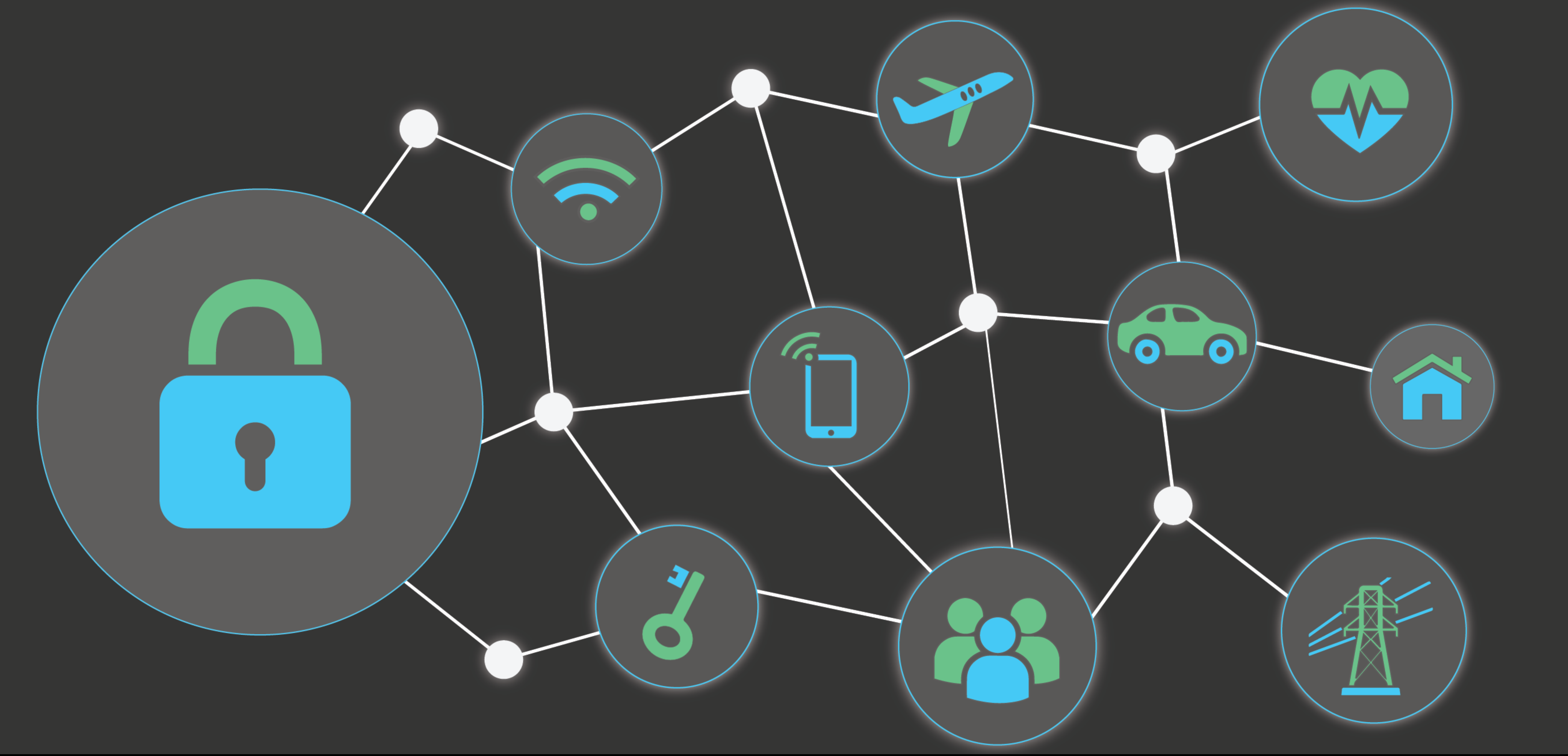


NIST Cybersecurity for IoT Program

LES

About the National Institute of Standards & Technology (NIST)

- Agency within the U.S. Department of Commerce.

- The NIST 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.

- The NIST Information Technology Lab (ITL) mission is "to **cultivate trust in information technology**"

- In accordance with the Federal Information Security Management Act (FISMA), NIST **develops information security standards and guidelines** for federal information systems.

- NIST under US Code Title 15 has a responsibility to "**prevent duplication** of regulatory processes and **prevent conflict** with or superseding of regulatory requirements, mandatory standards, and related processes"

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

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**.

IoT Cybersecurity-Related Initiatives at NIST

Research/Reports

- 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
- Mitigating IoT-Based DDoS/Botnet Report
- 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
- NCCoE IoT-Based Automated Distributed Threats
- NCCoE Use Case: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- NCCoE Wireless Medical Infusion Pumps
- Privacy Engineering Program

Cybersecurity for IoT Program Principles

Outcome-Based Approach

We embrace the Cybersecurity Framework’s outcome-based approach. We 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.

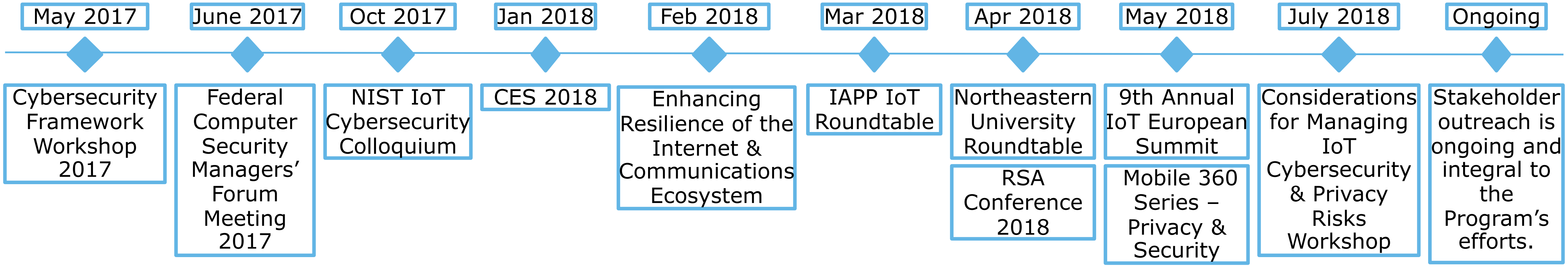
Ecosystem of Things

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.

We actively engaged with stakeholders to help inform the NIST Cybersecurity for IoT Program strategy



May 2017	Cybersecurity Framework Workshop 2017
June 2017	Federal Computer Security Managers' Forum Meeting 2017
Oct 2017	NIST IoT Cybersecurity Colloquium
Jan 2018	CES 2018
Feb 2018	Enhancing Resilience of the Internet & Communications Ecosystem
Mar 2018	IAPP IoT Roundtable
Apr 2018	Northeastern University Roundtable RSA Conference 2018
May 2018	9th Annual IoT European Summit Mobile 360 Series – Privacy & Security
July 2018	Considerations for Managing IoT Cybersecurity & Privacy Risks Workshop
Ongoing	Stakeholder outreach is ongoing and integral to the Program's efforts.

Over the course of these and other events, stakeholders tended to agree on key points.

- Need for a **common language** to discuss IoT and its associated risks.
- Preference for an **ecosystem** approach to IoT rather than looking only at the device.
- Importance of **understanding the uses** of IoT and where they are deployed.
- Interest in NIST publishing guidance that is **specific** and **points to existing cybersecurity and privacy controls**.

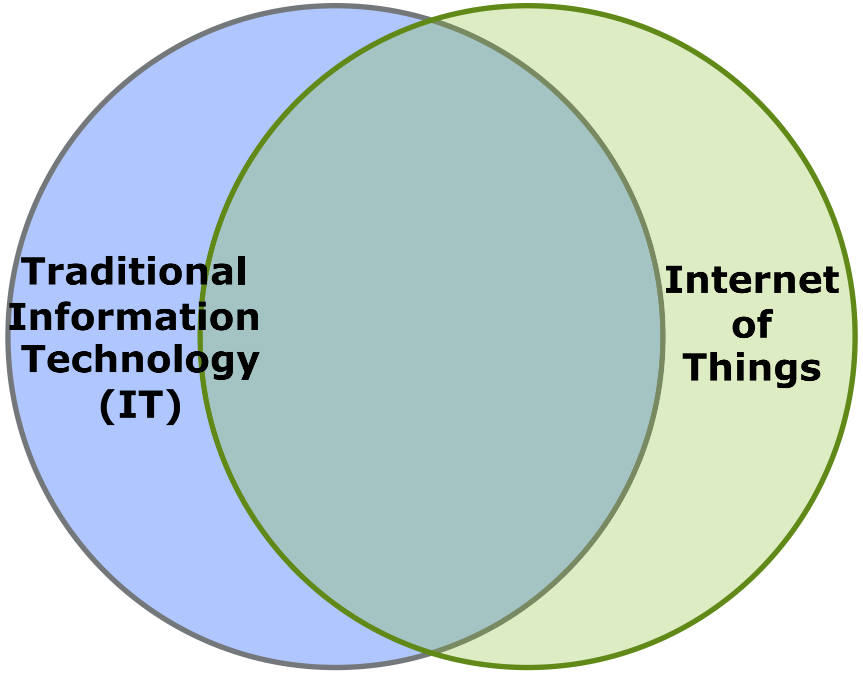
Draft NISTIR 8228: Considerations for Managing IoT Cybersecurity and Privacy Risks

- The publication is the result of **stakeholder interest in NIST guidance** on managing cybersecurity and privacy risks for IoT devices. The guidance addresses the realm of IoT cybersecurity and privacy risk not addressed in existing IT guidance.

- The primary audience is federal agencies, but the draft is intended to be **useful to any organization interested in managing their security and privacy risks associated with using IoT**. Stakeholders from federal agencies, industry, and academia provided input throughout the process.

- It includes **possible solutions for addressing cybersecurity and privacy risks**. These are not requirements: IoT devices and their uses are so varied that we wanted to allow for flexibility so the guidance can be applicable across various use cases, levels of risk, and device types.

- The intent is to be an **introduction** to managing risks. Future NIST work in IoT cybersecurity will build from this foundational document.



Using the Draft Publication: Introducing Four Concepts

Risk Considerations

Why and how IoT devices impact the management of cybersecurity and privacy risks

Risk Mitigation Goals and Areas

Which types of cybersecurity and privacy risks matter for IoT devices and may be most affected by the **risk considerations**

Expectations

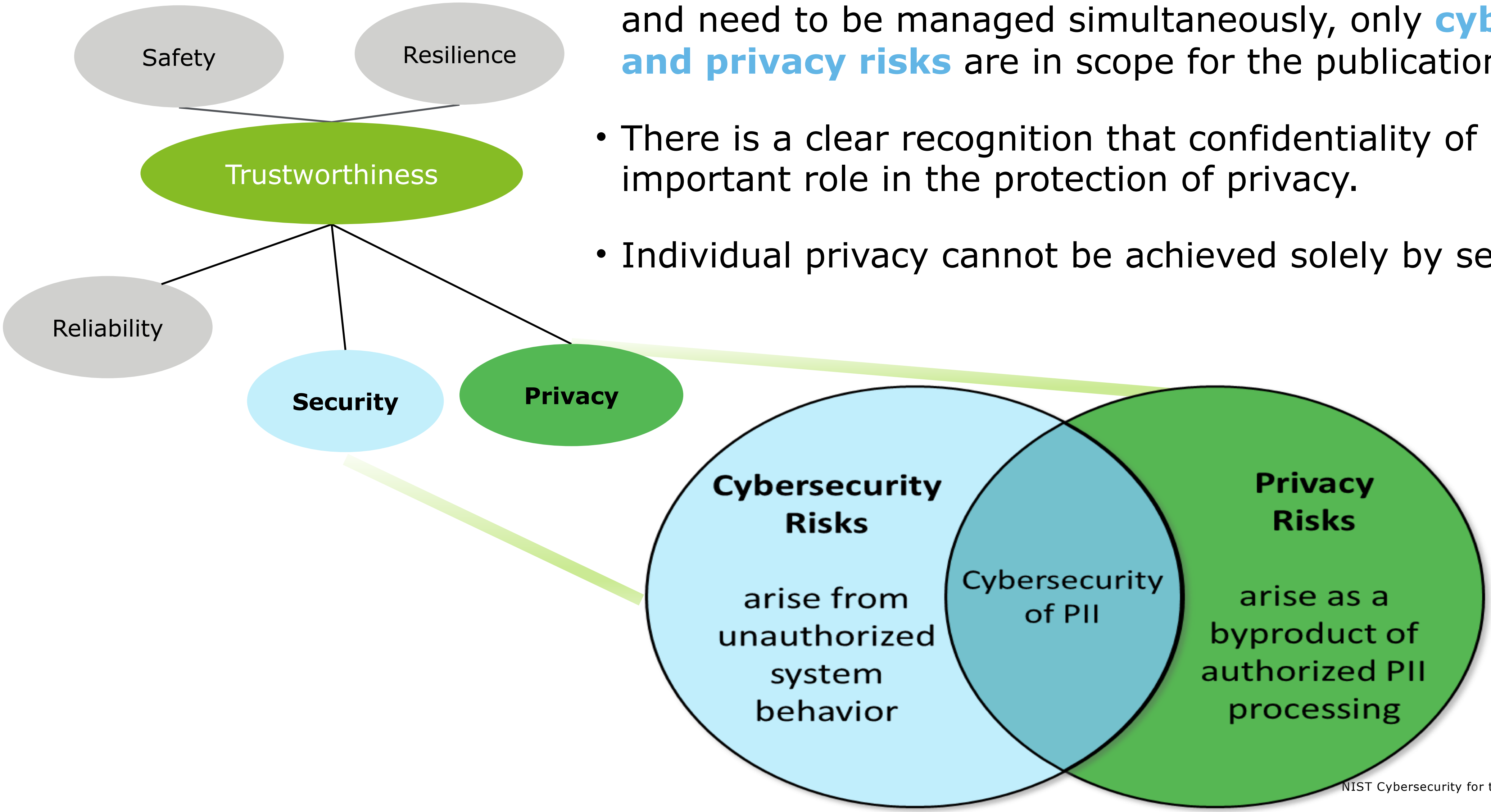
How organizations expect conventional IT devices to help mitigate cybersecurity and privacy risks for the **risk mitigation goals and areas**

Challenges

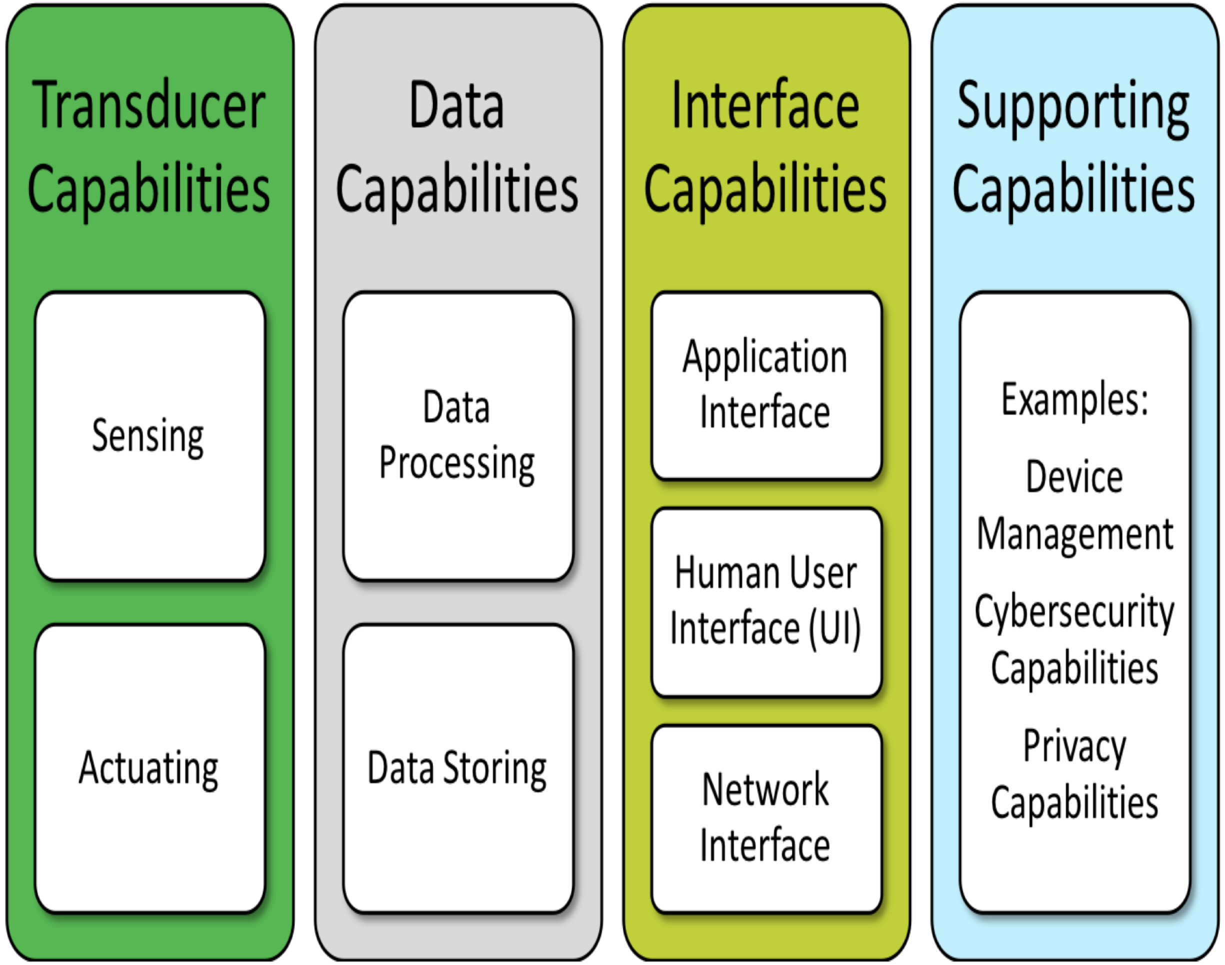
What challenges IoT devices may pose to the **expectations** and what the implications of those challenges are.

Cybersecurity and Privacy Risks are Related yet Distinct

- While multiple aspects of trustworthiness are needed for the IoT and need to be managed simultaneously, only **cybersecurity and privacy risks** are in scope for the publication.
- There is a clear recognition that confidentiality of PII plays an important role in the protection of privacy.
- Individual privacy cannot be achieved solely by securing PII.



IoT Device Capabilities Potentially Affecting Cybersecurity and Privacy Risk



While the full scope of IoT is not precisely defined, it is clearly vast. Instead of defining IoT, NIST has **scoped IoT** by identifying a set of characteristics and capabilities.

Each **IoT device provides one or more capabilities**—features or functions—it can use on its own or with other IoT and non-IoT devices to achieve one or more goals.

The Draft Publication Defines Three High-Level Risk Considerations that may Affect the Management of Cybersecurity and Privacy Risks for IoT Devices

1. **Device Interactions with the Physical World**: Many IoT devices interact with the physical world in ways conventional IT devices usually do not.
   - Examples: The ubiquity of IoT sensors in public and private environments; IoT devices with actuators have the ability to make changes to physical systems; IoT network interfaces often enable remote access to physical systems that previously could only be accessed locally
2. **Device Access, Management, and Monitoring Features**: Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.
   - Examples: Lack of management features; lack of interfaces; wide variety of software to manage
3. **Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness**: The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices.
   - Examples: Some post-market capabilities for conventional IT, such as network-based intrusion prevention systems, antimalware servers, and firewalls, may not be as effective at protecting IoT devices as they are at protecting conventional IT

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.

Challenges with Cybersecurity and Privacy Risk Mitigation for IoT Devices

Risk Mitigation Goals

Protect Device Security	Protect Data Security	Protect Individuals’ Privacy
Associated Risk Mitigation Areas		
• Asset Management • Vulnerability Management • Access Management • Device Security Incident Detection	• Data Protection • Data Security Incident Detection	• Information Flow Management • PII Processing Permissions Management • Informed Decision Making • Disassociated Data Management • Privacy Breach Detection

Potential Challenges to Risk Mitigation Goals

There are challenges to each set of the three risk mitigation goals.

Goal 1: 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.

Associated Risk Mitigation Areas

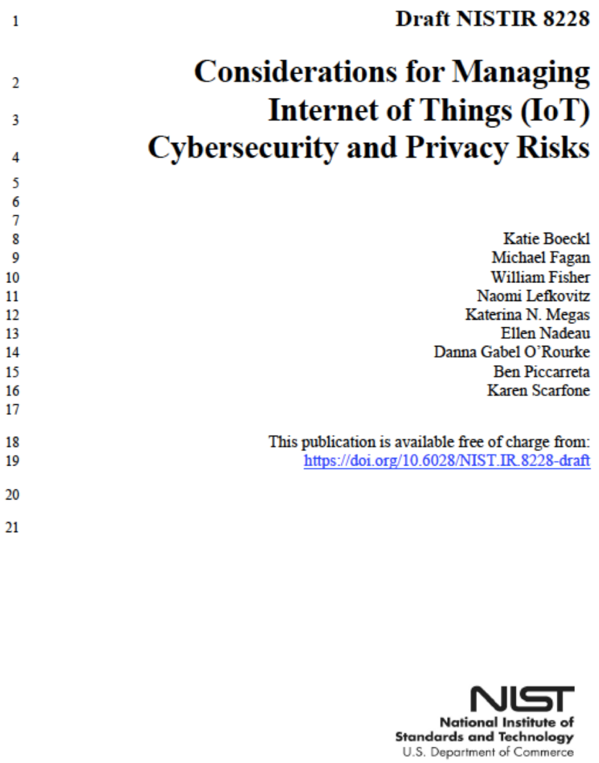
- **Asset Management**: Maintain a current, accurate inventory of all IoT devices and their relevant characteristics throughout the devices’ lifecycles in order to use that information for cybersecurity and privacy risk management purposes.
- **Vulnerability Management**: Identify and eliminate known 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 activity involving IoT devices for signs of incidents involving device security.

Potential Challenges to Protecting Device Security

- The IoT device may not have a unique identifier that the organization’s asset management system can access or understand.
- The IoT device may be a black box that provides little or no information on its hardware, software, and firmware.
- The IoT device may not be capable of having its software patched or upgraded.
- The IoT device may not support any use of identifiers.
- The IoT device may only support the use of one or more shared identifiers.
- The IoT device may not verify the identity of another computing device before sending sensitive data in its network communications.
- The IoT device may not support use of non-trivial credentials
- Etc…

Draft NISTIR 8228: Public Comment Period

- **Received 25+ sets of comments**
  - Examples: Amazon, Boeing, Chamber of Commerce, CTA, CTIA, ITI, Microsoft, Raytheon, Symantec, any many more.
- **Key takeaways:**
  - Overall a well-received foundational document, but stakeholders are eager for further elaboration. In particular, there is interest in continued engagement on Appendix A, to develop cybersecurity and privacy baselines for IoT.
  - Promote an ecosystem approach to IoT security.
  - Account for parallel privacy efforts, such as the Privacy Framework.
  - Mixed feedback on developing a comprehensive definition for IoT.
  - 8228 helps organizations manage their risk given what is available on the market today.



Draft NISTIR 8228

Considerations for Managing
Internet of Things (IoT)
Cybersecurity and Privacy Risks

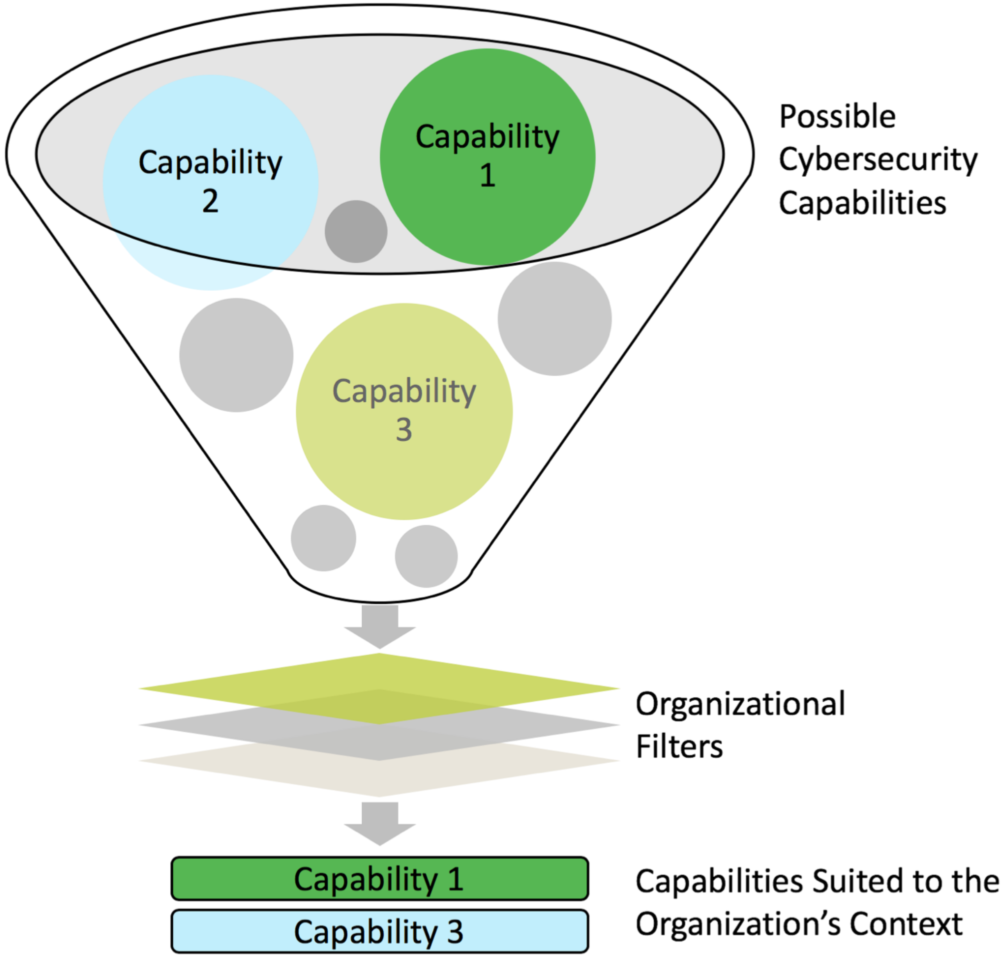
Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

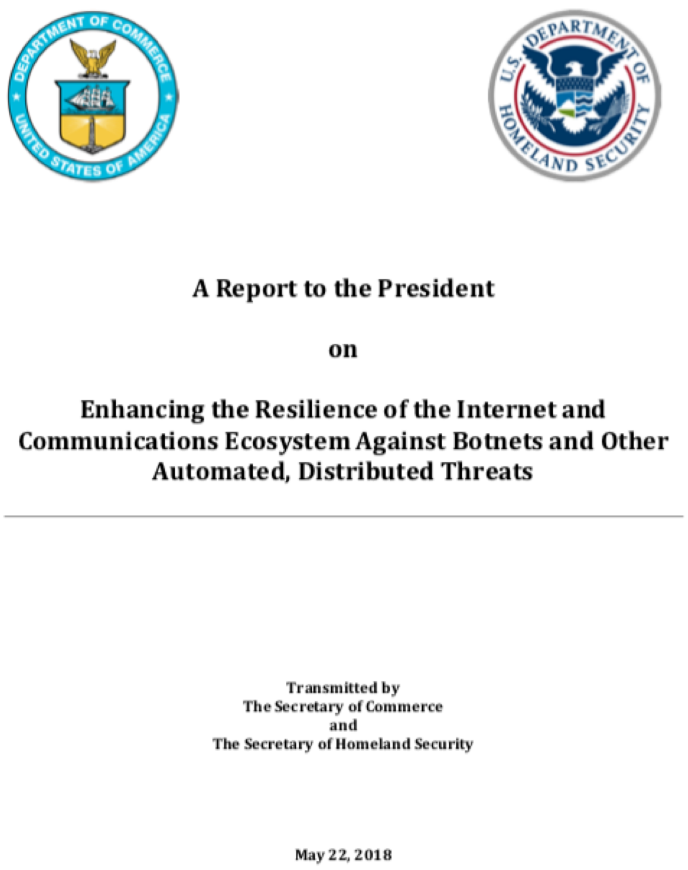
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8228-draft

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

Draft NIST IR 8228 Provides a Table of Possible Cybersecurity and Privacy Capabilities for Organizations to Consider for IoT Devices

- We started by looking at multiple existing efforts, domestic and international (BITAG; CSA; CTIA; ENISA; GSMA; IIC; IoTSF: OTA; UKDDCMS), and identified **15 common capabilities** .
- An organization might use this initial list to start and filter those **within the context of a particular situation**—a certain type of IoT device being deployed in a particular environment for a stated purpose. This reflects that in many cases, not all baseline capabilities will be applicable.
- **Appendix A** and the **public comments** serve as the **starting point for baseline candidates**.
- Next step: **Develop a core security capability baseline.**


Capability 2
Capability 1
Capability 3
Possible Cybersecurity Capabilities
Organizational Filters
Capability 1
Capability 3
Capabilities Suited to the Organization's Context



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 Road Map Toward Resilience Against Botnets

- Building on the Botnet Report, DoC and DHS have developed a road map that **charts a path** forward and **sets out a series of tasks** and deadlines for addressing automated, distributed attacks.
- The road map 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.

IoT Line of Effort: Raising the Bar for IoT Security

1. Define a Core Security Capability Baseline (FY19 Q3)

- Establish a core set of security capabilities required for secure deployment of IoT devices, regardless of intended environment (NIST lead)

2. Develop Consumer/Home IoT Security Baseline (FY20 Q1)

- Build on core capabilities to identify security baseline appropriate for consumer/home IoT (IoT industry, civil society, NIST, CSDE/CTA)

3. Establish or Support Assessment Programs for Consumer/Home IoT Devices (FY20 Q2)

- Establish or support agile assessment or attestation programs for consumer/home IoT devices that meet the above baseline (Industry, civil society, CTIA, NIST, other USG stakeholders)

4. Explore Labeling for Consumer/Home IoT (FY20 Q4)

- Explore utility of a voluntary labeling approach, or other informational options, to improve consumer/home IoT device consumer awareness. (FTC, NTIA, other federal partners, IoT Industry)

5. Implement Awareness Strategies for Trustworthy Consumer/Home IoT Devices (FY21 Q2)

- Develop informational tools such as labeling or branding that assist motivated consumers in identification of conforming consumer/home IoT products. (IoT industry, retailers, CSDE/CTA)

6. Federal Support for Consumer/Home IoT Security Baseline & Assessment (FY23 Q1)

- Increase USG engagement with targeted user communities and civil society to promote awareness and acceptance of the consumer/home IoT security baseline and supporting assessment program(s); leverage DHS’ existing awareness activities, such as STOP. THINK. CONNECT. (DHS, Commerce, FTC, civil society)

As Stated in the Botnet Report, the Federal Government Will Lead by Example

1. Define a Core Security Capability Baseline (FY19 Q3)

- Establish a core set of security capabilities required for secure deployment of IoT devices, regardless of intended environment (NIST lead)

2. Identify Federal IoT Security Requirements (FY19 Q4)

- Convene key stakeholders to identify non-core security capabilities that are common to Federal environments (OMB, GSA, DoD, DHS, NIST)

3. Specify Federal IoT Security Baseline (FY20 Q1)

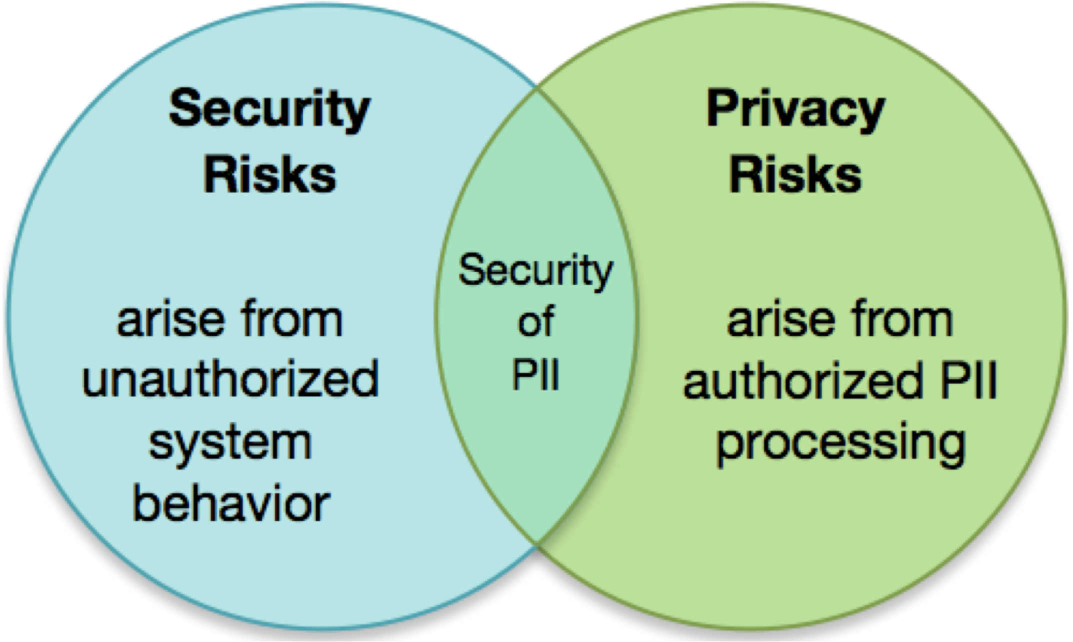
- In collaboration with industry and agencies, develop and publish a Federal IoT security capability baseline (NIST lead)

4. Establish Federal IoT Procurement Regulations (FY21 Q1)

- Establish federal procurement regulations to support acquisition of IoT devices consistent with the federal IoT security capability baseline (GSA lead)

The 15 Initial Baseline Candidates from Draft NISTIR 8228 Appendix A

- 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.
- The IoT device’s **configuration can be securely changed** by authorized users when needed, including restoring a secure default configuration, and unauthorized changes to the IoT device’s configuration 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 **well-known and 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.
- Information confirming the **sources** of all the IoT device’s software, firmware, hardware, and services is **disclosed and accessible.**
- An **inventory** of the IoT device’s current internal software and firmware, including versions and patch status, is **disclosed and accessible.**
- The IoT device can **enforce the principle of least functionality** through its design and configuration.
- The IoT device is designed to allow **physical access** to it to be controlled.
- The IoT device can **interact through an interface** with individuals regarding the device's **progressing of the individual’s PII**.
- Information about what PII the IoT device is **processing** and where the PII may be transmitted is **disclosed and accessible**.
- The IoT device can **read data tags** that identify PII processing **permission**, then conform its processing accordingly.
- The IoT device can be configured to **minimize** the processing of predefined elements of PII.


Security Risks
arise from unauthorized system behavior
Security of PII
Privacy Risks
arise from authorized PII processing

Privacy Framework

- NIST is developing a **framework** that can be used to improve organizations' management of **privacy risk** for individuals arising from the collection, storage, use, and sharing of their information.
- We are putting into account the **parallel privacy efforts** while creating this baseline.
- The upcoming roundtables will just account for the **security capabilities** in Appendix A of Draft NISTIR 8228.
- We removed **four security** capabilities from Appendix A when creating our core baseline using our criteria.

Criteria to Assess Core Baseline Candidates

Utility

How critical is the capability towards improving security?

When used alone, does the capability directly improve the cybersecurity?

Do other cybersecurity capabilities rely on this capability to function?

Which cybersecurity risk mitigation areas does the capability help achieve?

Verifiability

Can the manufacturer easily verified that they have implemented the capability in an IoT device?

Feasibility

Are there roadblocks to implementing the capability that will make the device overly costly, complex, or less interoperable?

Is the hardware, firmware, software, or protocols needed to implement the capability proprietary or other wise limited in availability?

Core Baseline: 7 Top Candidates from Draft NISTIR 8228 Appendix A

- 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.
- The IoT device’s **configuration can be securely changed** by authorized users when needed, including restoring a secure default configuration, and unauthorized changes to the IoT device’s configuration 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 **well-known and 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.

Questions to Consider

1. Are these reasonable capabilities for a core baseline?

   Are any capabilities “**asking too much**?”

   Is the value to cybersecurity for each capability **apparent**?

   Should we **add** or **remove** any capabilities?

2. Are the capabilities **defined with enough specificity** to be useful? Could a **manufacturer** make use of this?

3. Is the **criteria reasonable** for identifying baseline capabilities?

Stakeholder-Engaged Drafting Process: Core Capability Security Baseline

The Program plans to engage with stakeholders from its inception, which informs the approach and the document itself.

To date, the Program has received guidance from:

- Report to the President on Enhancing Resilience Against Botnets
- NIST workshop in Gaithersburg, MD on 7/11
- Public comments of Appendix A on Draft NISTIR 8228
- **Up Next:** Roundtable at CES on January 9th

For this document to be valuable, we need industry participation and feedback.

This is a multi-pronged approach to achieve our vision to support a more secure internet, US competitiveness abroad, and innovation.

Planned approach:

- Release essays to inform stakeholder engagement and discussions
- Roundtables and workshops
- Panel discussions
- Feedback at iotsecurity@nist.gov

Have 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