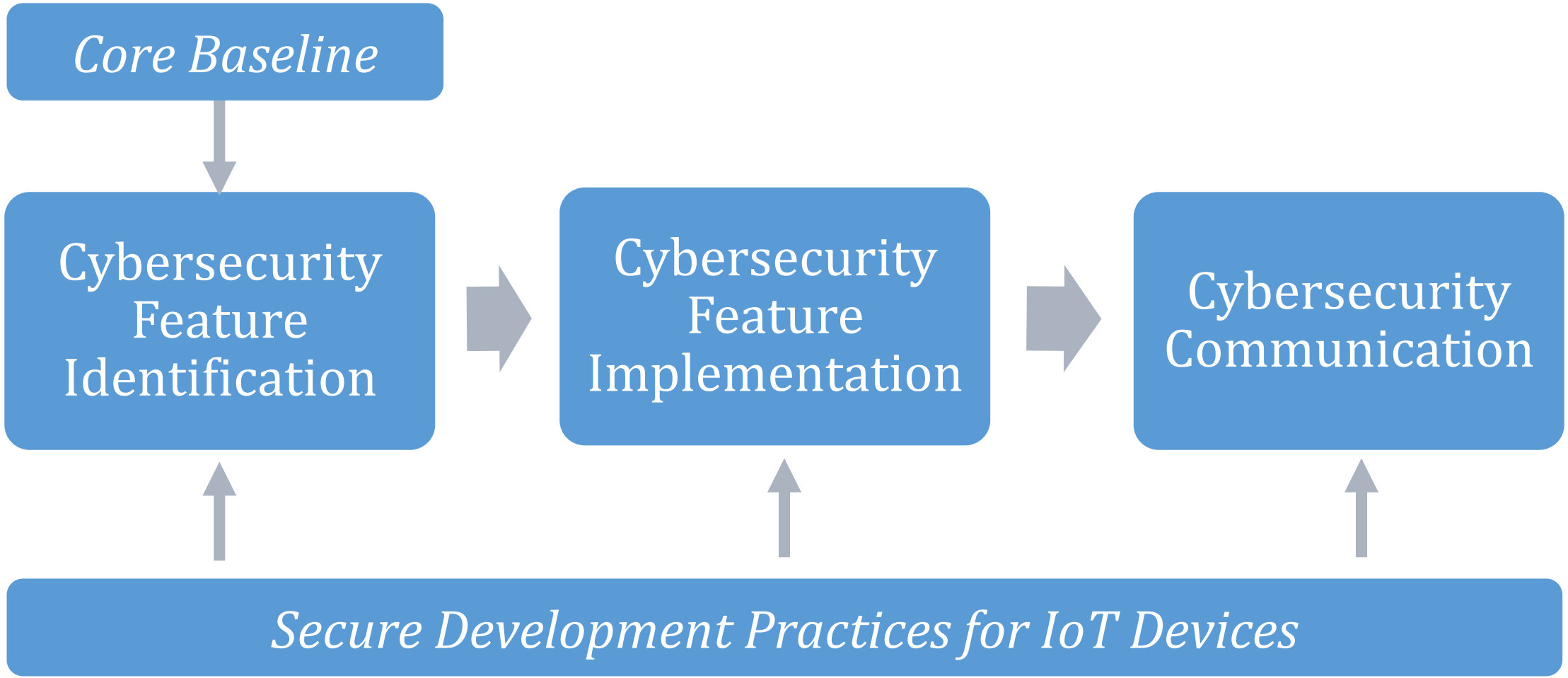
DOCUMENTATION

Publication:
NISTIR 8259 (DRAFT) (DOI)
Local Download

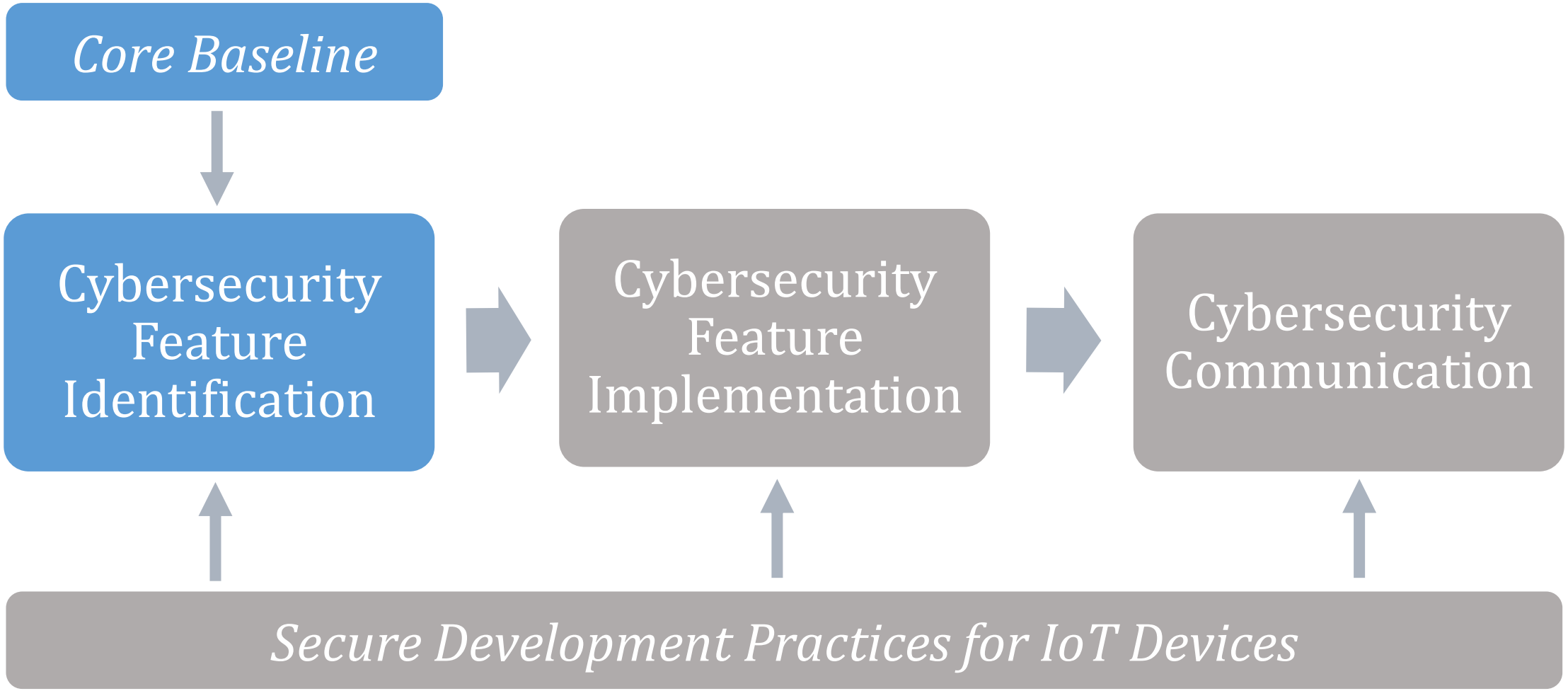
Supplemental Material:
NIST news article (other)

Related NIST Publications:
NISTIR 8228

Draft NISTIR 8259 defines a process manufacturers can use to develop inherently more *securable* IoT devices



First, manufacturers should identify the cybersecurity features their customers may need



Cybersecurity Feature Identification

Determine expected customers and use cases

- Who will use the device?
- How and where will they use it?

Understand customers' cybersecurity wants and needs

- Device management
- Configurability
- Network characteristics
- Nature of device data created, stored, and/or used
- Level of access to devices when deployed

Core baseline is a **starting point** for feature identification

The **Core Cybersecurity Feature Baseline** is the set of features needed by a *generic* customer:

Device Identification

The IoT device can be uniquely identified logically and physically.

Device Configuration

The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.

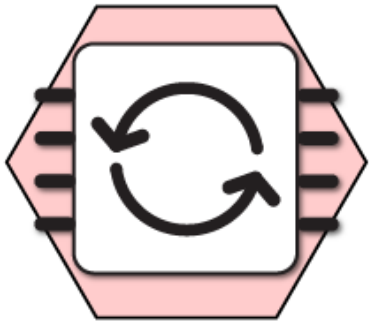
Data Protection

The IoT device can protect the data it stores and transmits from unauthorized access and modification.

The **Core Cybersecurity Feature Baseline** is the set of features needed by a *generic* customer:

Interface Access

The IoT device can limit logical access to its local and network interfaces to authorized entities only.



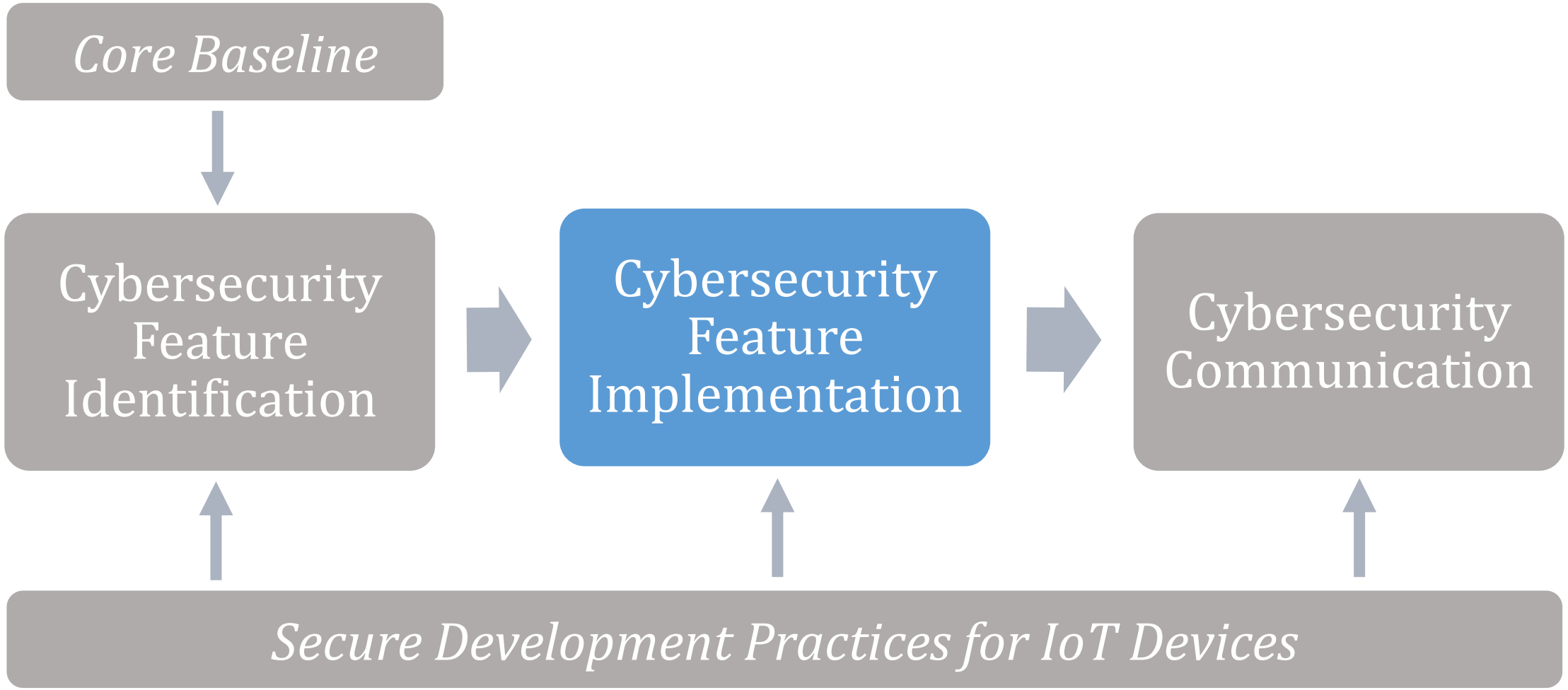
Software & Firmware Update

The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.

Security Event Logging

The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

When features are identified, their **implementations** should be considered



Feature Implementation

Should consider the device and its technical specifications

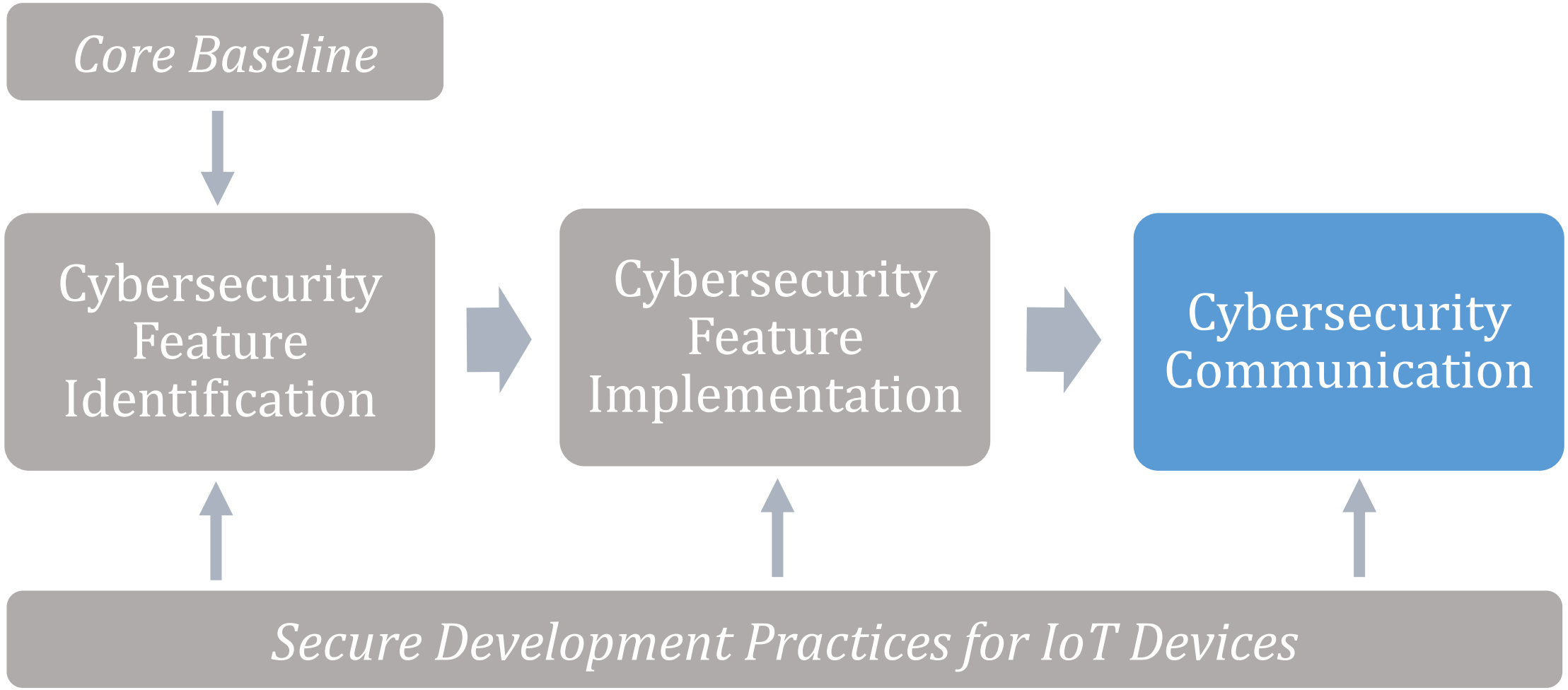
- Select or build a device with sufficient hardware resources to support the desired features
  - Be forward-looking and size hardware resources for potential future use
- Use hardware-based cybersecurity features
- Disable unneeded features provided by hardware, firmware, and/or the operating system
- Do not force the use of features that may negatively impact operations
- Consider using established IoT platform instead of acquiring and integrating hardware, firmware and supporting software components

Feature Implementation

Should consider where key elements of cybersecurity features may be inherited from other devices or aspects of the use case

- An IoT device intended for use in an environment with physical security controls in place
- An IoT device that is dependent on an IoT gateway or hub for its communications
- An IoT device fully contained within another IoT device

Once features are more thoroughly defined, attention should still be given to **communication** with customers



Cybersecurity Communication: Device & Features

Device cybersecurity features

- Which cybersecurity features the device provides
- How these features may affect risk
- Features customer may expect the device to provide that are not provided & why not provided

Device transparency

- Usable information on cybersecurity-related aspects of the device
- An inventory of the IoT device's current internal software and firmware
- A list of sources of all of the IoT device's software, firmware, hardware, and services
- Sufficient information on the IoT device's operational characteristics
- A list of the functions the IoT device performs

Cybersecurity Communication: Support & Lifespan

Software and firmware update transparency

- If and when updates will be made available
- Circumstances under which updates will be issued
- Who will be responsible for performing updates
- Notification if installing an update may alter existing configuration settings
- Update availability and contents

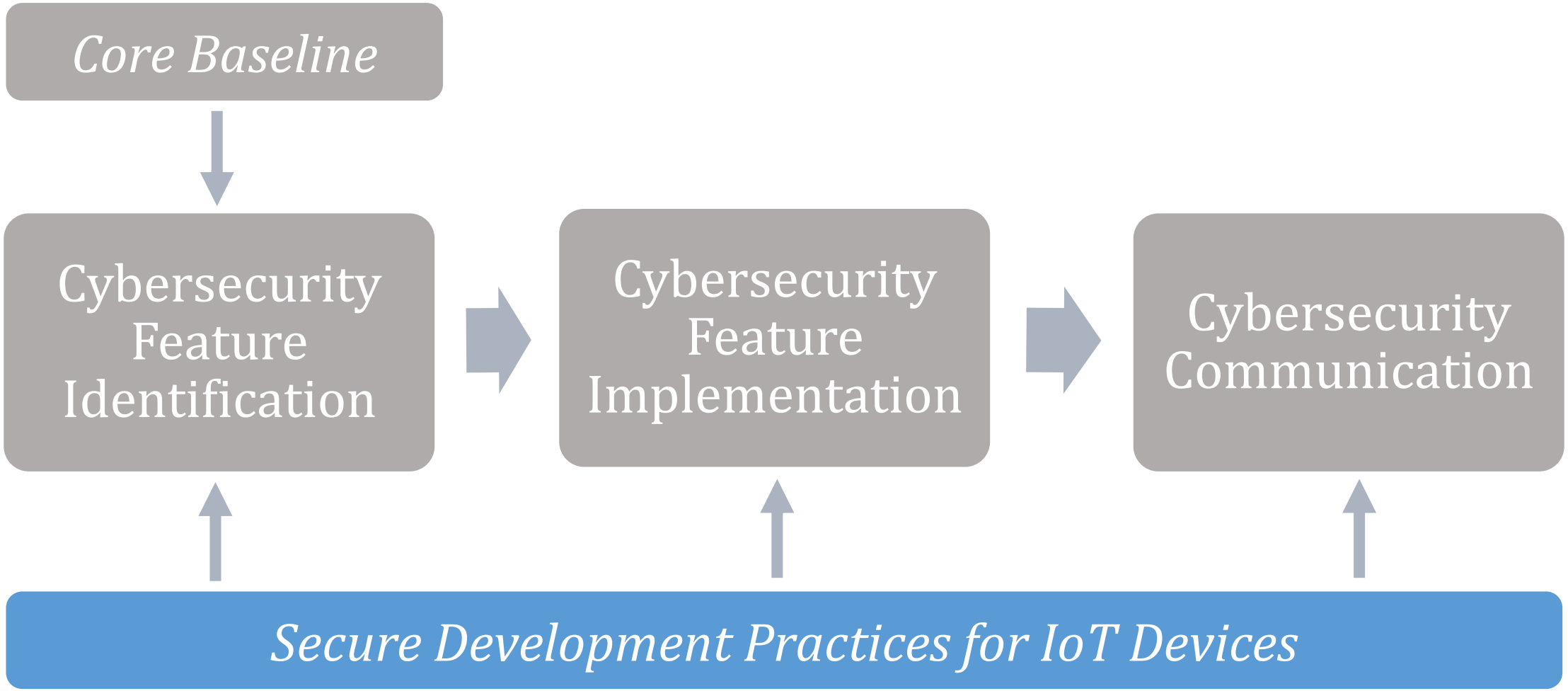
Support and lifespan expectations

- Timeframe for the end of product support
- The timeframe for product end-of-life
- What functionality, if any, the device will have after support ends and at end-of-life

Decommissioning

- Provide sufficient information on whether the device can be decommissioned & how to decommission it

Throughout the process, **secure development practices** can inform and facilitate each step



Highlighted Secure Development Practices for IoT

NIST white paper, Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), can help guide IoT device manufacturers

- Ensure workforce has necessary skills to securely develop IoT devices
- Take steps to protect code & give customers ability to verify software integrity
- Take steps to reduce vulnerabilities in IoT devices
- Accept and respond to vulnerability reports

Share your feedback on Draft NISTIR 8259

- Access Draft NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* at https://csrc.nist.gov/publications/detail/nistir/8259/draft
- **Comments Due: September 30, 2019**
- Email Comments to: iotsecurity@nist.gov
- Follow the conversation on Twitter using #IoTBaseline

Questions?

Resources

NIST Resources

- A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats
- A Road Map Toward Resilience Against Botnets
- NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
- Discussion Draft: Considerations for a Core IoT Cybersecurity Capabilities Baseline
- Draft NISTIR 8259: Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufactu
- Framework for Improving Critical Infrastructure Cybersecurity Version 1.1
- NISTIR 8183: Cybersecurity Framework Manufacturing Profile
- Cybersecurity for Smart Manufacturing Systems
- Video: What is the Internet of Things (IoT) and how can we secure it?

Resources

NCCoE Resources

- NISTIR 8219: Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection
- Securing Small Business and Home IoT Devices: Mitigating Network-Based Attacks using Manufacture Usage Description (MUD) Practice Guide

Resources

Other Government Resources

- Careful Connections: Building Security in the Internet of Things (FTC)
- Securing the Internet of Things (DHS CSIA)

Articles

- Manufacturing industry at higher risk of cyberattacks thanks to industrial IoT
- Cyber Secure Manufacturing Is Smart Manufacturing
- Industrial IoT Security: How to Protect Smart Manufacturing
- How IoT Opens the Door for Insider Attacks Against Industrial Infrastructure
- 2018 Vectra spotlight report: The Increased Risk of Cyberattacks against Manufacturing Organizations

Thank you!

@NISTcyber
#IoTSecurityNIST

iotsecurity@nist.gov

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