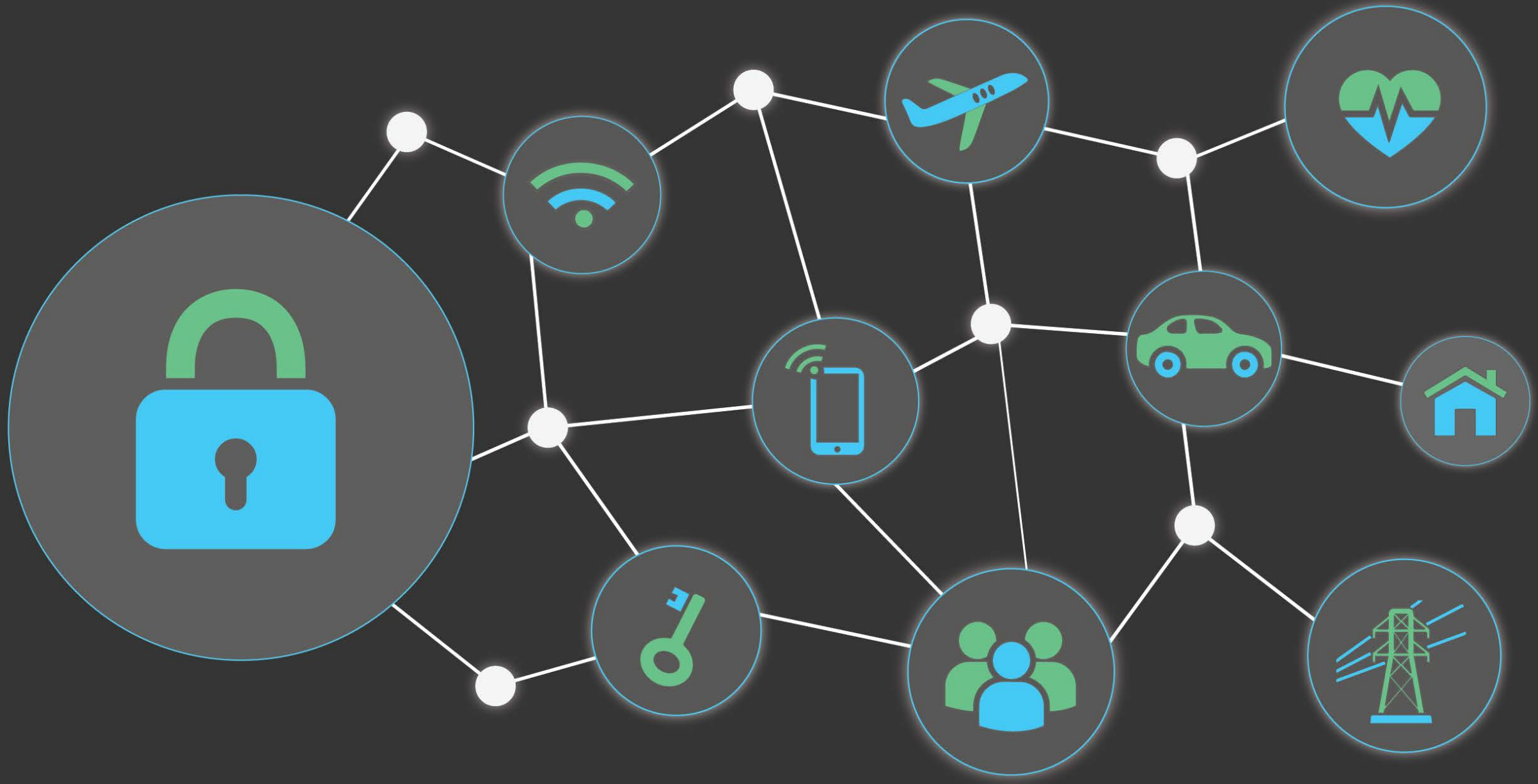


NIST Cybersecurity for IoT Program

Update to ISPAB Board of Directors, August 2019

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

Research/Reports

- **Mitigating IoT-Based DDoS/Botnet Report**
- Vehicle-to-vehicle transportation
- 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)

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

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
  - Healthcare Sector Projects
    - Wireless Infusion Pumps, etc.
- Privacy Engineering Program

Cybersecurity for IoT Program Principles

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.

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.

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.

Ecosystem of Things

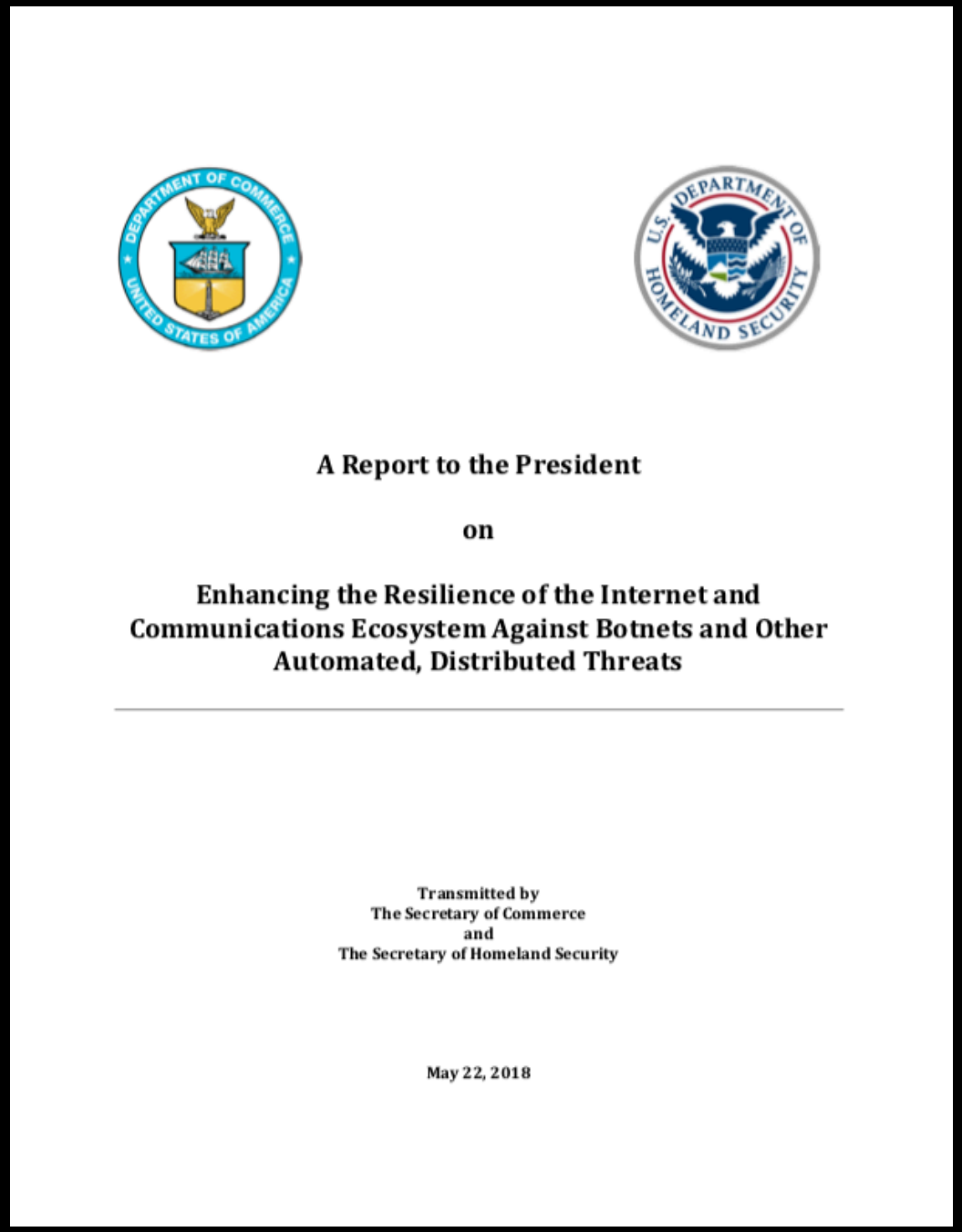
Recognizing that no device exists in a vacuum, NIST takes an ecosystem approach to IoT cybersecurity. For many devices, much of the functionality happens outside the device—not all the security is on the device itself. As such, we look at the entire ecosystem, not just endpoints.

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: Core Cybersecurity Feature Baseline for Securable IoT Devices

- NISTIR 8228 Final version was published on July 31, 2019
- NISTIR 8228 approaches risk management from the organizational use of IoT but what about **the manufacturers of devices**?
- In writing NISTIR 8228, multiple existing efforts, domestic and international were analyzed, and **15 common capabilities** identified included in Appendix A of NISTIR 8228.
- **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.
  - Key takeaway: In particular, **there was interest in continued engagement on Appendix A**, to develop cybersecurity and privacy baselines for IoT.
- Next step: **Developing a core cybersecurity capability baseline from the perspective of a device manufacturer.**



A Report to the President

on

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

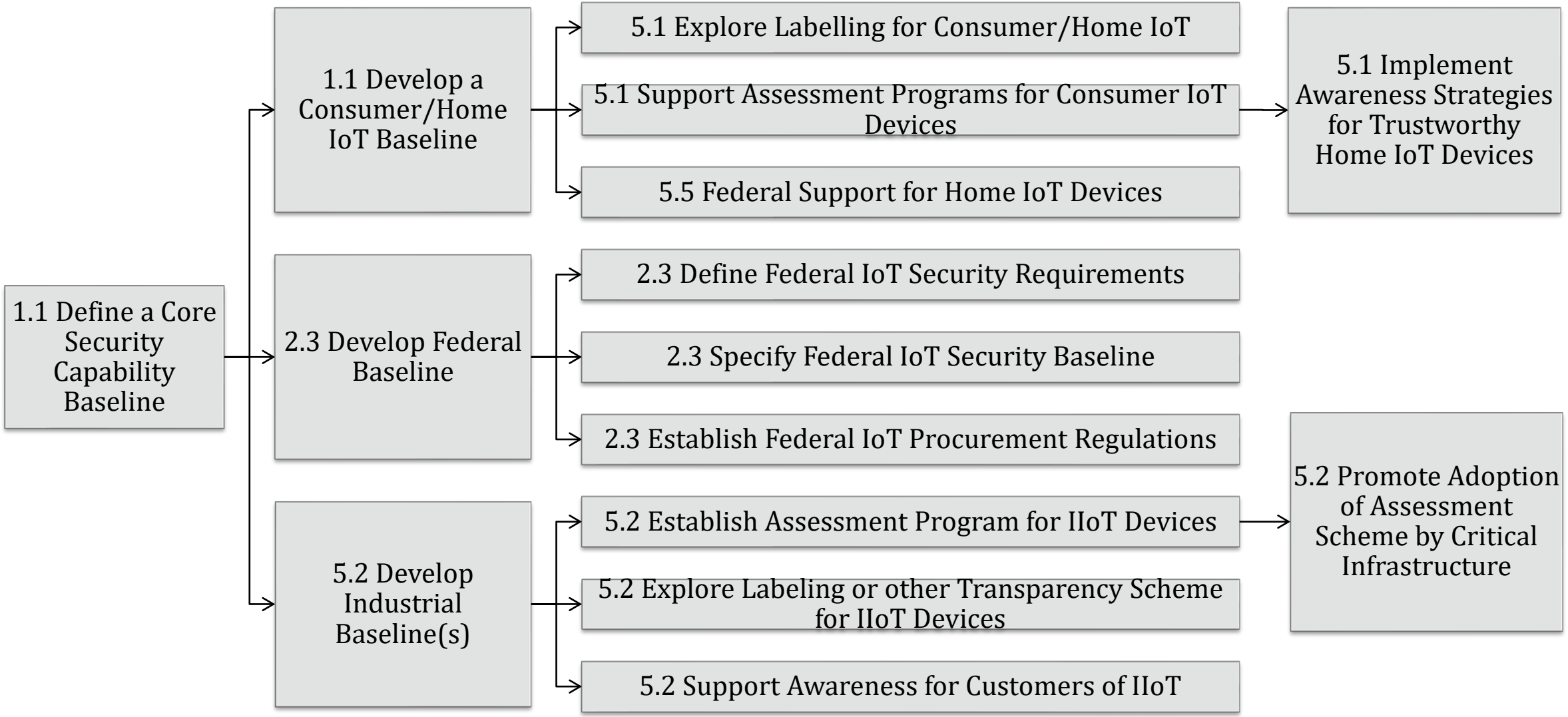
Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

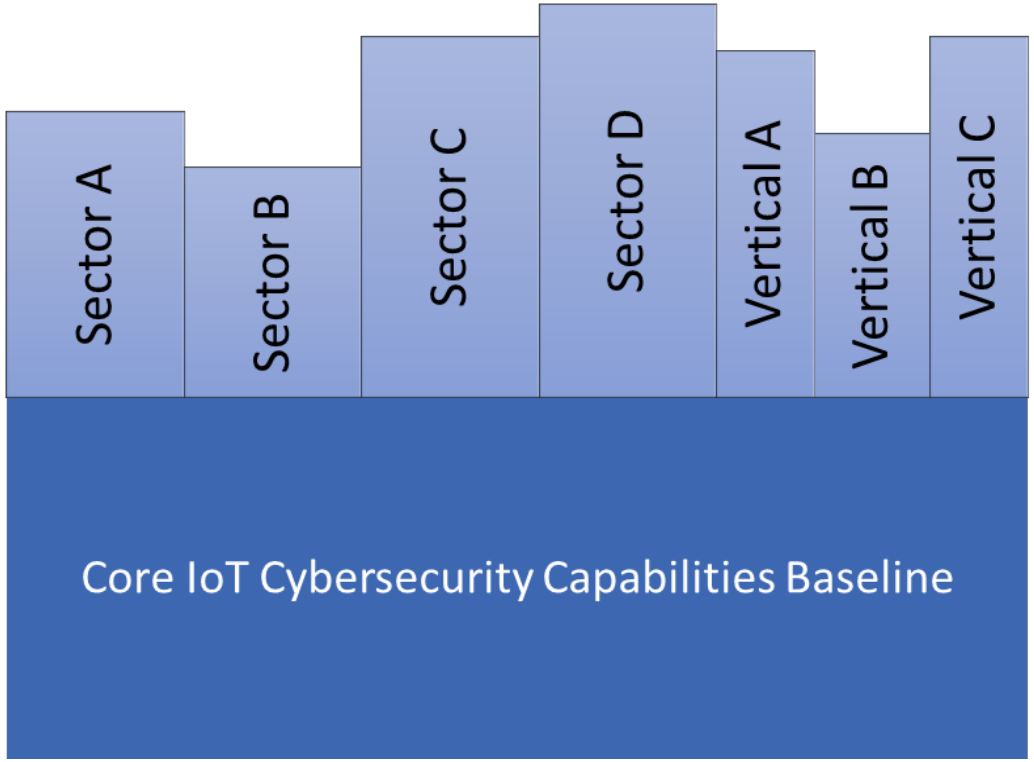
A Roadmap Toward IoT Security

- 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



Identifying a core baseline of security capabilities for devices



- **Risk-Based Understanding:** Our approach to managing risk is rooted in an understanding of how IoT can affect cybersecurity.
- **Ecosystem of Things:** Recognizing that no device exists in a vacuum, NIST takes an ecosystem approach to IoT cybersecurity.
- **Outcome-Based Approach:** Specify desired cybersecurity outcomes, allowing organizations to choose the best solution for each IoT device.
- **No One Size Fits All:** There is no one-size-fits-all approach to managing IoT cybersecurity risk.
- **Stakeholder Engagement:** NIST works with diverse stakeholders to advance IoT cybersecurity.

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

The IoT device can be identified both logically and physically.

The IoT device's software and firmware can be updated using a secure, controlled, and configurable mechanism.

Authorized users can securely change the IoT device's configuration, including restoration to a secure "default." Unauthorized changes to the IoT device's configurations can be prevented.

Local and remote access to the IoT device and its interfaces can be controlled.

The IoT device can use cryptography to secure its stored and transmitted data.

The IoT device can use industry-accepted, standardized protocols for all layers of the device's transmissions.

The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.

The IoT device can be reset by authorized users so all data-at-rest on the device is securely removed from all internal data storage.

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

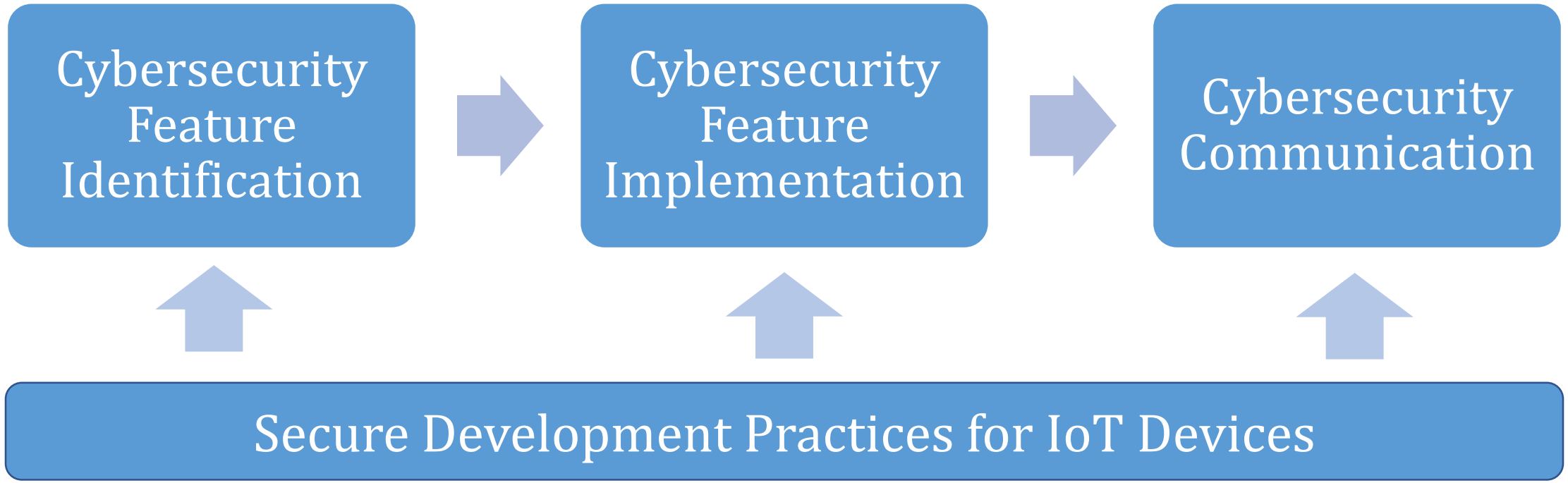
Supplemental Material:
NIST news article (other)

Related NIST Publications:
NISTIR 8228

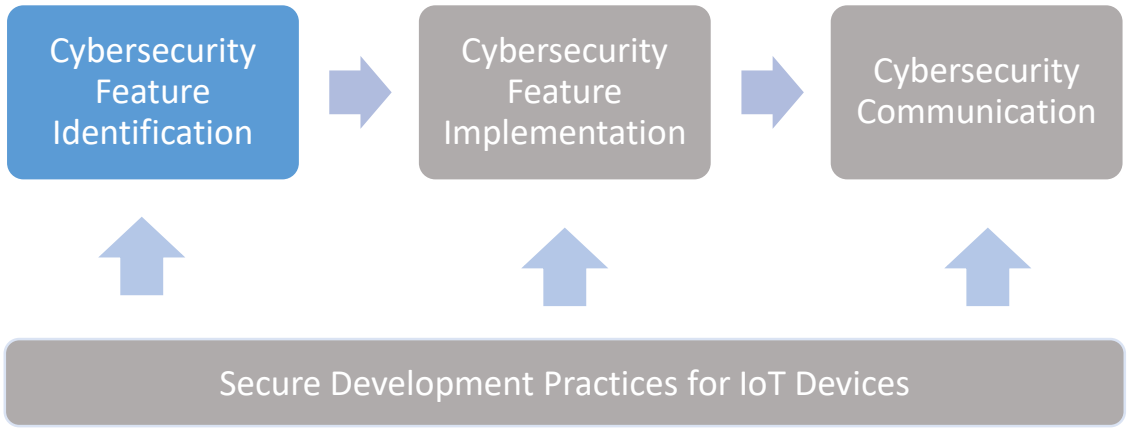
Feedback on Draft Essay

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..

Process for manufacturers to develop *securable* IoT devices



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

What if not much is known about all customers or the use case is broad?

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.
- *Logical Access to Interfaces* - The IoT device can limit logical access to its local and network 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 Event Logging* - The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

Core Baseline: Device Identification

The IoT device can be uniquely identified logically and physically.

Key Elements:

1. A unique logical identifier
2. A unique physical identifier on it at an external or internal location authorized entities can access

Note: the physical and logical identifiers may represent the same value, but they do not have to.

Core Baseline: Device Configuration

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

Key Elements:

1. The ability to change the device's software and firmware configuration settings
2. The ability to restrict configuration changes to authorized entities only
3. The ability for authorized entities to restore the device to a secure default configuration defined by an authorized entity

Core Baseline: Data Protection

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

Key Elements:

1. The ability to use accepted cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised
2. The ability for authorized entities to configure the cryptography use itself when applicable, such as choosing a key length
3. The ability for authorized entities to render all data on the device inaccessible by all entities, whether previously authorized or not (e.g., through a wipe of internal storage, destruction of cryptographic keys for encrypted data)

Core Baseline: Logical Access to Interfaces

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

Key Elements:

1. The ability to logically or physically disable any local and network interfaces that are not necessary for the core functionality of the device
2. The ability to logically restrict access to each network interface (e.g., device authentication, user authentication)
3. The ability to enable, disable, and adjust thresholds for any ability the device might have to lock or disable an account or to delay additional authentication attempts after too many failed authentication attempts

Core Baseline: Software and Firmware Update

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

Key Elements:

1. The ability to update all the device's software and firmware through remote (e.g., network download) and/or local means (e.g., removable media)
2. The ability to confirm the validity of any update before installing it
3. The ability to restrict updating actions to authorized entities only
4. The ability to enable or disable updating
5. The ability to set remote update mechanisms to be either automatically or manually initiated for update downloads and installations
6. The ability to enable or disable notification when an update is available and specify who or what is to be notified

Core Baseline: Cybersecurity Event Logging

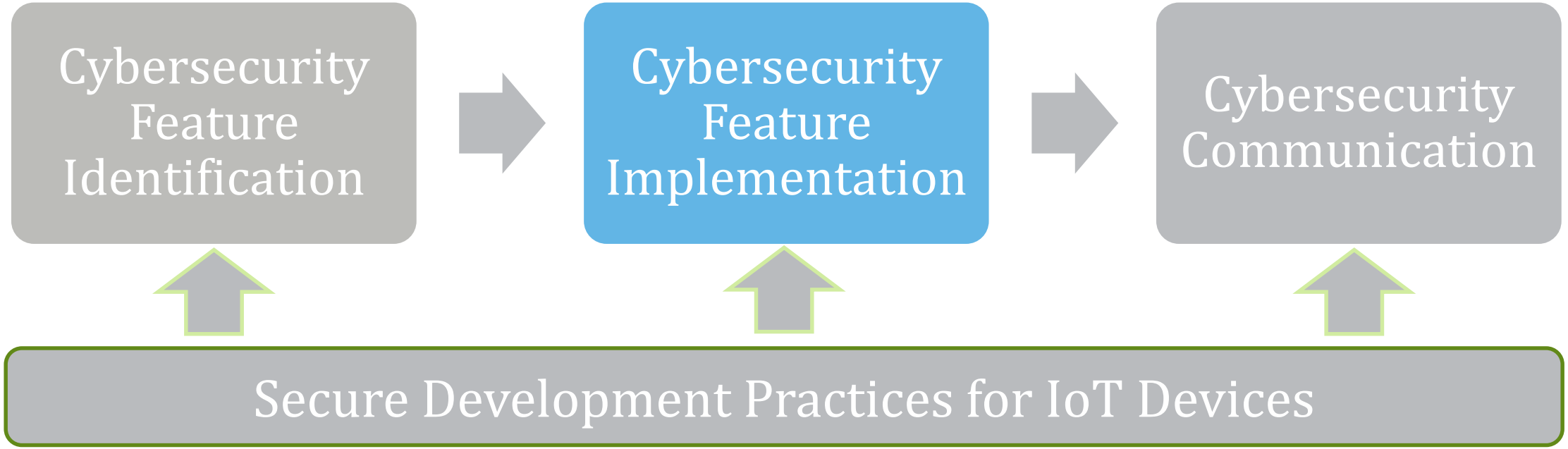
The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

Key Elements:

1. The ability to log cybersecurity events across the device's software and firmware
2. The ability to record sufficient details for each event to facilitate an authorized entity examining the log and determining what happened
3. The ability to restrict access to the logs so only authorized entities can view them
4. The ability to prevent any entities (authorized or unauthorized) from editing the logs
5. The ability to make the logs available to a logging service on another device, such as a log server

NISTIR 8259 provides consideration for cybersecurity feature implementation

- Device specification
  - Hardware considerations
  - Use of established platform
- Cybersecurity feature inheritance
  - Device design may impact implementation



Feature Implementation: Device 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
- Do not include 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

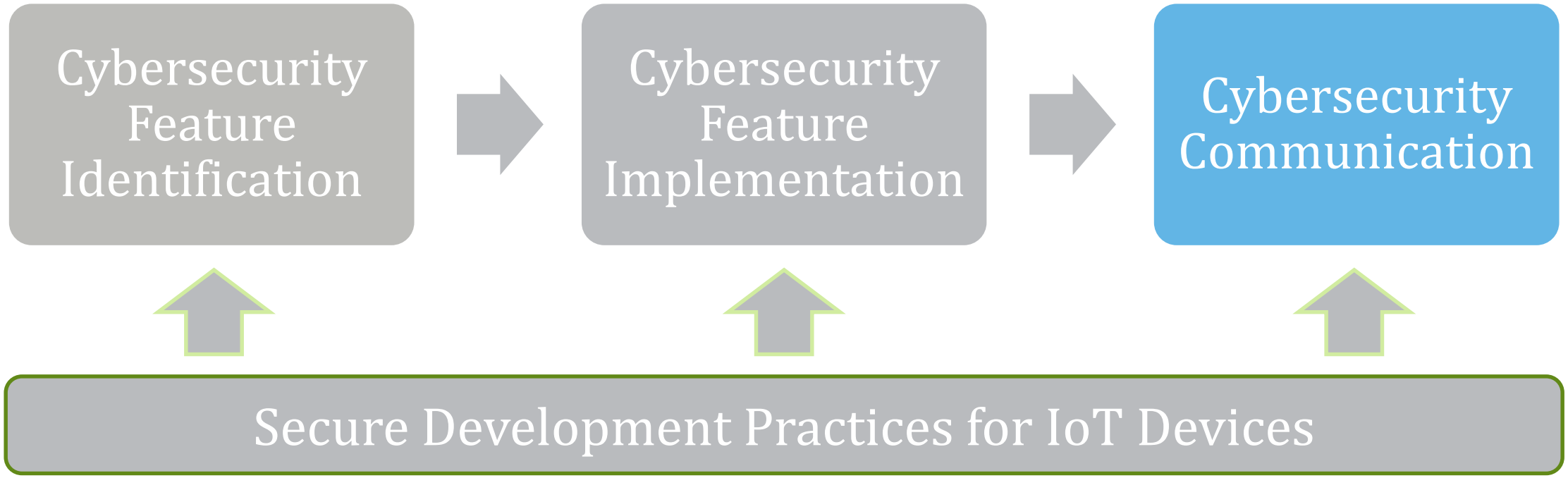
Feature Implementation: Feature Inheritance

IoT device design processes may determine that certain cybersecurity features can be omitted because equivalent protection will be inherited from elsewhere.

- An IoT device intended for use in an environment with stringent 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

Cybersecurity Communication

- Device cybersecurity features
- Device transparency
- Software and firmware update transparency
- Support and lifespan expectations
- Decommissioning



Cybersecurity Communication

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

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

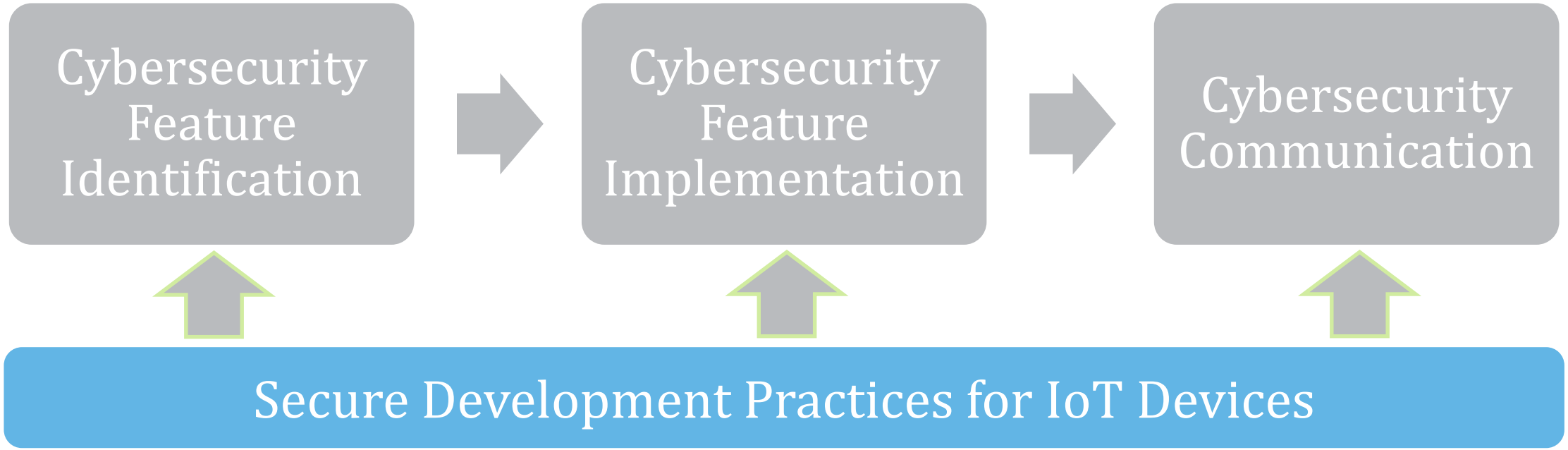
- Timeframe for the end of product support
- The timeframe for product end-of-life
- What functionality, if any, the device will have after support ends and at end-of-life

Decommissioning

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

Secure Development Practices for IoT Devices

- Workforce considerations
- Code protection and software integrity
- Vulnerability reduction
- Vulnerability reporting and handling



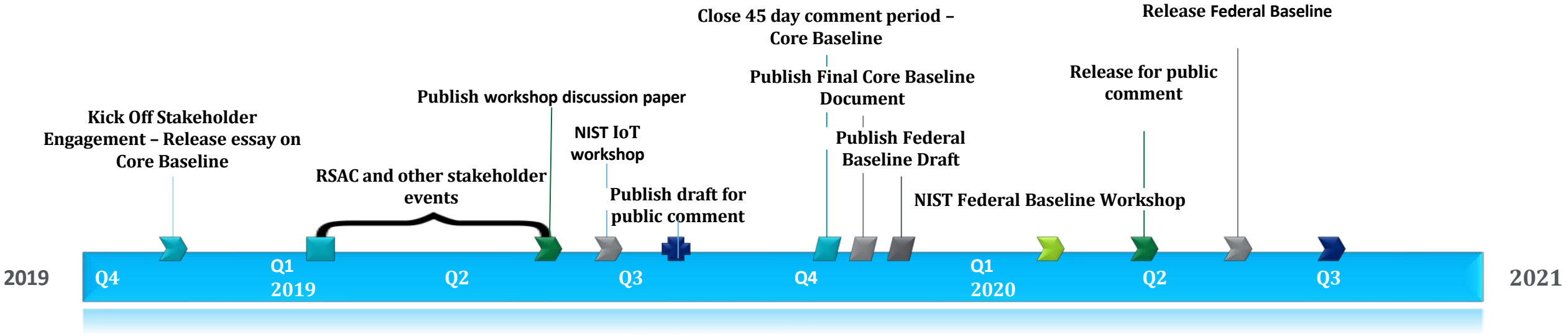
Secure Development Practices for IoT Devices

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

Next steps

1. Publish Draft for Public Comment core baseline NISTIR (July ‘19)
2. NIST Core Baseline Workshop & feedback sessions(August ‘19)
3. Provide comments on ISO/IEC 27030 working draft (August ‘19)
4. Attend ISO/IEC JTC1/SC 27 meeting (October ‘19)
5. Publish Final core baselines NIST publication (Winter ‘19)
6. Federal Government profile of IoT Baseline: (Spring ‘20)



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

@NISTcyber
#IoTSecurityNIST

We welcome **your** written feedback at:

iotsecurity@nist.gov

iotsecurity@nist.gov

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