National Institute of Standards and Technology
U.S. Department of Commerce

# NIST Cybersecurity for IoT:

Katerina Megas
Program Manager,
NIST Cybersecurity for IoT Program

ISPAB 04 March 2021

# The IoT Cybersecurity Program coordinates across NIST on IoT security

- Non-Regulatory agency and technical arm of the U.S. Department of Commerce
- NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- In accordance with the Federal Information Security Modernization Act (FISMA), NIST develops information security standards and guidelines for federal information systems.

## IoT cybersecurity related initiatives

**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 Feature Baseline for Securable IoT Devices
- Trustworthy Network of Things

**Special Publications**

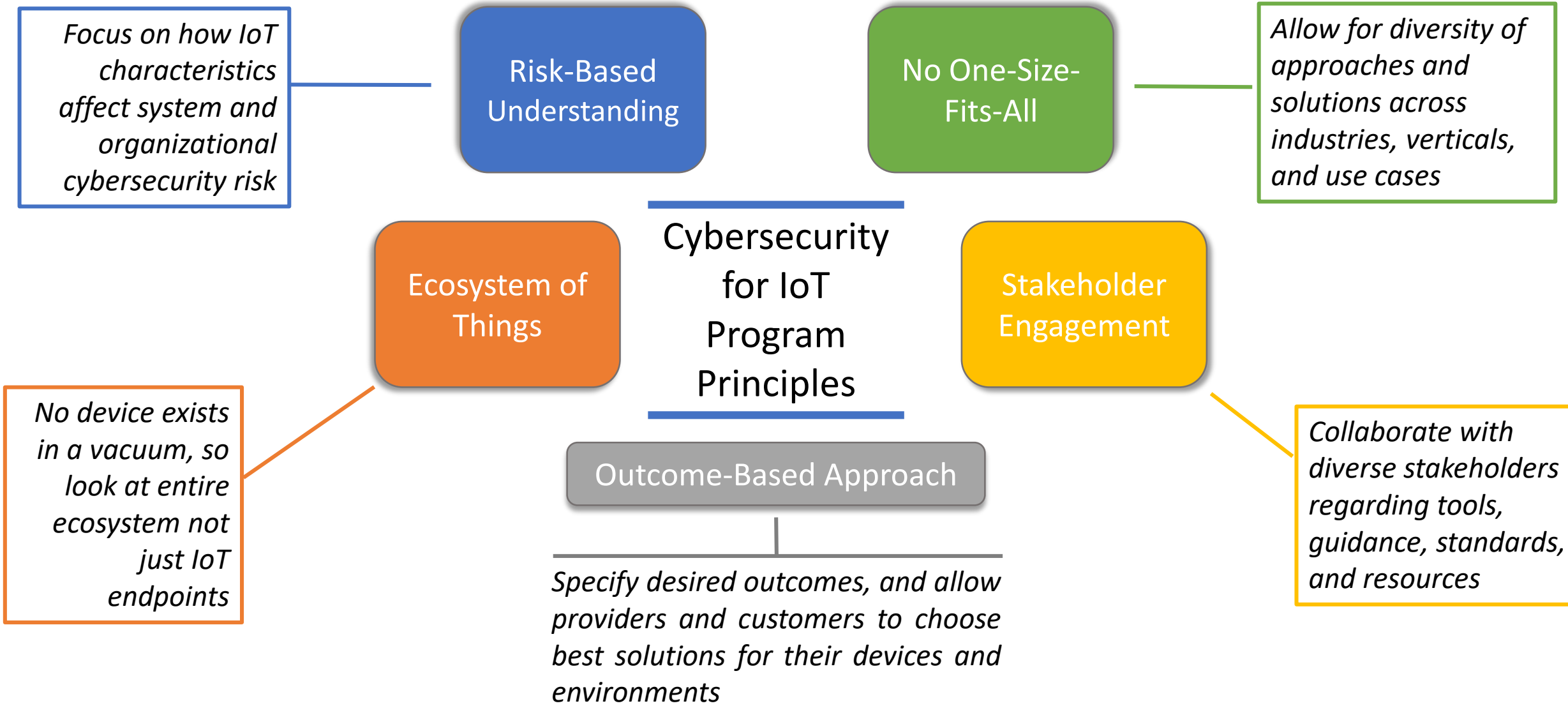
- BLE Bluetooth
- Cloud security
- Digital Identity Guidelines
- Guide to Industrial Control Systems (ICS) Security
- RFID Security Guidelines
- Software Assessment Management Standards and Guidelines
- Supply Chain Risk Management
- Security Content Automation Protocol (SCAP) Standards and Guidelines
- 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
- Securing the Industrial IoT (IIoT)
- IIoT-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
  - Securing Telehealth Remote Patient Monitoring Ecosystem
- Privacy Engineering Program
- Zero Trust Architecture Project
- IoT Device Network-Layer Onboarding Taxonomy

National Institute of Standards and Technology
U.S. Department of Commerce

# Program Principles Guiding Our Efforts



# Key Events In the IoT Cybersecurity Program

## NISTIR 8201 (Dec 2017)

- NIST IR 8200
- Takeaways from Oct 2017 Colloquium
  - IoT did introduce new risks and challenges
    - No one size fits all
    - Would require an ecosystem approach
    - Risk based understanding
    - Outcome based
  - Lots of existing guidance applicable
  - Focus on the gaps
  - Provide guidance to help tie together all the guidance

## NISTIR 8228 (June 2019)

- Focuses on what is different about managing risks associated with the use of IoT
- Frames IoT risks and challenges in the context of implementation of SP800-53 controls and Cybersecurity Framework
- *Customers dependent on security capabilities of IoT devices*

## NISTIR 8259 / 8259A (May 2020)

- Three public workshops, two public comment periods and over 600 comments
- Cybersecurity recommendations for IoT device manufacturers
- Activities for manufacturers to incorporate into product development lifecycle
- Six core Cybersecurity capabilities for IoT devices

## Federal Profile Workshop (Jul 2020)

- Published on GitHub analysis of SP 800-53 controls dependencies on IoT device capabilities. Suggested this to be a 'catalogue' for agency use
- Takeaways
  - Confirmed device centric approach useful
  - Confirmed that non-technical dependencies need to be identified
  - Confidence mechanisms desired for the market but more discussions required

## 4 Public Drafts (Dec 2020)

- Non-Technical Supporting Activities Baseline recommended for all IoT device manufacturers
- NIST published the process NIST followed to adapt the baseline to Federal agency use case
- Starting point for agencies in a Federal profile identifying the key capabilities likely needed to support agency implementation of Low baseline
- Guidance for Federal Agencies with considerations for IoT risk in agency RMF processes and how to develop requirements for IoT devices leveraging catalogue and Federal profile

**Botnet Report (May 2018)**

**Botnet Roadmap (Nov 2018)**

**Botnet Report Update (July 2020)**

**IoT Cybersecurity Improvement Act (Dec 2020)**

# Existing NIST cybersecurity-related guidance is technology-neutral and applicable to IoT

***The Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (Public Law (PL) 116 207) directs NIST to publish "standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices"***

- NIST has developed cybersecurity-related guidance that is device-neutral and highly applicable to all IoT devices.
- IoT device cybersecurity should be addressed within a risk management hierarchy from enterprise-level through organization, system, and finally component level, where IoT devices are understood as system components with a distinctive set of risk characteristics.

# In June 2020 we published a working description of IoT to frame our publication

- NISTIR 8259 described IoT devices as having:

At least one **transducer** for interacting directly with the **physical world**

(e.g., a sensor or actuator)

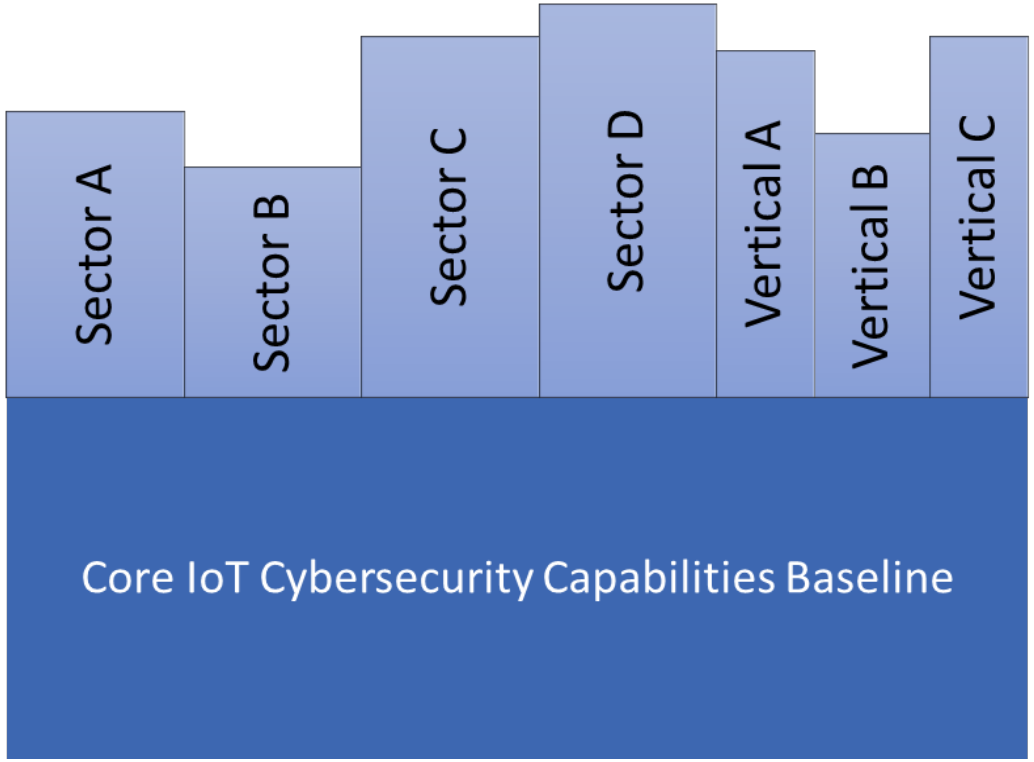
&

At least one **network interface** for interfacing with the **digital world**

(e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB])

*This is the definition used in U.S. Public Law 116-207, IoT Cybersecurity Improvement Act of 2020*

# NIST published recommendations which can be used across a wide range of IoT devices in NIST IR 8259A (May 2020)

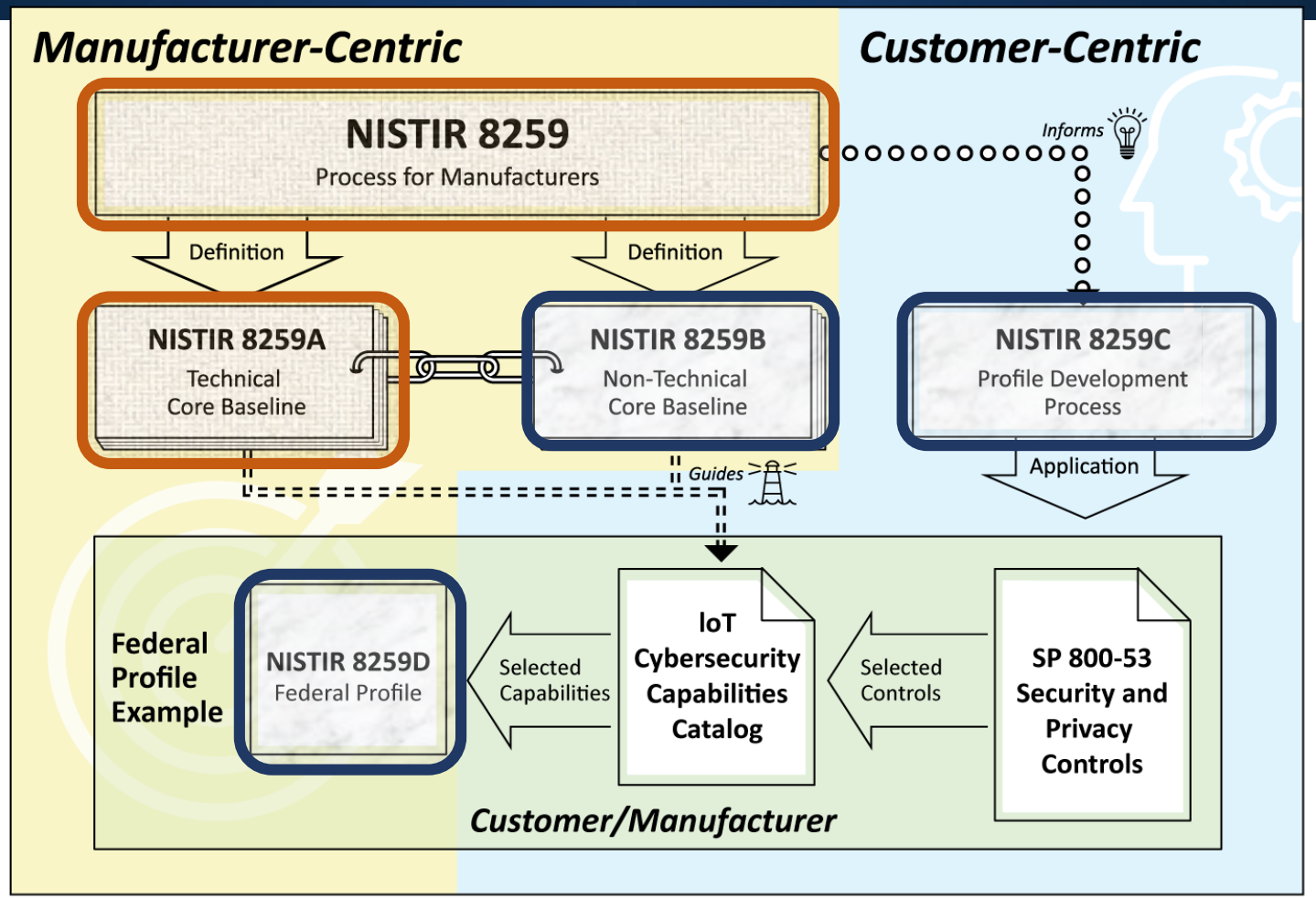



**Program Principles**

- **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.

***Profiles can be developed building on the core baseline to define the market or vertical specific needs***

# Four new publications create a framework for profiling requirements for devices




Previously Published

New Public Drafts

# Identified non-technical capabilities that might be broadly applicable and could be considered 'core'

## NISTIR 8259A (May 2020) Technical Baseline

- Device Identification
- Logical Access to Interfaces
- Device Configuration
- Software Update
- Data Protection
- Cybersecurity State Awareness

## *Draft* NISTIR 8259B (Dec 2020) Non-Technical Baseline

- Documentation

- Information & Query Reception

- Information Dissemination

- Education & Awareness

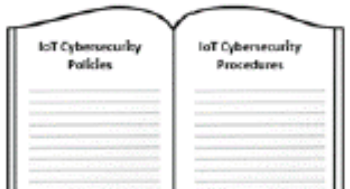
Cybersecurity controls consist of People, Processes, and Technology

# Some examples of non-technical capabilities that a manufacturer can consider during IoT product development

- Policies and procedures
- Training and awareness
- Providing support to tech users
- Changing settings on tech devices
- Risk management activities
- Disposal practices

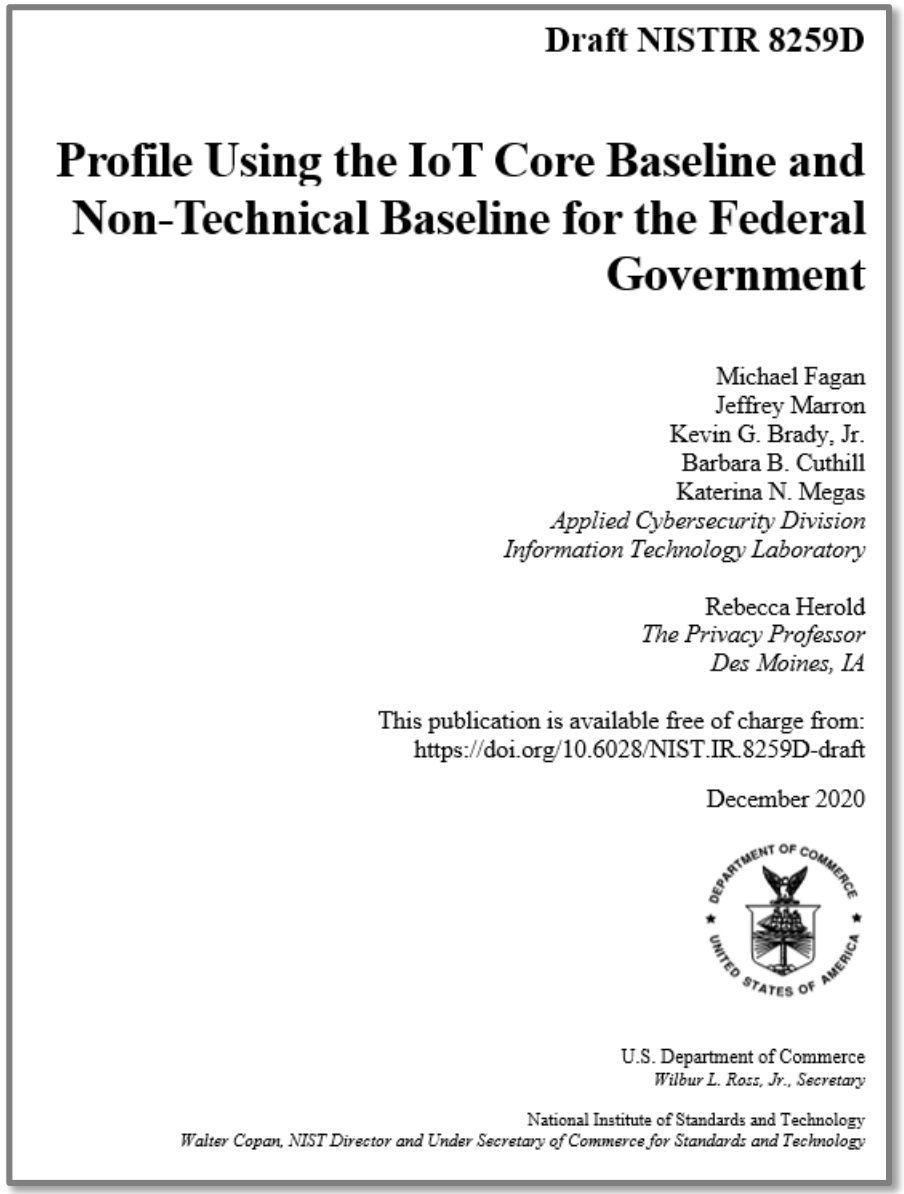
- Physical protections
- Vulnerability assessments
- Bug reporting
- Contracts
- Audits
- Contingency plans
- Systems and applications development lifecycles
- Compliance






*Images Show a Few Examples*

# NIST IR 8259D profiles and adapts the Core Baseline in 8259B to Federal agency needs



Draft NISTIR 8259D

Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Rebecca Herold
*The Privacy Professor*
*Des Moines, IA*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259D-draft

December 2020

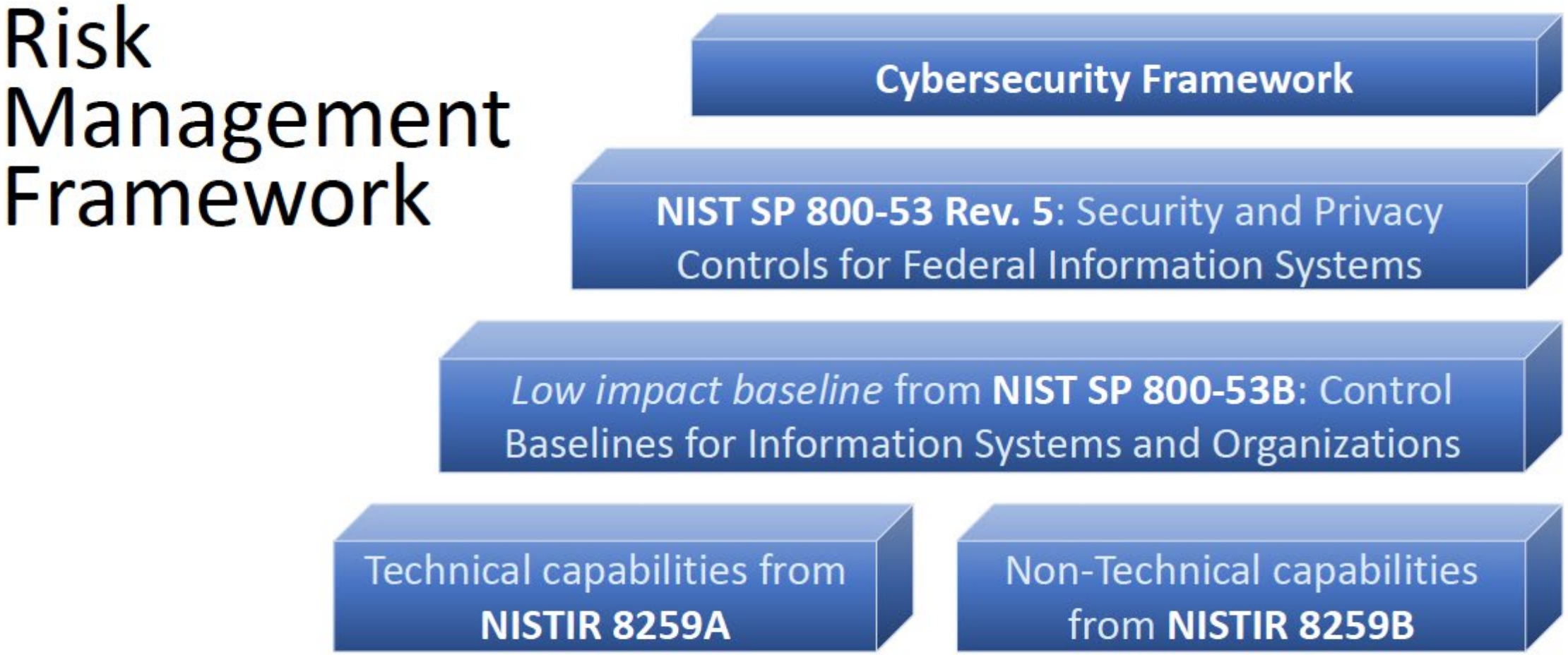
U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

**NISTIR 8159D**, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

The Federal Profile provides a starting point for agencies to consider as they identify requirements for IoT devices

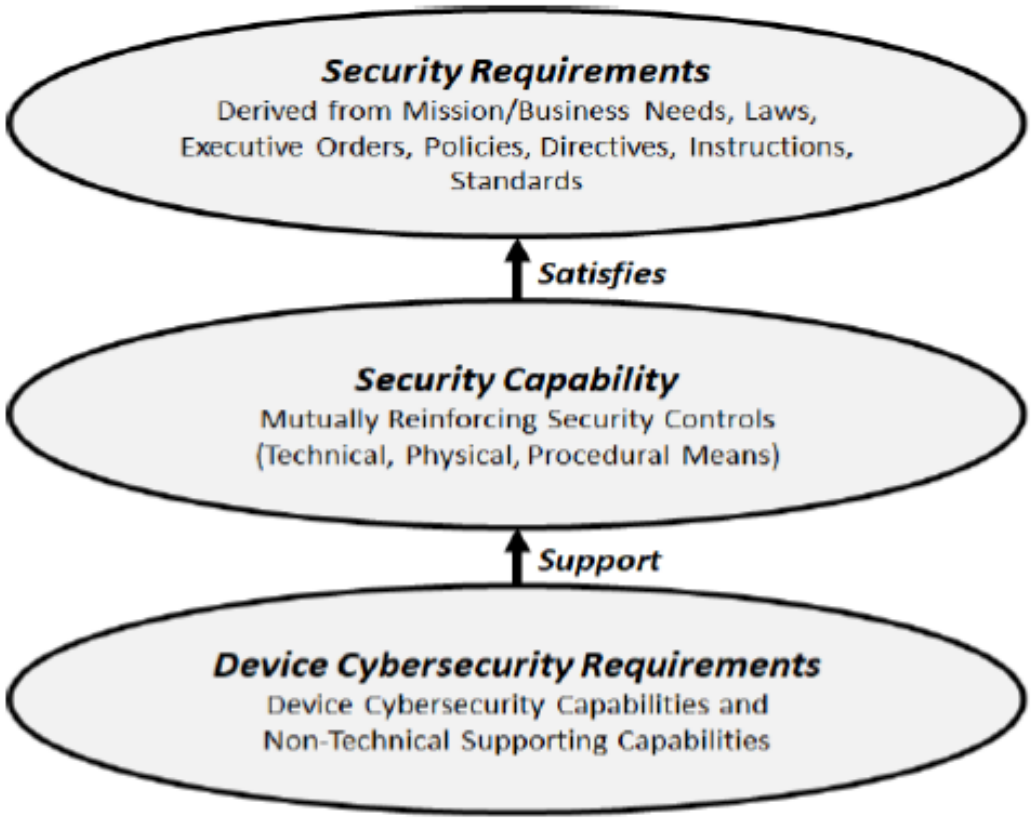
# Step 1. Primary Source Documents




Additional NIST Special Publications and other documents as needed

# 2. Assess How Documents Support…

- Device Centricity
  - Many documents are at the organization/system level
  - Extract device centric requirements implied by organization level documents
  - Most documents are device neutral
- Cybersecurity focused documents selected
- Minimal Securability
  - Focus on Low impact baseline from NIST SP 800-53B: Control Baselines for Information Systems and Organizations



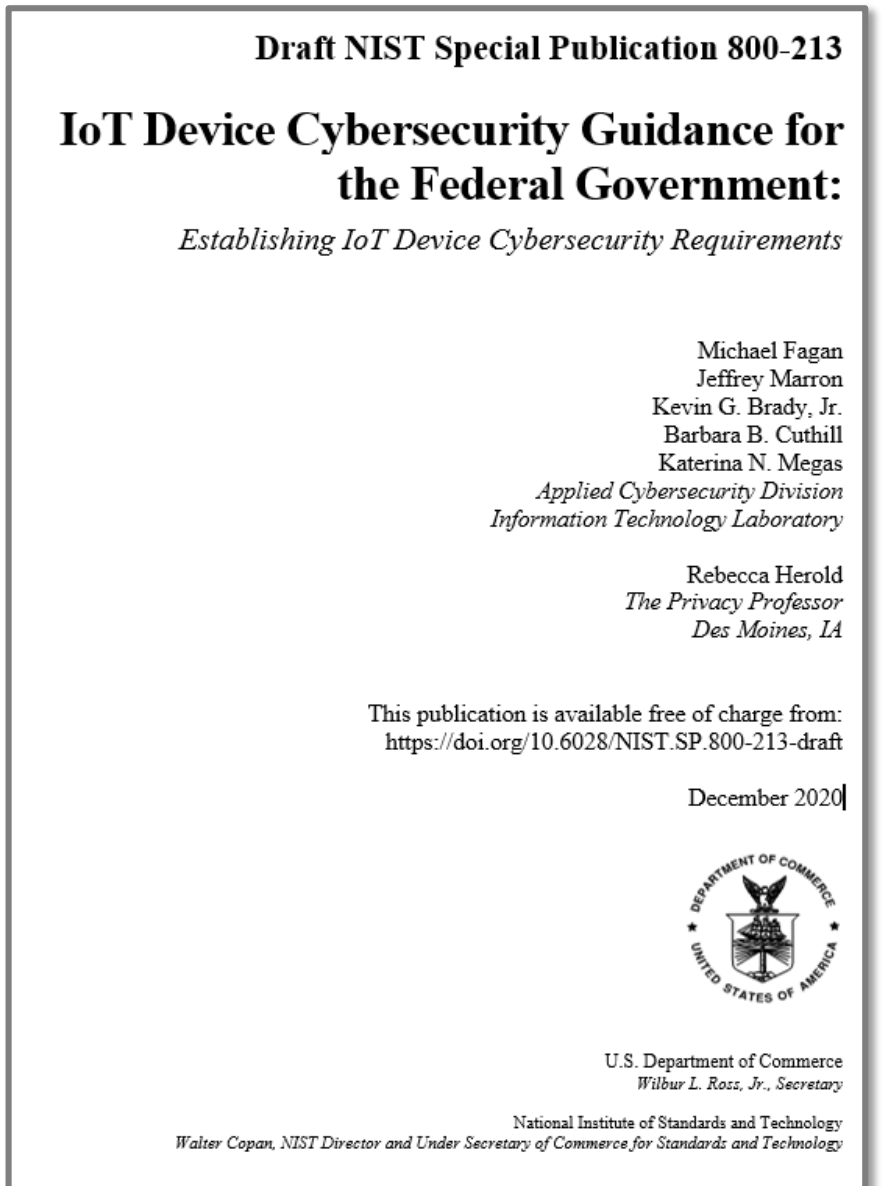
# 3. Apply the Three Concepts to Source Documents

- Device Centricity
  - Elaborated on the core baseline and non-technical baseline with a catalog of device-centric, cybersecurity- focused capabilities that would typically be needed by federal government organizations to implement 800-53 controls
  - Identified cluster of capabilities which did not fit within core technical baseline
- Focus on device capabilities needed for cybersecurity
- Minimal Securability
  - Using the controls from the low-impact RMF baseline from SP 800-53B as guidance, device cybersecurity capabilities and non-technical supporting capabilities were selected from the catalog for inclusion in the federal profile

# We identified an additional technical capability for IoT devices

- Device Securability
  - The IoT device can operate securely by protecting its hardware and software integrity and securely utilizing system resources, managing communications, and executing code.

# Draft Special Publication 800-213 provides guidance for federal agencies to consider as they establish requirements



Draft NIST Special Publication 800-213

IoT Device Cybersecurity Guidance for the Federal Government:

*Establishing IoT Device Cybersecurity Requirements*

Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Rebecca Herold
*The Privacy Professor*
*Des Moines, IA*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-213-draft

December 2020

U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

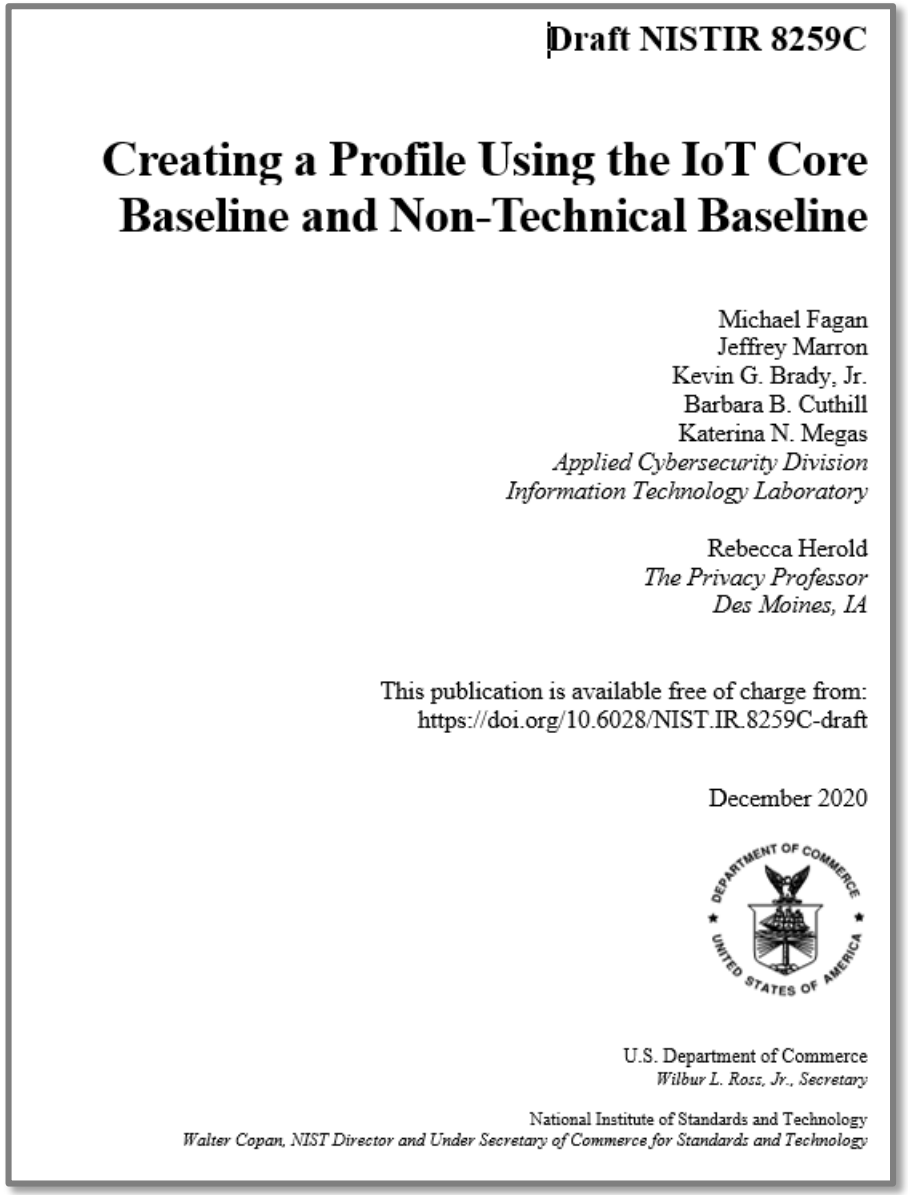
National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

**SP 800-213**, *IoT Device Cybersecurity Guidance for the Federal Government:*

*Establishing IoT Device Cybersecurity Requirements*

- When agencies determine that the risk or type of device requires additional controls beyond minimal securability or modification, agencies should consult the IoT Device Security Capabilities Catalogue to select additional capabilities to require of the device.

# Profiling: Process For Applying The Baselines



Draft NISTIR 8259C

## Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline


Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Rebecca Herold
*The Privacy Professor*
*Des Moines, IA*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259C-draft

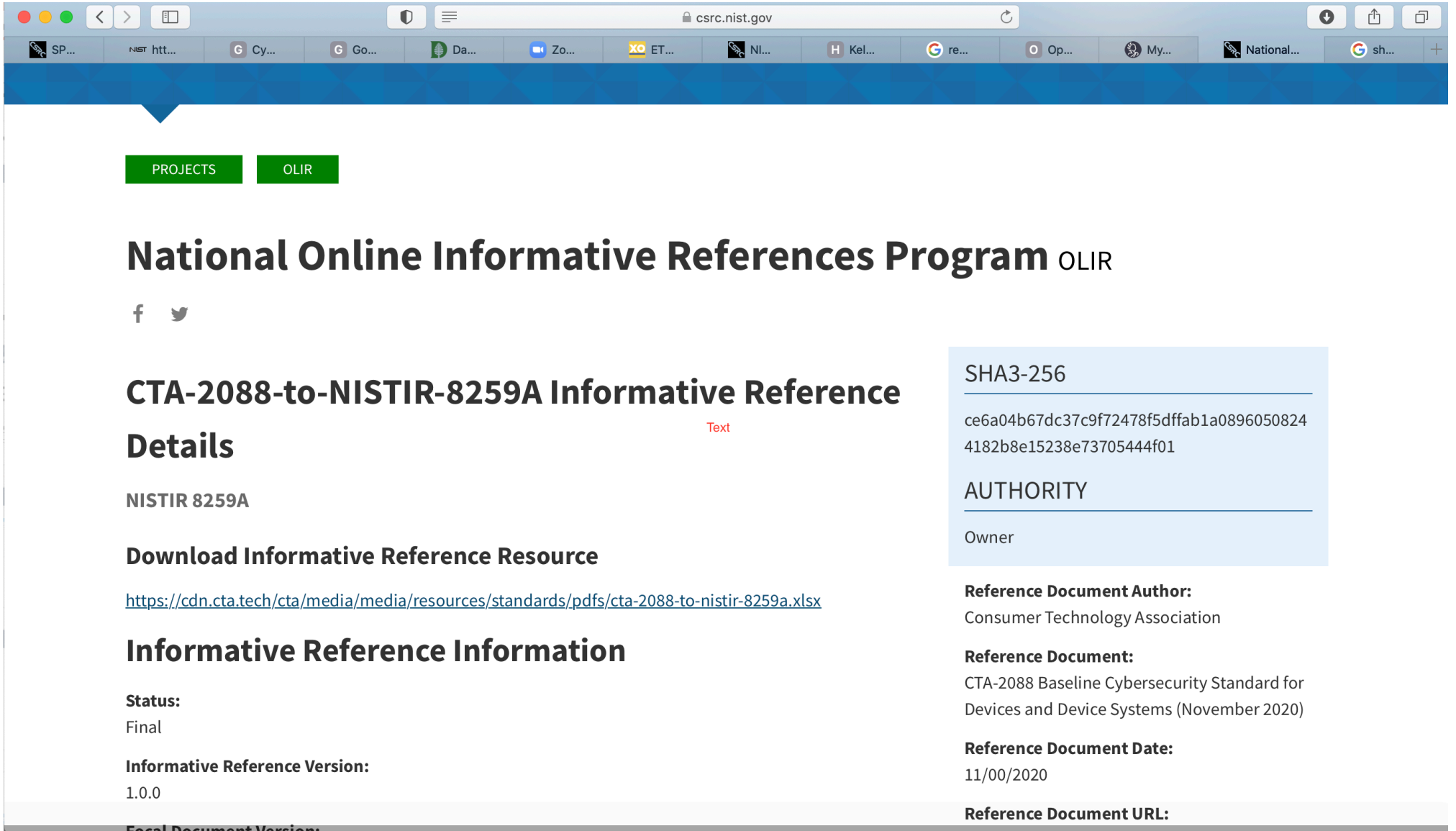
December 2020

U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

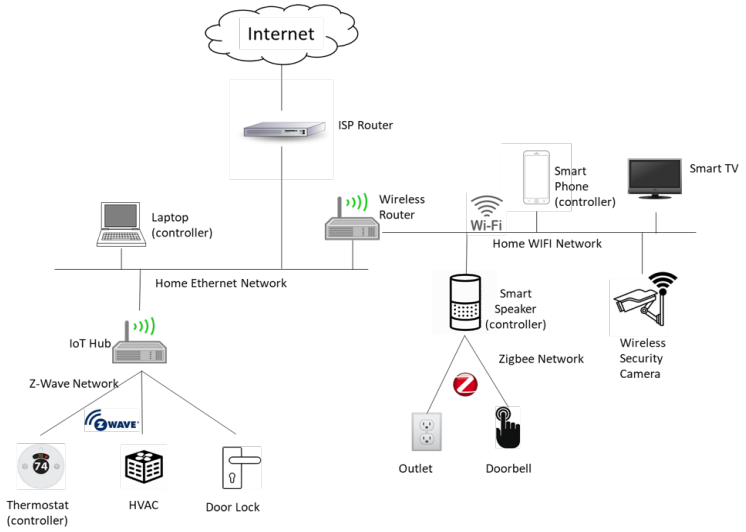

**NISTIR 8159C**, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*

# NIST rolled out first OLIR mapping of NIST recommendations to standard.. more to come

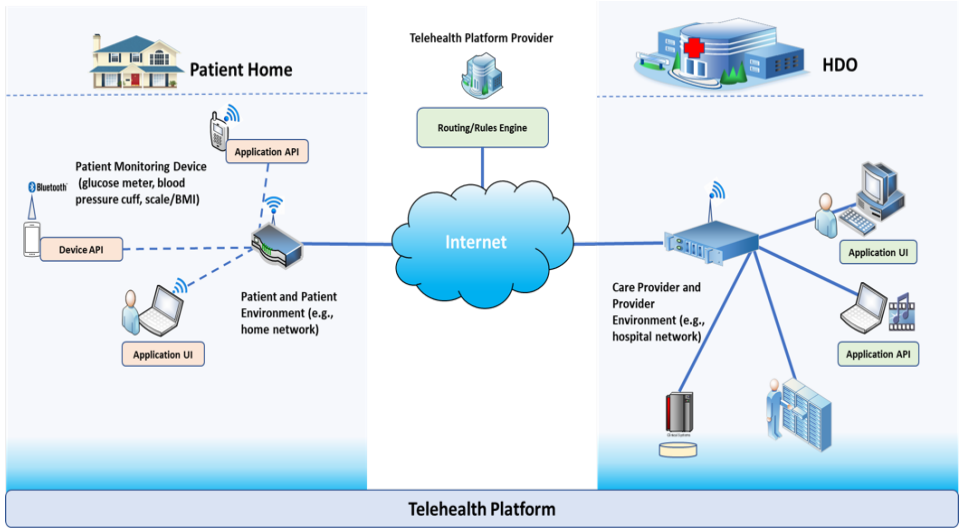


# NIST mapping NCCoE projects implementation guidance to NIST recommendations for capabilities in IoT devices

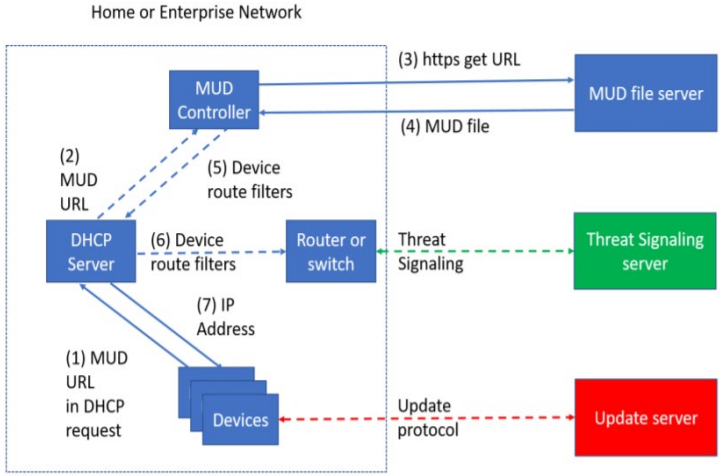
## Consumer Home IoT Product Security




## Securing Telehealth Remote Patient Monitoring




## Mitigating IoT-Based DDOS




- Protecting Information and System Integrity in Industrial Control Systems
- Securing Wireless Infusion Pumps
- Securing Picture Archiving and Communication System
- Securing Property Management Systems
- Security for 5G
- Securing the Industrial IoT: Distributed

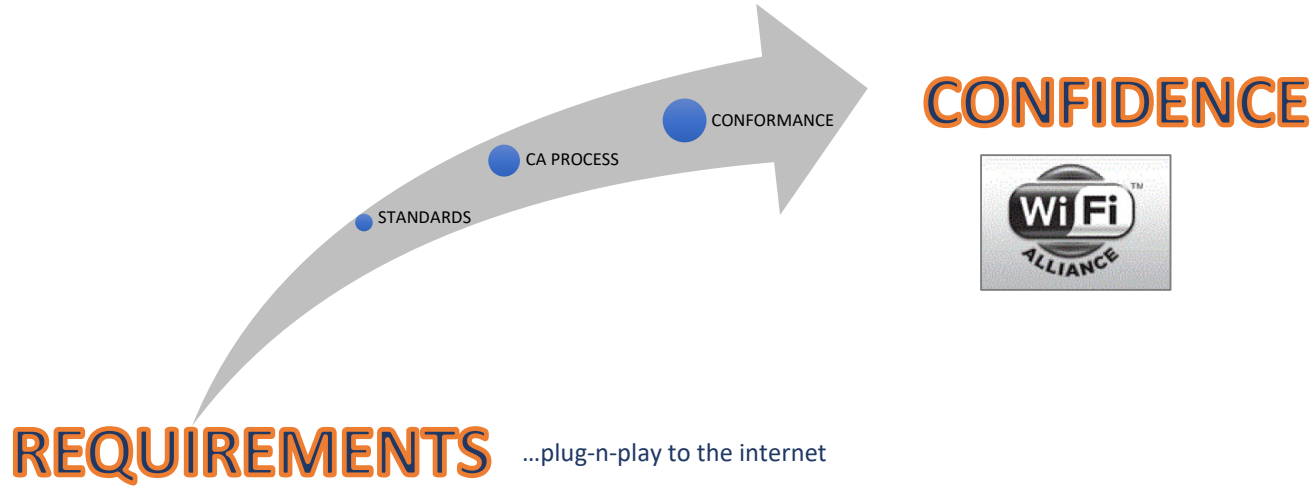
# NIST is expanding work on key areas


## Consumer devices applying the guidance in NIST IR 8259

- Updates to NIST IR 8267 Security Survey of Consumer Home Internet of Things (IoT) Products and
- Workshop on Cybersecurity Risks in Consumer Home IoT Products (October 2020)

## Confidence mechanisms for the marketplace

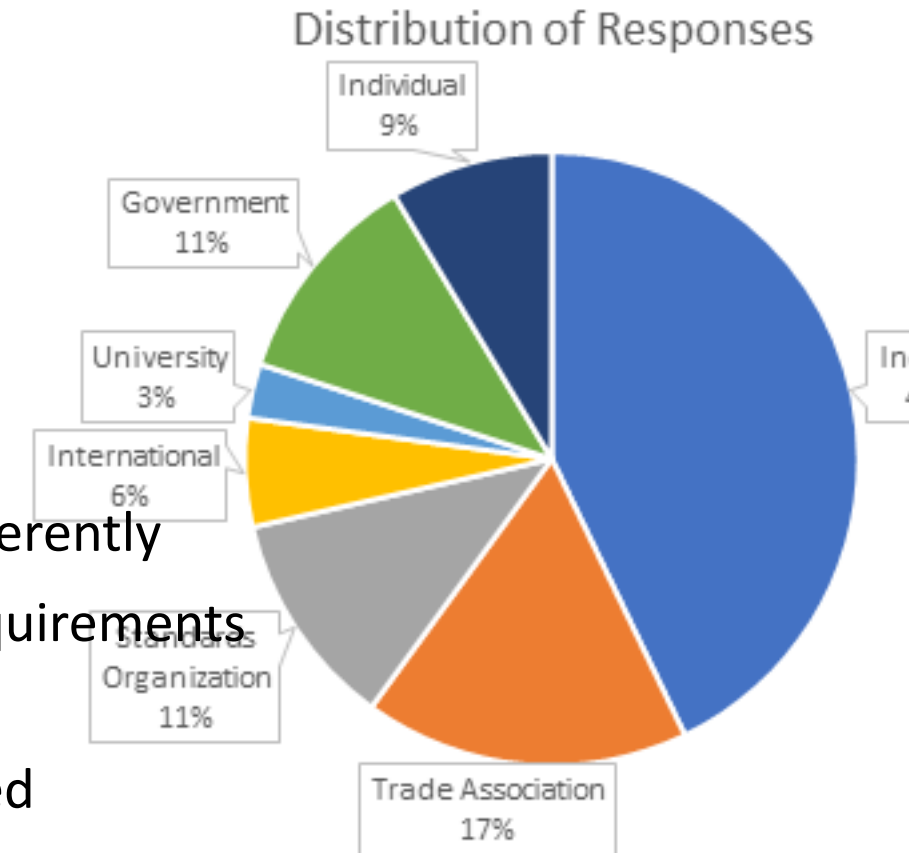
- A white paper: We want to have confidence in the security of IoT Devices: How to get there?



# Next steps

Held a public webinar and a number of roundtable discussions with stakeholders pre-closing of the public comment period. Public comments closed: February 26, 2021

- Preliminary high level themes in comments:
- What is the risk of adding an IoT device to a government network?
  - Various views of how this risk should be characterized.
- Various views on the problem of fragmentation:
  - Market fragmentation
  - Policy fragmentation
  - Different agencies defining IoT cybersecurity requirements differently
- Many IoT devices are too constrained to be able to support the requirements
  - Precluding use of large numbers of IoT devices by government
- Templates of requirements for different types of devices are needed
- Call to make distinctions among device “types”
- Tentative public workshop: April 2020



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

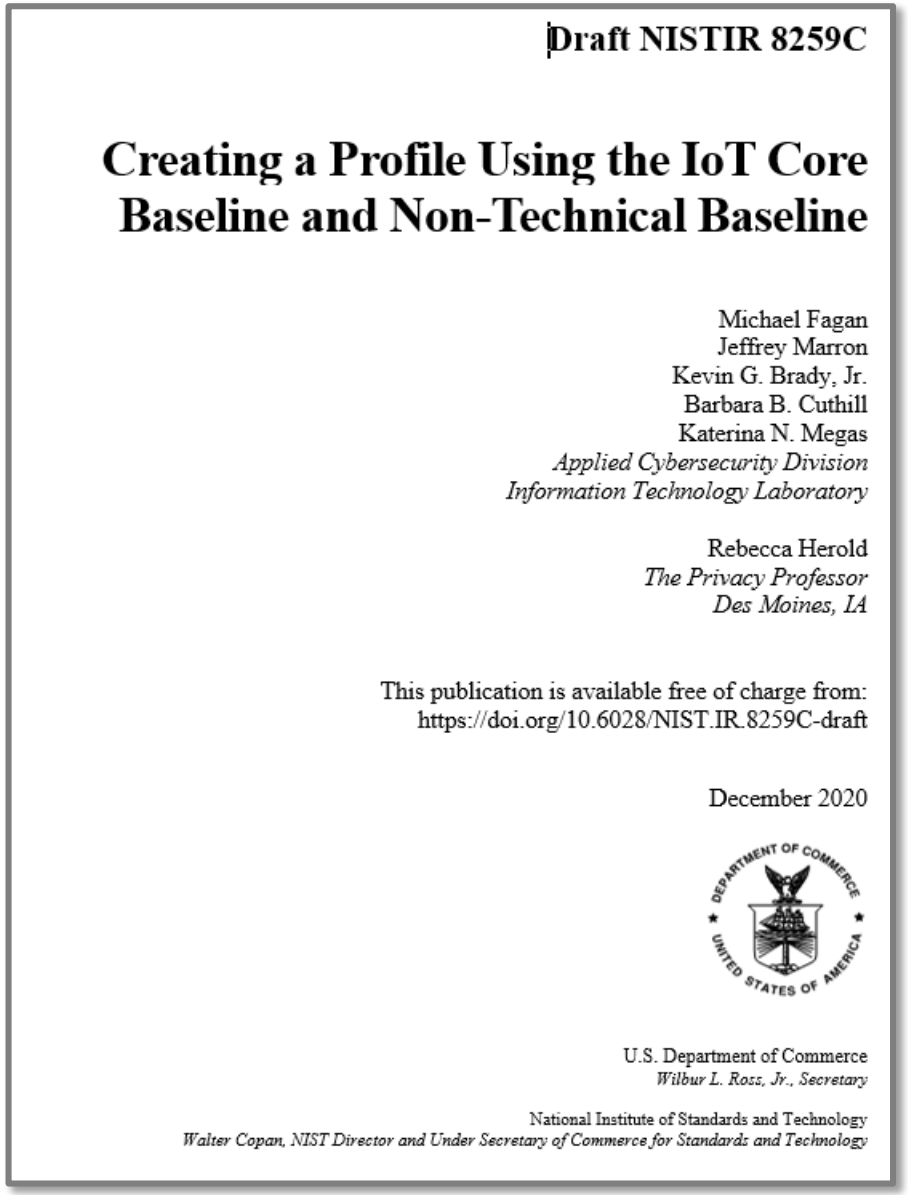
@NISTcyber
#IoTSecurityNIST

iotsecurity@nist.gov

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

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

# Profiling: Process For Applying The Baselines



Draft NISTIR 8259C

**Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline**


Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Rebecca Herold
*The Privacy Professor*
*Des Moines, IA*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259C-draft

December 2020

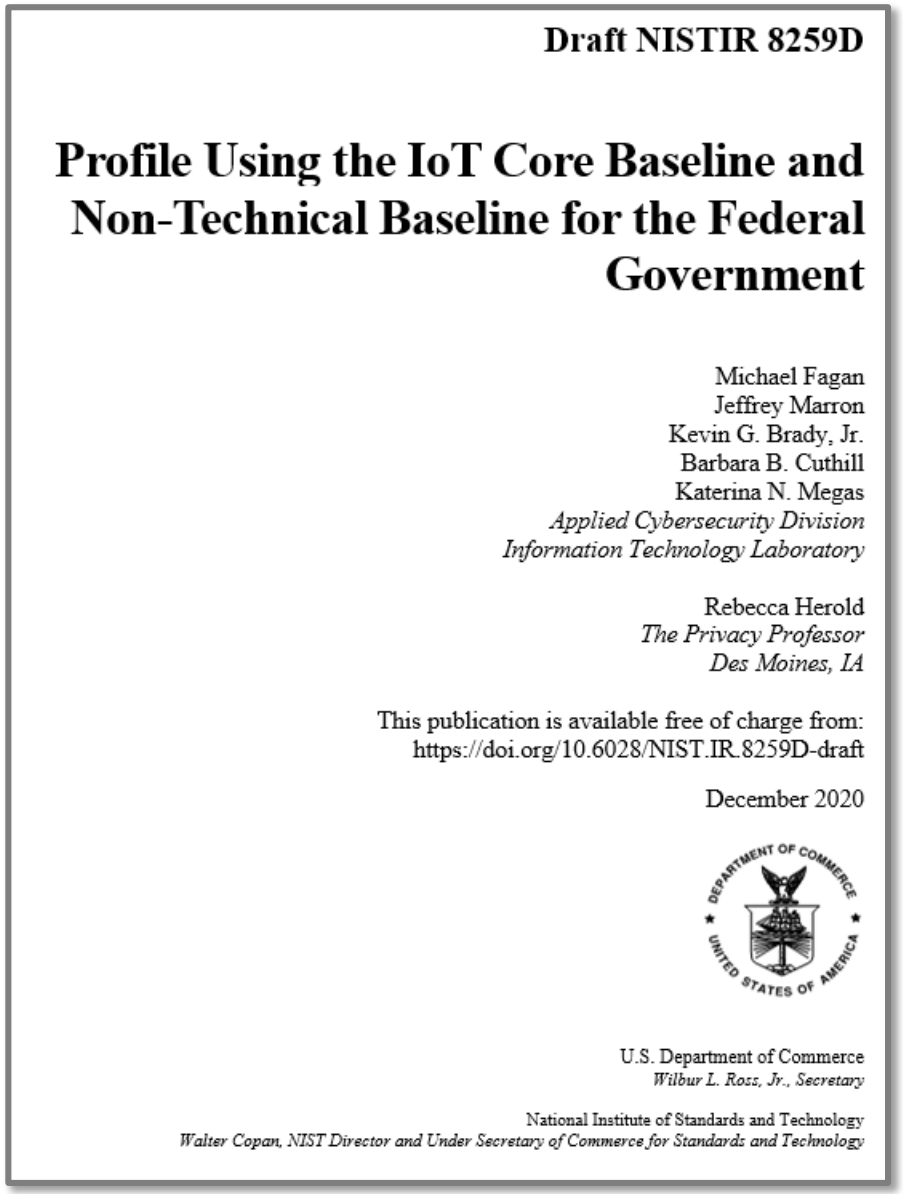


U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*


**NISTIR 8159C**, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*

# Federal Profile: A Worked Example



Draft NISTIR 8259D

**Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government**


Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Rebecca Herold
*The Privacy Professor*
*Des Moines, IA*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8259D-draft

December 2020

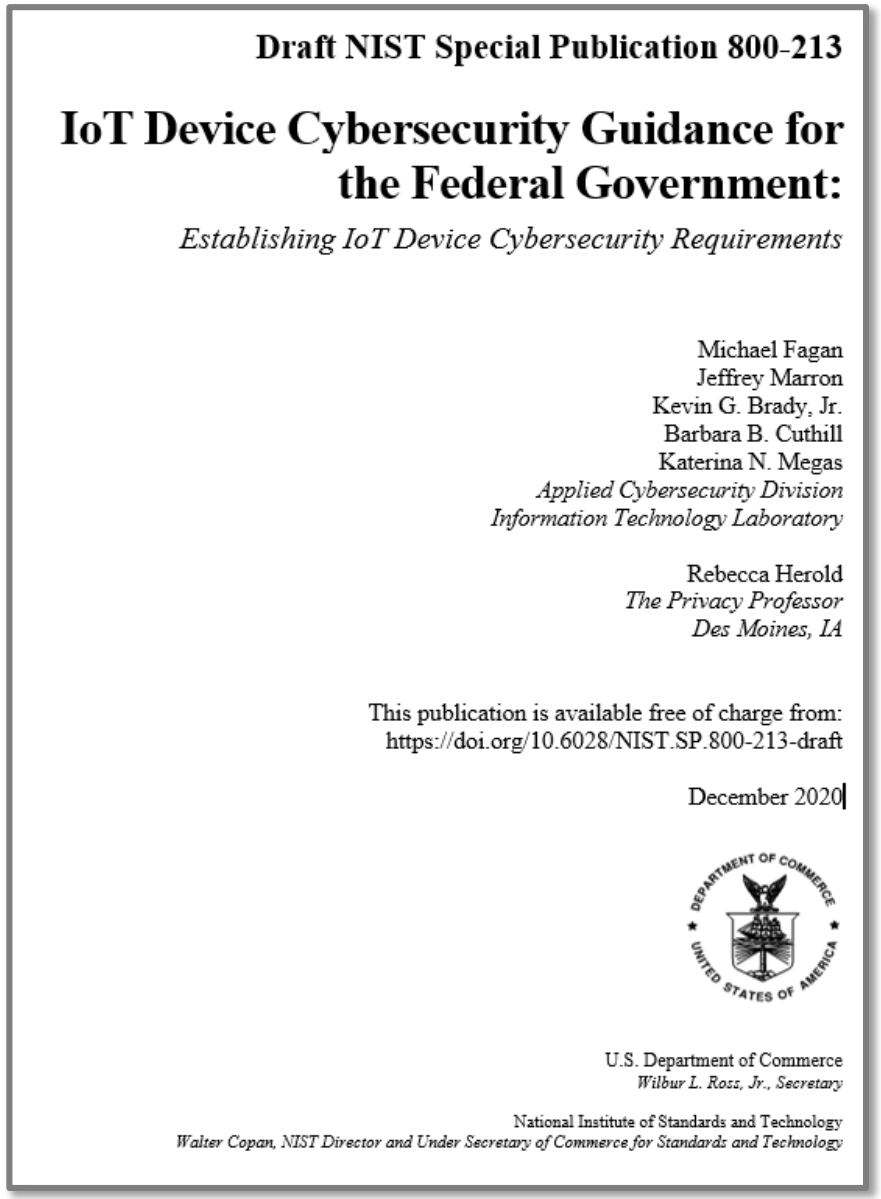


U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*


**NISTIR 8159D**, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

# Guidance for Federal Agencies



Draft NIST Special Publication 800-213

**IoT Device Cybersecurity Guidance for the Federal Government:**

*Establishing IoT Device Cybersecurity Requirements*


Michael Fagan
Jeffrey Marron
Kevin G. Brady, Jr.
Barbara B. Cuthill
Katerina N. Megas
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Rebecca Herold
*The Privacy Professor*
*Des Moines, IA*



This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-213-draft

December 2020



U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*


**SP 800-213**, *IoT Device Cybersecurity Guidance for the Federal Government:*

*Establishing IoT Device Cybersecurity Requirements*

# Agenda

- Background on the NIST ITL & the Cybersecurity for IoT Program
- Review
  - Program History
  - Published Guidance
  - Draft Guidance
  - Next Steps

# The IoT Cybersecurity Program coordinates across NIST on IoT security

- Non-Regulatory agency and technical arm of the U.S. Department of Commerce
- NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
- In accordance with the Federal Information Security Modernization Act (FISMA), NIST develops information security standards and guidelines for federal information systems.

## IoT cybersecurity related initiatives

**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 Feature Baseline for Securable IoT Devices
- Trustworthy Network of Things

**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
- Securing the Industrial IoT (IIoT)
- IIoT-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
  - Securing Telehealth Remote Patient Monitoring Ecosystem
- Privacy Engineering Program
- Zero Trust Architecture Project
- IoT Device Network-Layer Onboarding Taxonomy

National Institute of Standards and Technology
U.S. Department of Commerce

# Core Principles Guide the program Efforts

## 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.

# NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks

**Discusses how IoT may affect risk and where expectations of customers and challenges may exist when applying existing risk management frameworks**

*Protect Device Security*

- Asset Management
- Vulnerability Management
- Access Management
- Device Security Incident Detection

*Protect Data Security*

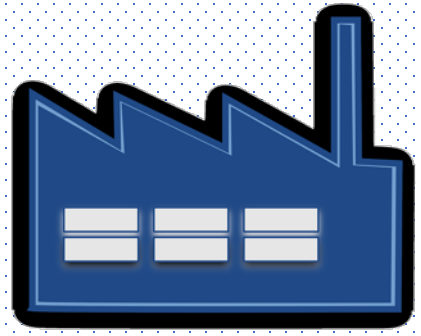
- Data Protection
- Data Security Incident Detection

*Protect Individual's Privacy*

- Information Flow Management
- PII Processing Permissions Management
- Informed Decision Making
- Disassociated Data Management
- Privacy Breach Protection

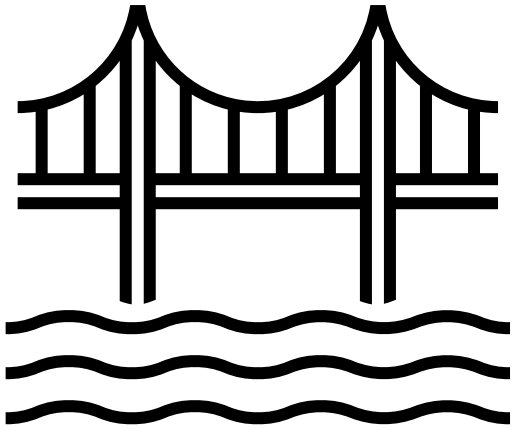
***Appendix A identifies where capabilities on the device could address some of the challenges***

# Risk management frameworks exist for the organization using IoT devices: what about what about the manufacturer?



*Manufacturers/ Producers*

*Products: IoT Devices*



*Consumers (Individual or Enterprise)*

*Cybersecurity Framework*
*Risk Management Framework*

*Information and Operational Systems (where IoT Devices are integrated)*