Workshop on Core IoT Cybersecurity Baseline

August 13, 2019

Follow the conversation on Twitter!

@NISTcyber
#IoTBaseline

Note to Webcast Participants

- We will be using **Sli.do** to help facilitate questions and answers from remote participants
- To access Sli.do, visit **www.slido.com** and enter event code **#IOTBASELINE**

Agenda

9:00 – 9:20 Welcome Remarks

9:20 – 9:50 Overview of NIST Information Technology Lab's work in IoT cybersecurity

9:50 – 10:15 Overview Cybersecurity for IoT Program and background on Draft NISTIR 8259

10:15 – 11:15 Next Steps on the Road

11:15 – 11:30 Instructions for Breakouts

11:30 – 12:30 Lunch

12:30 – 2:30 Core Baseline Feedback Breakout

2:30 – 2:45 Break

2:45 – 3:30 Feedback Summary Panel

3:30 – 4:00 Closing remarks

Welcome Remarks

- **Katerina Megas**, Program Manager, Cybersecurity for IoT Program, NIST
- **Jim St. Pierre**, Deputy Director, Information Technology Laboratory, NIST

Overview of ITL's work in IoT cybersecurity

- **Kevin Stine**, Chief, Applied Cybersecurity Division, NIST
- **Mary Theofanos**, Computer Scientist, Material Measurement Laboratory, NIST

Overview Cybersecurity for IoT Program and background on Draft NISTIR 8259

- **Katerina Megas**, Program Manager, Cybersecurity for IoT Program, NIST
- **Michael Fagan**, Computer Scientist, Cybersecurity for IoT Program, NIST

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

Cybersecurity for IoT Program Principles

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.

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.

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.

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.

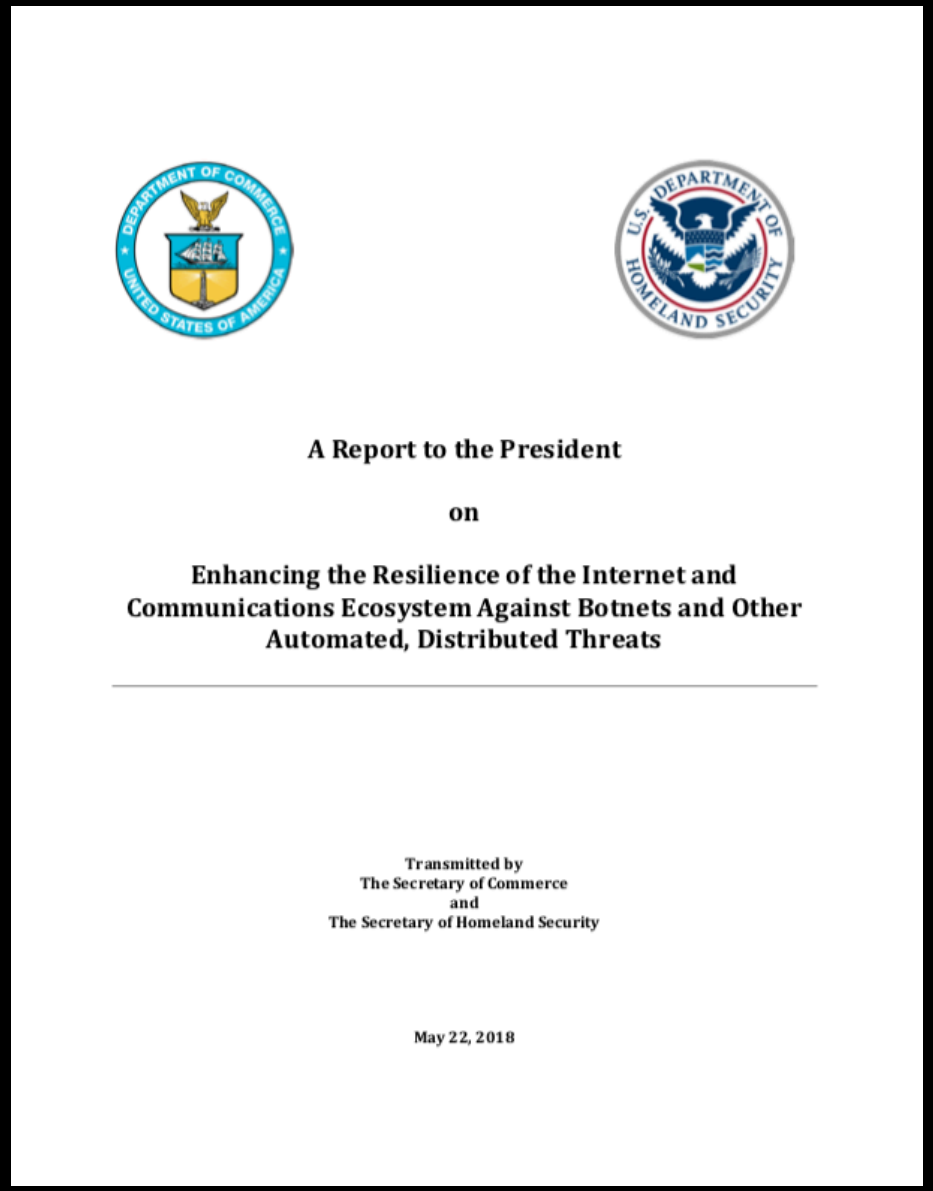
NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks

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

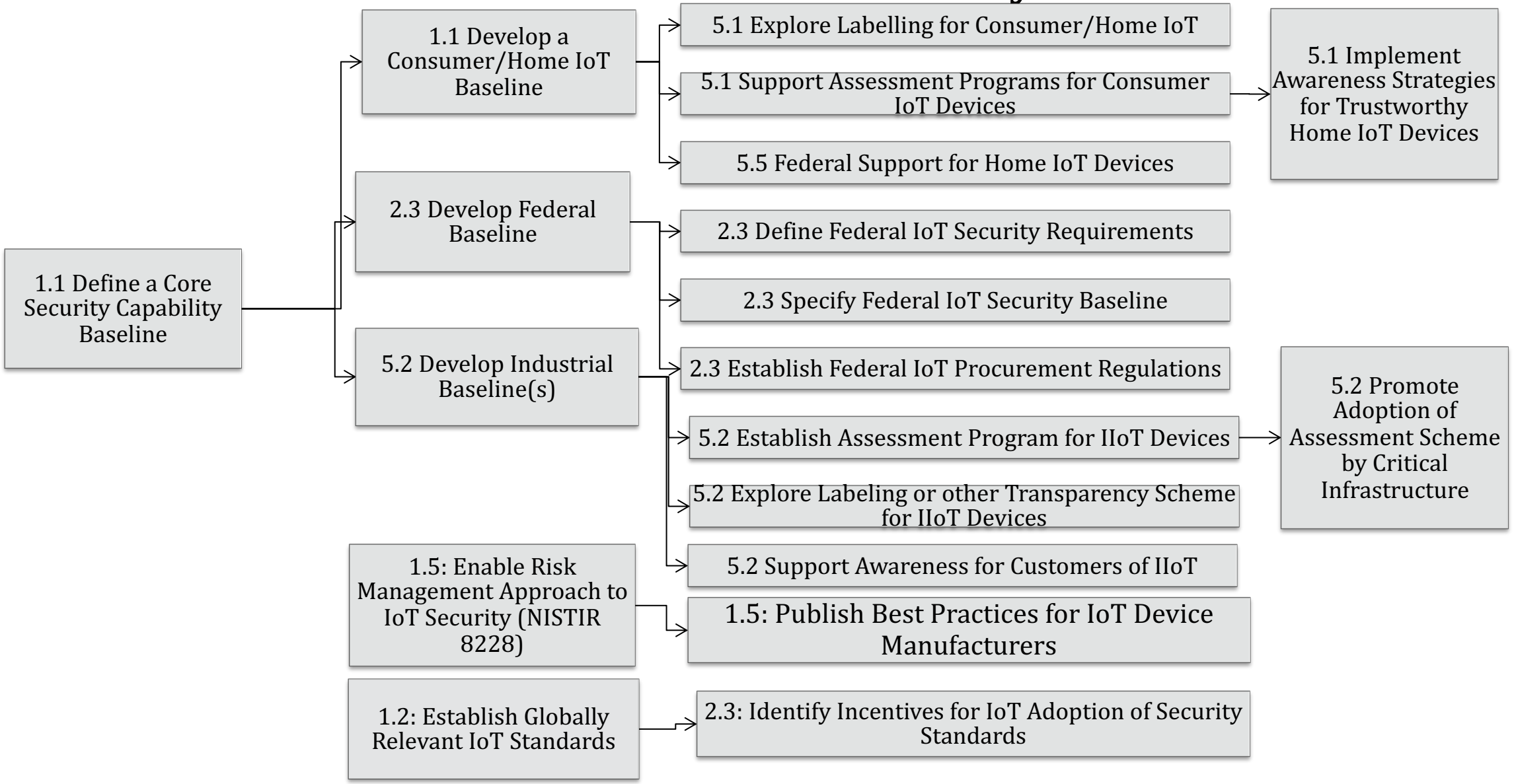
Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

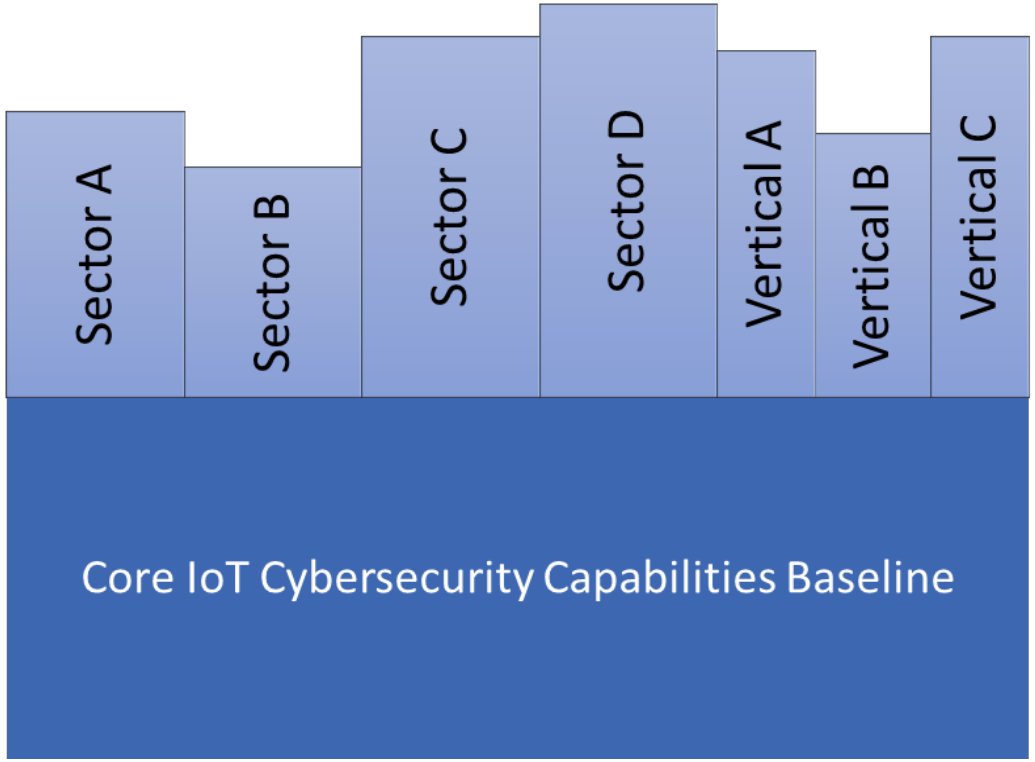
A Roadmap Toward IoT Security

- 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



Identifying a core baseline of security capabilities 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.

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

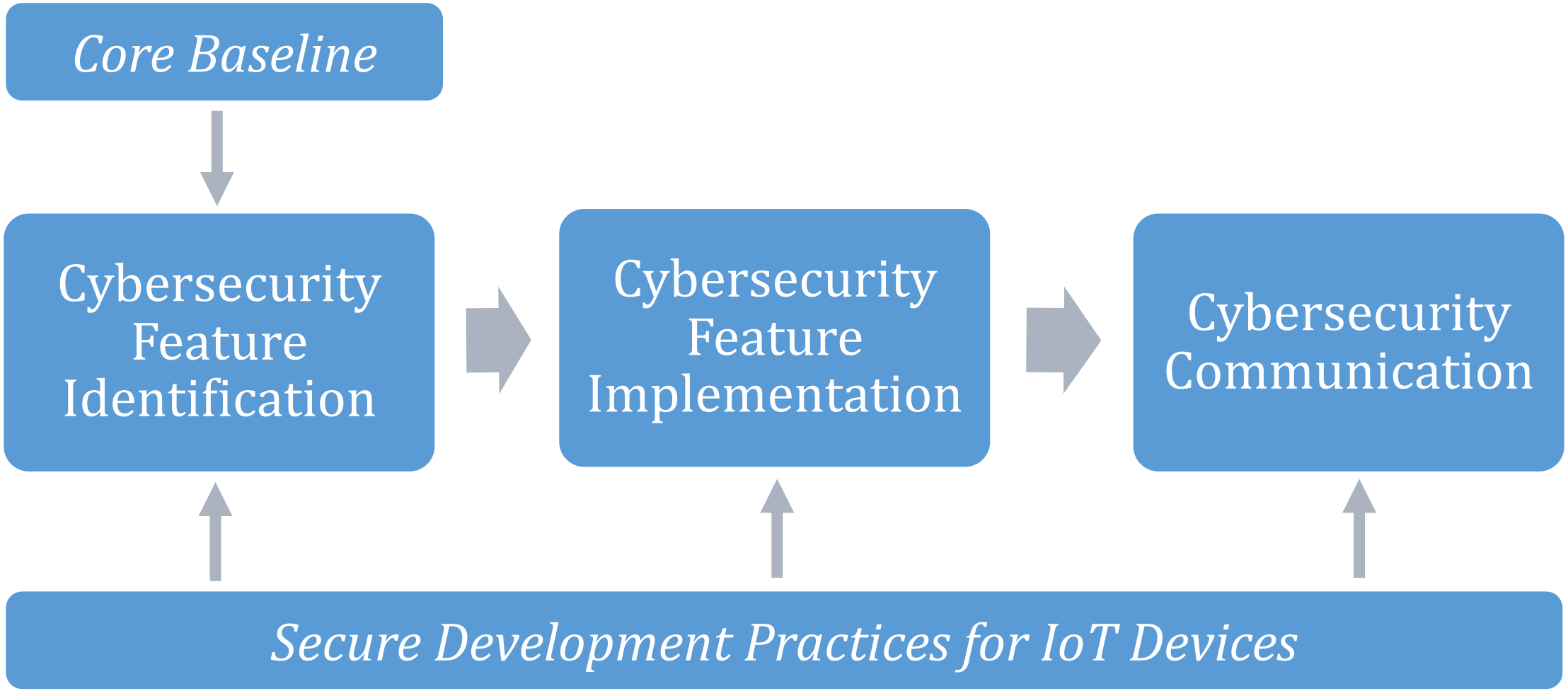
DOCUMENTATION

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

Supplemental Material:
NIST news article (other)

Related NIST Publications:
NISTIR 8228

Process for manufacturers to develop securable IoT devices



Next Steps on the Road

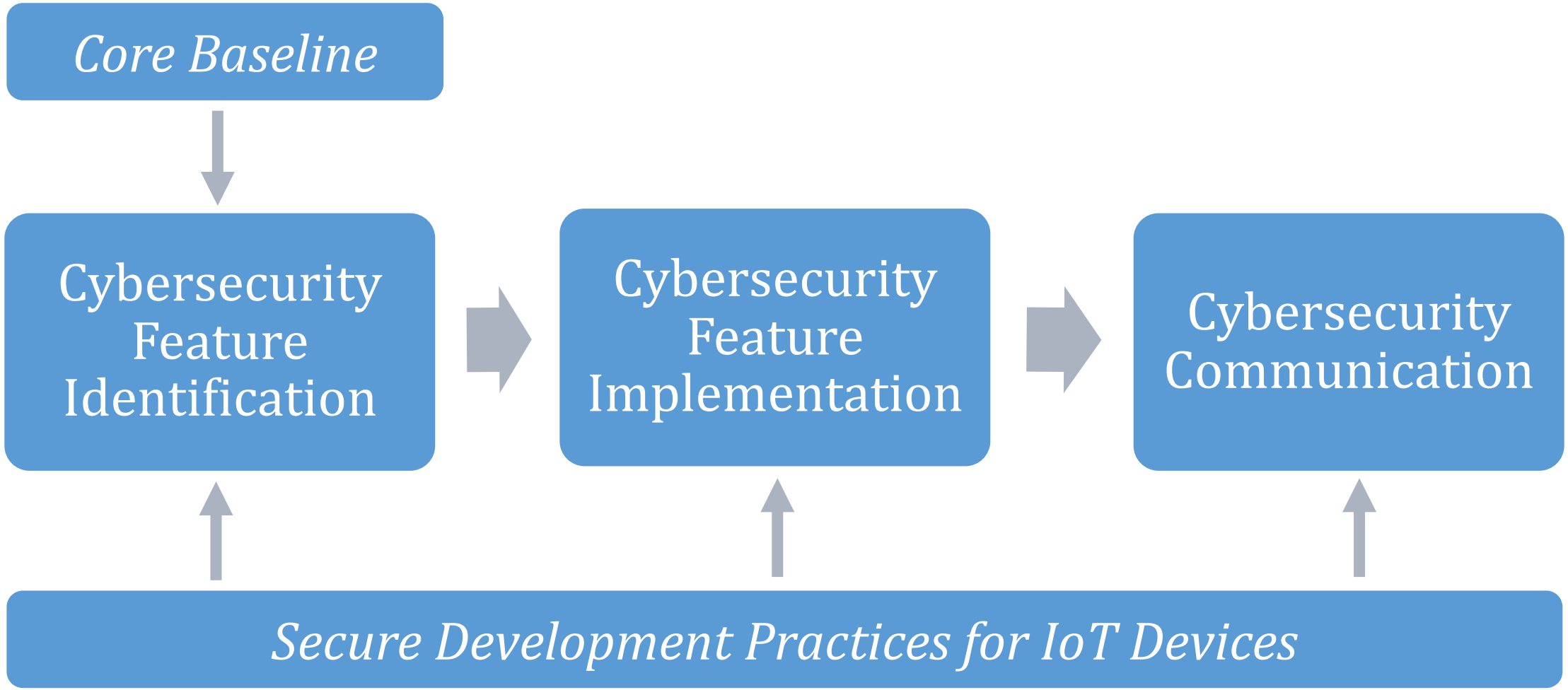
Moderator

- **Ari Schwartz**, Managing Director of Cybersecurity Services, Venable LLP

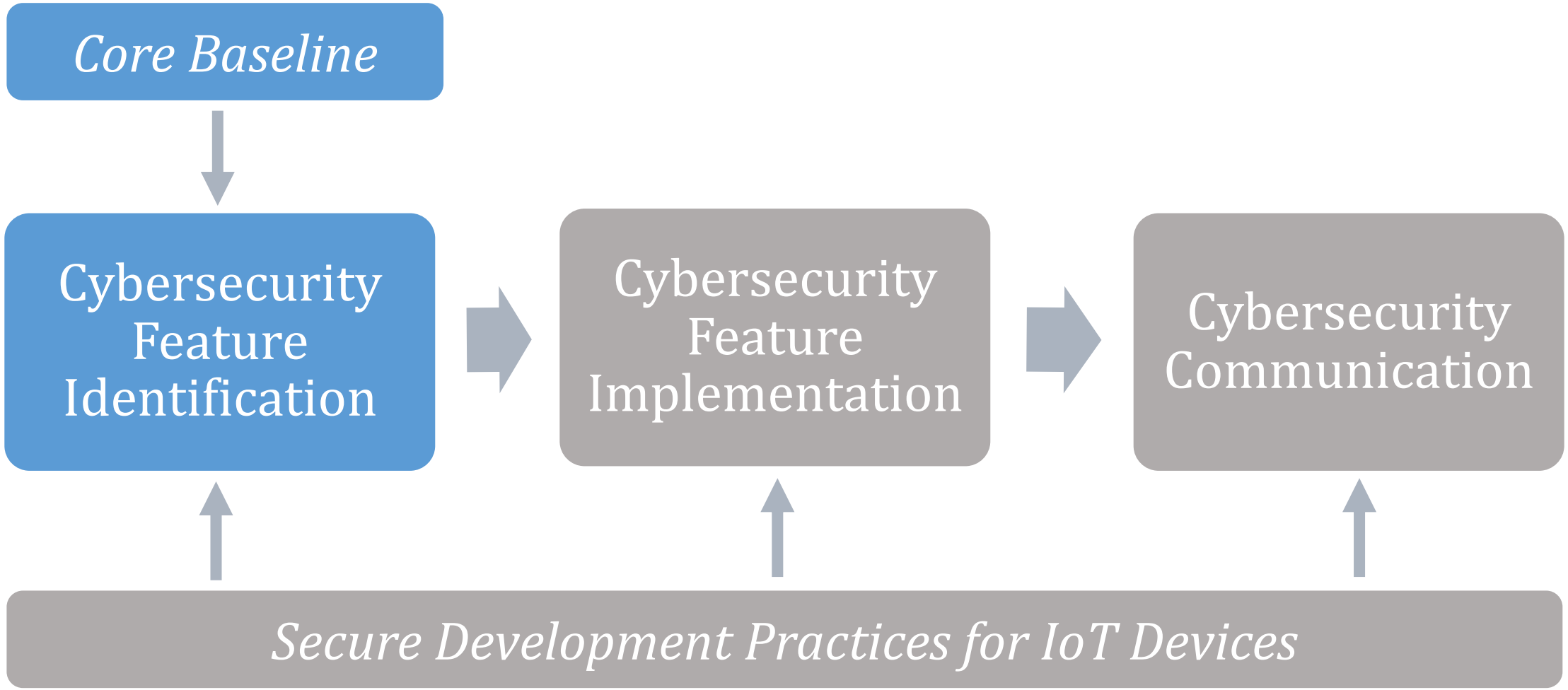
Panelists

- **Patricia Adair**, Director, Risk Management Group, US Consumer Product Safety Commission
- **William Barker**, Cybersecurity Standards and Technology Advisor, NIST
- **Michael Bergman**, Vice President, Technology & Standards, Consumer Technology Association
- **Robert Cantu**, Director, Cybersecurity, CTIA
- **Kevin Moriarty**, Attorney, Division of Privacy and Identity Protection, Federal Trade Commission

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.

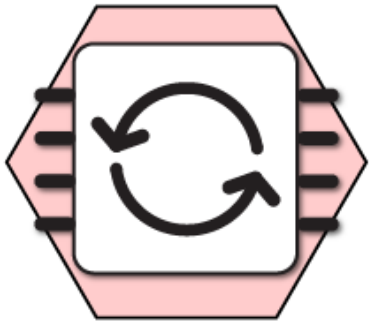
Data Protection

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.



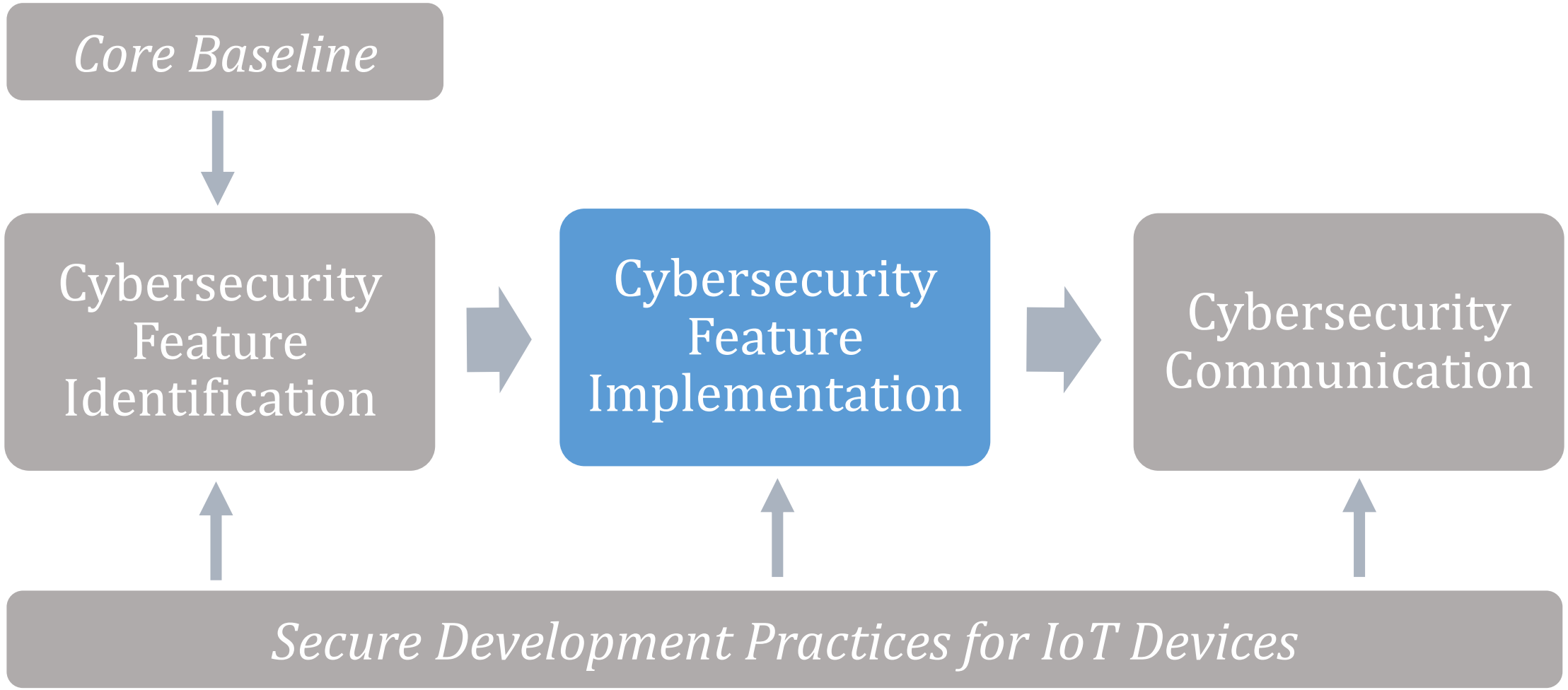
Software & Firmware Update

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

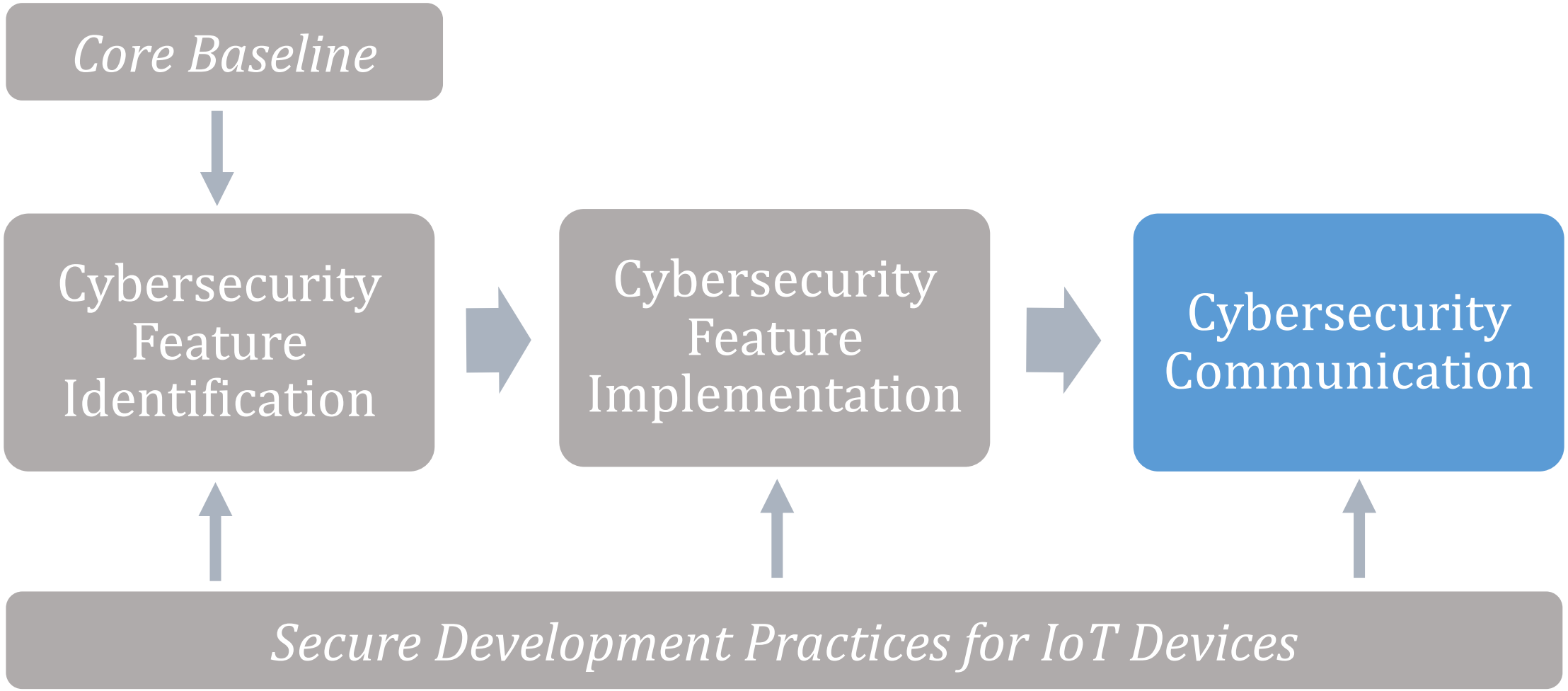
- Select or build a device with sufficient hardware resources to support the desired features
  - Be forward-looking and size hardware resources for potential future use
- Use hardware-based cybersecurity features
- Disable unneeded features provided by hardware, firmware, and/or the operating system
- 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

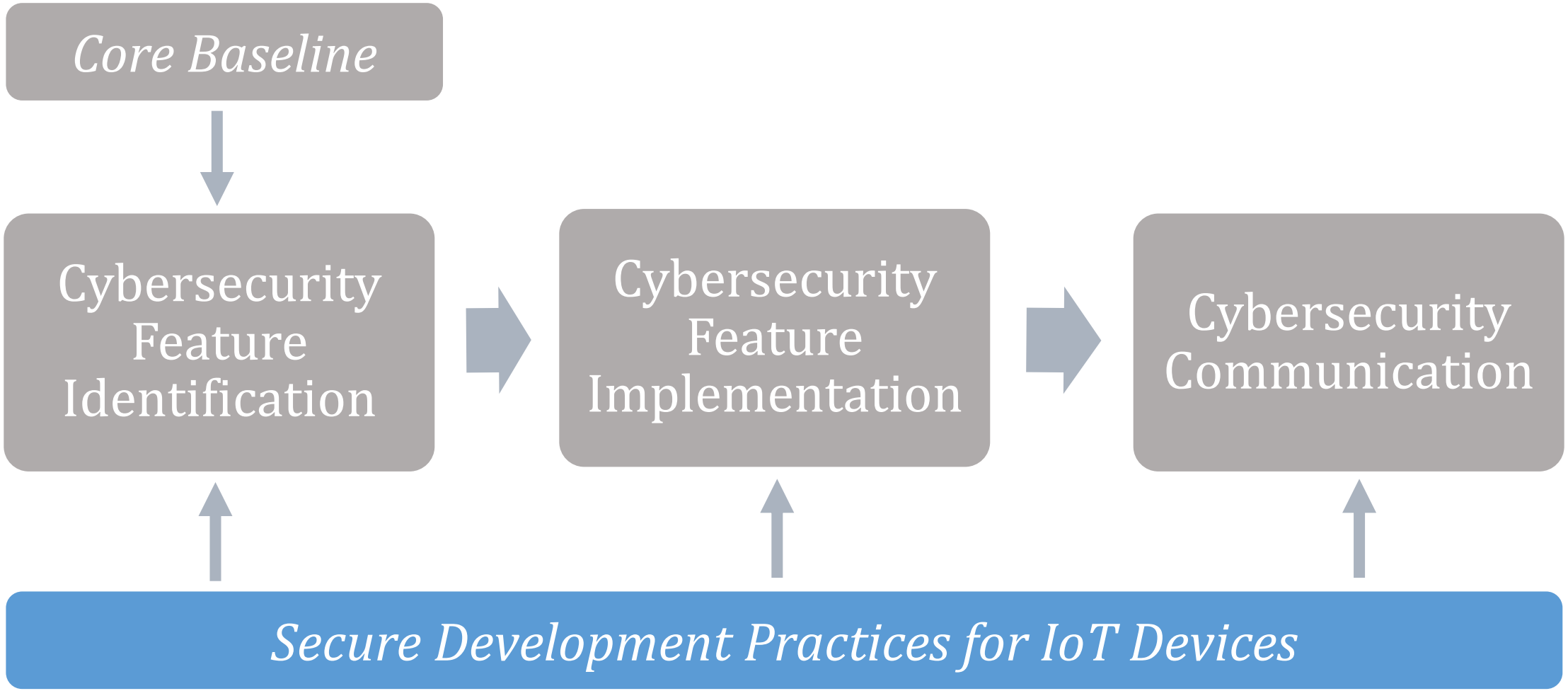
Support and lifespan expectations

- 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

Instructions for Breakouts

After lunch, we will gather in 4 separate rooms based on the number written on your badge, but all rooms will focus on the same key questions:

- Is the proposed process in Section 3 for manufacturers to determine the cybersecurity features their devices should have appropriate and reasonable?
- Are the presented Core Features the right Features for a generic starting point?
  - More, fewer, different Features?
- Are the Key Elements the right set of Key Elements?
  - More, fewer, different Key Elements?
- Is the table of the Core Baseline helpful (formatting and presentation)?
- Are the communication considerations helpful for consumers and manufacturers?
- What would you recommend as next steps for the IoT program?

Lunch

Breakout rooms:

1. West Square
2. Heritage
3. Portrait
4. Lecture Room A

Lunch is available in the NIST Cafeteria

Please report to your assigned breakout room by **12:30pm**

Breakouts will last 2 hours and then a coffee break

Feedback From Breakout Sessions

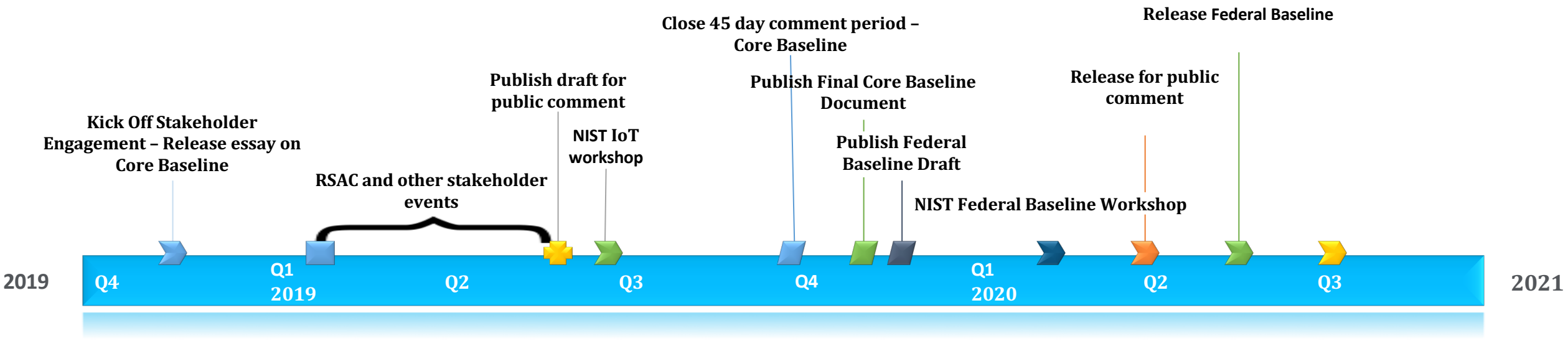
Moderator

- **Adam Sedgewick,** Senior Information Technology Policy Advisor, NIST

Panelists

- **Christine Abruzzi**
- **Joseph Drissel**
- **Matthew Barrett**
- **Matthew Smith**

Thank you for your participation!



Thank you for your participation!

- 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