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

KAREN SCARFONE, SCARFONE CYBERSECURITY

NOVEMBER 9, 2018

Agenda

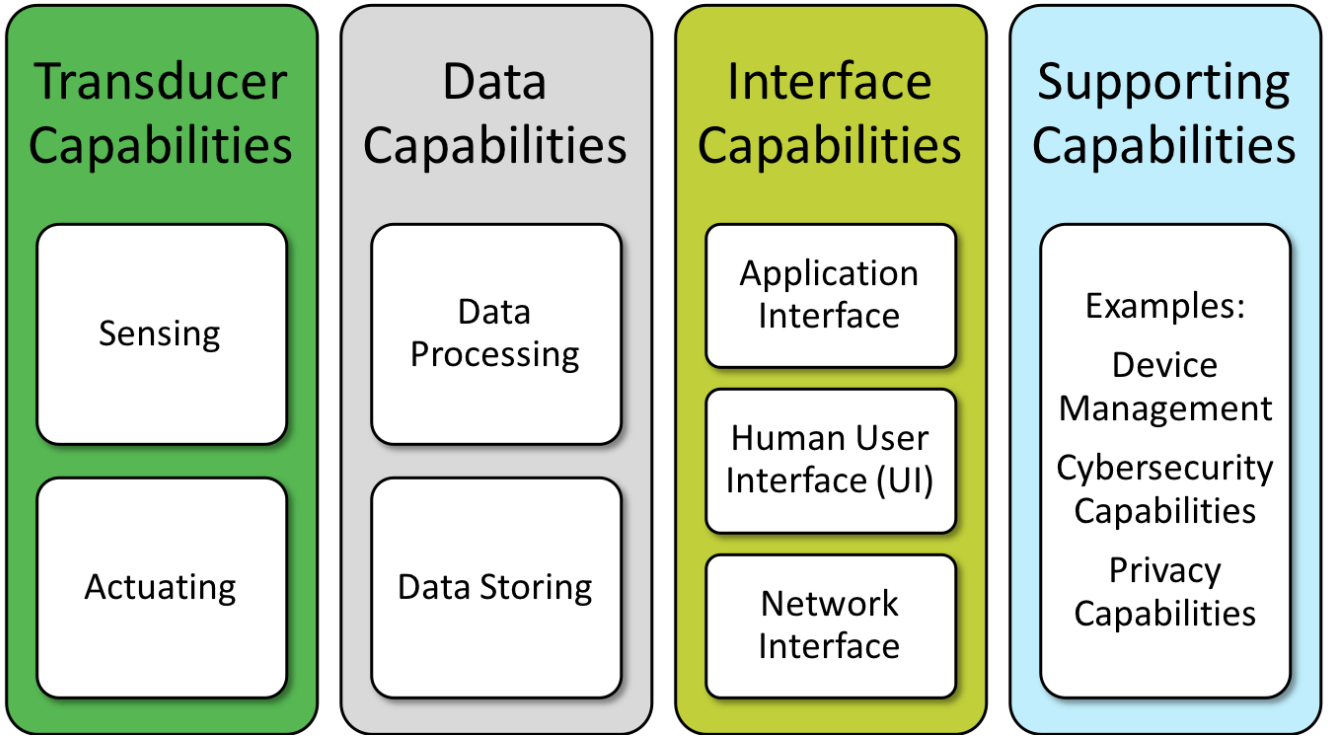
- Explain the key findings and recommendations of draft NIST IR 8228
  - "Show our work" throughout the process so you can see how the lowest-level items trace back to the highest-level concepts
  - Give you an understanding of all the types of findings and recommendations so you can decide which would be helpful to you
- Recap public comments received on IR 8228 that may cause changes to IR 8228 and shape future work
- Preview possible next steps

Draft NISTIR 8228

- Draft NIST Internal Report 8228, *Considerations for Managing IoT Cybersecurity and Privacy Risks* (https://doi.org/10.6028/NIST.IR.8228-draft)
- Public comment period was September 24 – October 24, 2018
- Purpose: help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their IoT devices throughout their lifecycles
- Emphasizes what makes managing these risks different for IoT devices than conventional IT devices, and omits all aspects of risk management that are largely the same for conventional IT and IoT
- Provides insights to inform organizations' existing risk management processes

Capabilities

- Each IoT device provides *capabilities*—features or functions—it can use on its own or in conjunction with other IoT and non-IoT devices.
- IR 8228 references the depicted types of capabilities IoT devices can provide that are of primary interest in terms of affecting cybersecurity and privacy risk. This is not a comprehensive list of all possible capabilities.



Thanks to Eric Simmon at NIST for his work on defining the capabilities

Scoping IoT for IR 8228

- No universally agreed on definition for IoT
- Scoped as all computing devices that are connected to a network and interact with the physical world
  - **Sensing**: the ability to provide an observation of an aspect of the physical world in the form of measurement data. Examples include temperature measurement, computerized tomography scans (radiographic imaging), optical sensing, and audio sensing.
  - **Actuating**: the ability to change something in the physical world. Examples of actuating capabilities include heating coils, cardiac electric shock delivery, electronic door locks, unmanned aerial vehicle operation, servo motors, and robotic arms.

Each IoT device is part of a broader IoT ecosystem, but anything besides the IoT device itself is out of scope, including:

- Other devices (including IoT and non-IoT devices)
- Cloud-based applications and services used by IoT devices
- Mobile apps used to access or manage IoT devices
- People

Starting with a Conventional IT Perspective

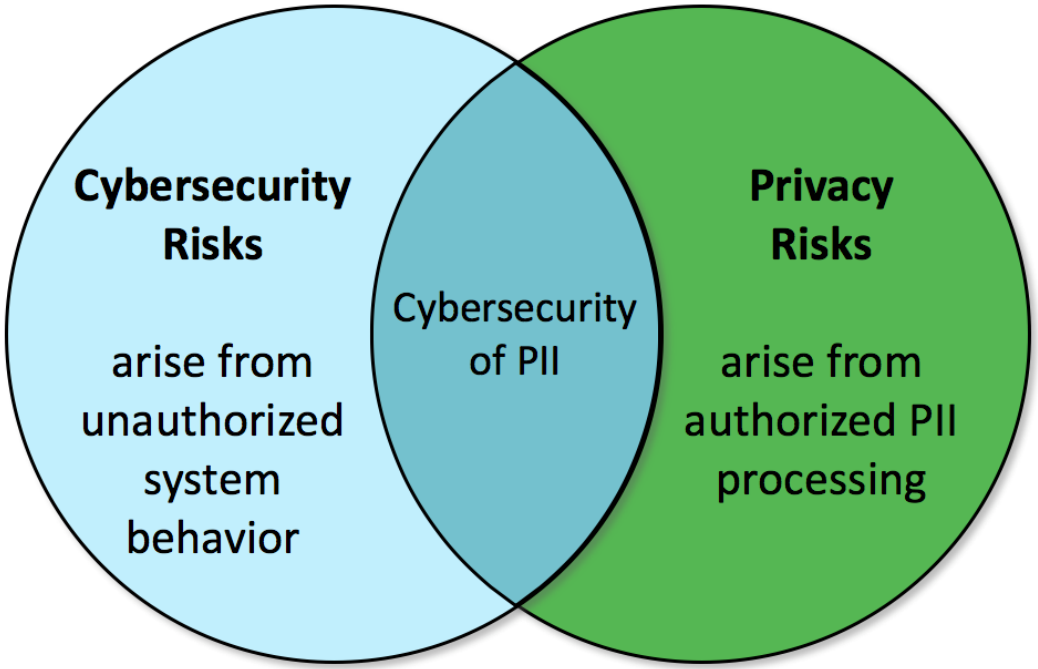
- IoT devices generally face the same types of cybersecurity and privacy risks as conventional IT devices, though the prevalence and severity of such risks often differ.
  - For example, there may not be data security risks for some IoT devices because they lack data capabilities.
- Our approach has been to articulate the differences between managing cybersecurity and privacy risk for conventional IT and for IoT.
- IR 8228 focuses on mitigating risk and does not address other forms of risk response: accepting, avoiding, sharing, and transferring.
  - Our analysis has shown that mitigation options may be significantly different for IoT devices than conventional IT devices.

Scoping Risk

- Only cybersecurity and privacy risks are in scope for this publication.
- For some IoT devices, additional types of risks, including safety, reliability, and resiliency, need to be managed simultaneously with cybersecurity and privacy risks because of the effects addressing one type of risk can have on others.
- For more information on understanding other types of risks and their relationship to cybersecurity and privacy, see NIST SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, which provides an operational technology (OT) perspective on cybersecurity and privacy.

Cybersecurity and Privacy Risk

- For *cybersecurity*, risk is about *threats*—the exploitation of vulnerabilities by threat actors to compromise device or data confidentiality, integrity, or availability.
- For *privacy*, risk is about *problematic data actions*—operations that process PII to meet mission or business needs of an organization or "authorized" PII processing and, as a side effect, cause individuals to experience some type of problem.
- Privacy and cybersecurity risk overlap with respect to concerns about the cybersecurity of PII, but there are also privacy concerns without implications for cybersecurity, and cybersecurity concerns without implications for privacy.



Categories of Findings in IR 8228

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

Risk Considerations

- **Consideration 1: Device Interactions with the Physical World**

  Many IoT devices interact with the physical world in ways conventional IT devices usually do not.

- **Consideration 2: Device Access, Management, and Monitoring Features**

  Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can.

- **Consideration 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.

Risk Consideration 1: Device Interactions with the Physical World

- Potential impact of IoT devices making changes to physical systems and thus affecting the physical world
- Ubiquity of sensors in public and private environments and their collection of data about individuals
- Remote access to physical systems that previously could only be accessed locally
- Conflicts between operational requirements for performance, reliability, resilience, and safety, and common cybersecurity and privacy practices for conventional IT devices
- Availability and integrity may be more important than confidentiality

Risk Consideration 2: Device Access, Management, and Monitoring Features

- "Black boxes" with little or no internal visibility
- Numerous challenges, including availability of features and interfaces, management at scale, lifespan expectations, lack of inventory capabilities, and heterogeneous ownership
- Can necessitate many changes to conventional IT practices, including
  - Doing tasks manually for large numbers of IoT devices
  - Expanding staff knowledge and tools to include a much wider variety of IoT device software
  - Addressing risks with manufacturers and other third parties having remote access or control over IoT devices

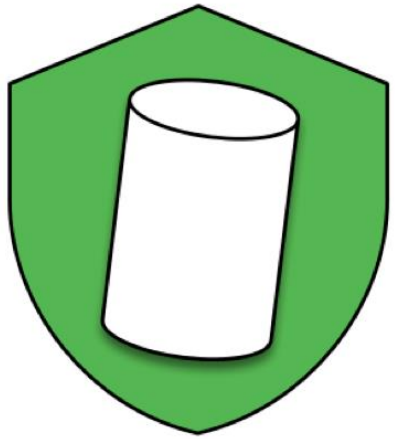
Risk Consideration 3: Cybersecurity and Privacy Capability Availability, Efficiency, and Effectiveness

- Two types of cybersecurity and privacy capabilities
  - *Pre-market*: built in to IoT devices
  - *Post-market*: selected, acquired, and deployed by organizations themselves
- Many IoT devices do not or cannot support the range of cybersecurity and privacy capabilities typically built into conventional IT devices
- The level of effort needed to manage, monitor, and maintain pre-market capabilities on each IoT device may be excessive
- Some post-market capabilities for conventional IT may not be as effective at protecting IoT devices as they are at protecting conventional IT

Risk Mitigation Goals

Protect device security

- Prevent a device from being used to conduct DDoS attacks, eavesdrop on local network traffic, or compromise other devices on the same network segment.
- Goal applies to all IoT devices.



Protect data security

- Protect the confidentiality, integrity, and/or availability of data collected by, stored on, processed by, or transmitted to or from the IoT device.
- Goal applies to each IoT device with data that needs protection.

Protect individuals' privacy

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

Risk Mitigation Areas for Goal 1, Protect Device Security

- **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.

Risk Mitigation Areas for Goal 2, Protect Data 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.

Risk Mitigation Areas for Goal 3, Protect Individuals' Privacy

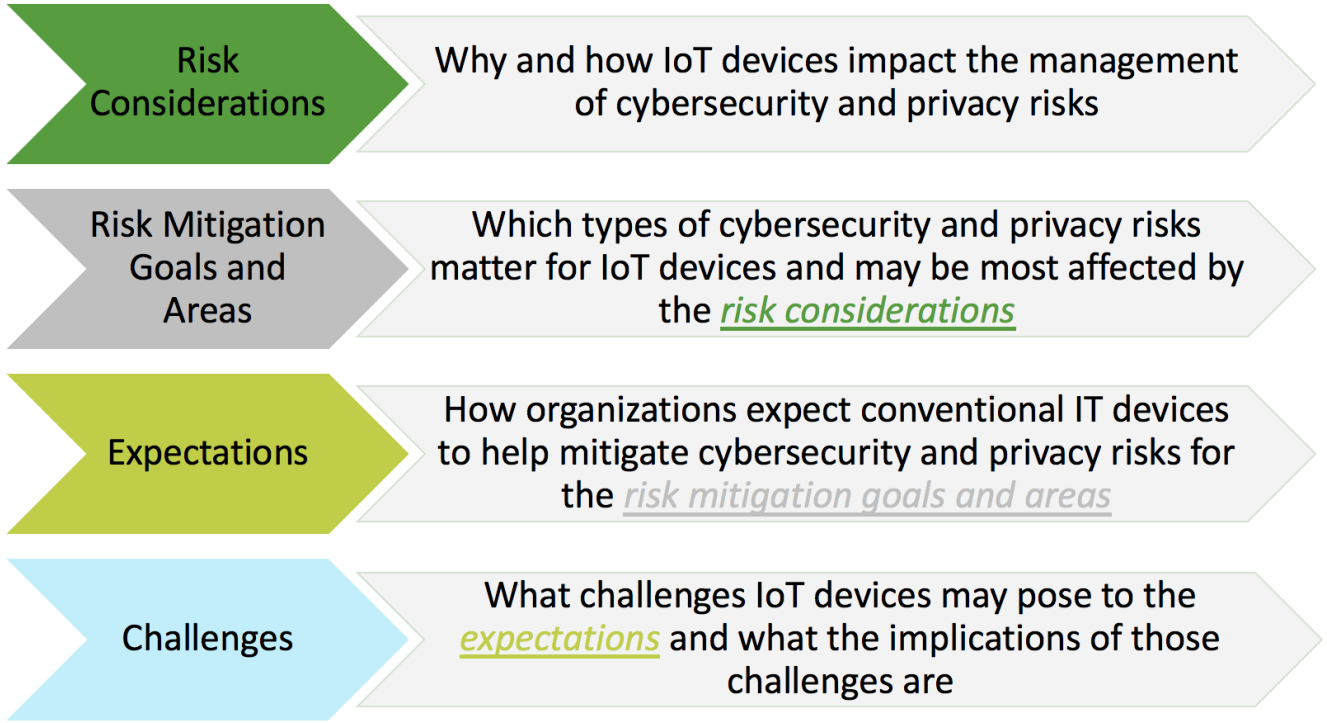
- **Information Flow Management:** Maintain a current, accurate mapping of the information lifecycle of PII, including the type of data action, the elements of PII being processed by the data action, the party doing the processing, and any additional relevant contextual factors about the processing to 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.

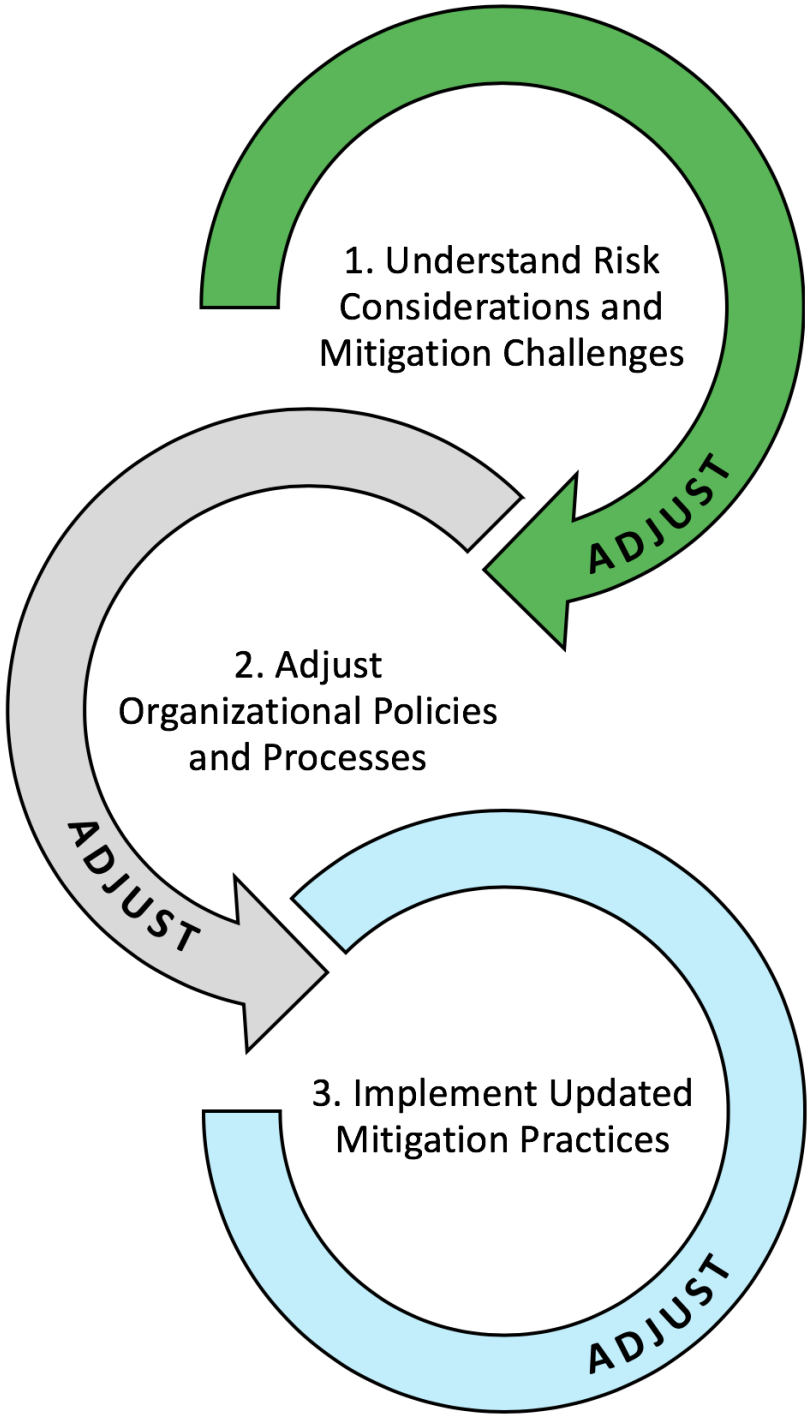
Examples of Potential Challenges with Achieving Risk Mitigation Goals

Challenges for Individual IoT Devices, and Risk Considerations Causing the Challenges	Affected Draft NIST SP 800-53 Revision 5 Controls	Implications for the Organization	Affected Cybersecurity Framework Subcategories
Asset Management			
Expectation 1: The device has a built-in unique identifier.			
1. The IoT device may not have a unique identifier that the organization's asset management system can access or understand. **Risk Consideration 2**	• CM-8, System Component Inventory	• May complicate device management, including remote access and vulnerability management.	• ID.AM-1: Physical devices and systems within the organization are inventoried
Expectation 2: The device can interface with enterprise asset management systems.			
2. The IoT device may not be able to participate in a centralized asset management system. **Risk Consideration 2**	• CM-8, System Component Inventory	• May have to use multiple asset management systems. • May have to perform asset management tasks manually.	• ID.AM-1: Physical devices and systems within the organization are inventoried • ID.AM-2: Software platforms and applications within the organization are inventoried • PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition

Summary of Potential Challenges with Achieving Risk Mitigation Goals

- Identified 25 expectations for the pre-market capabilities of conventional IT devices
- Identified 49 challenges to those 25 expectations that individual IoT devices may pose
- Most expectations and challenges involve Goal 1, Protect Device Security

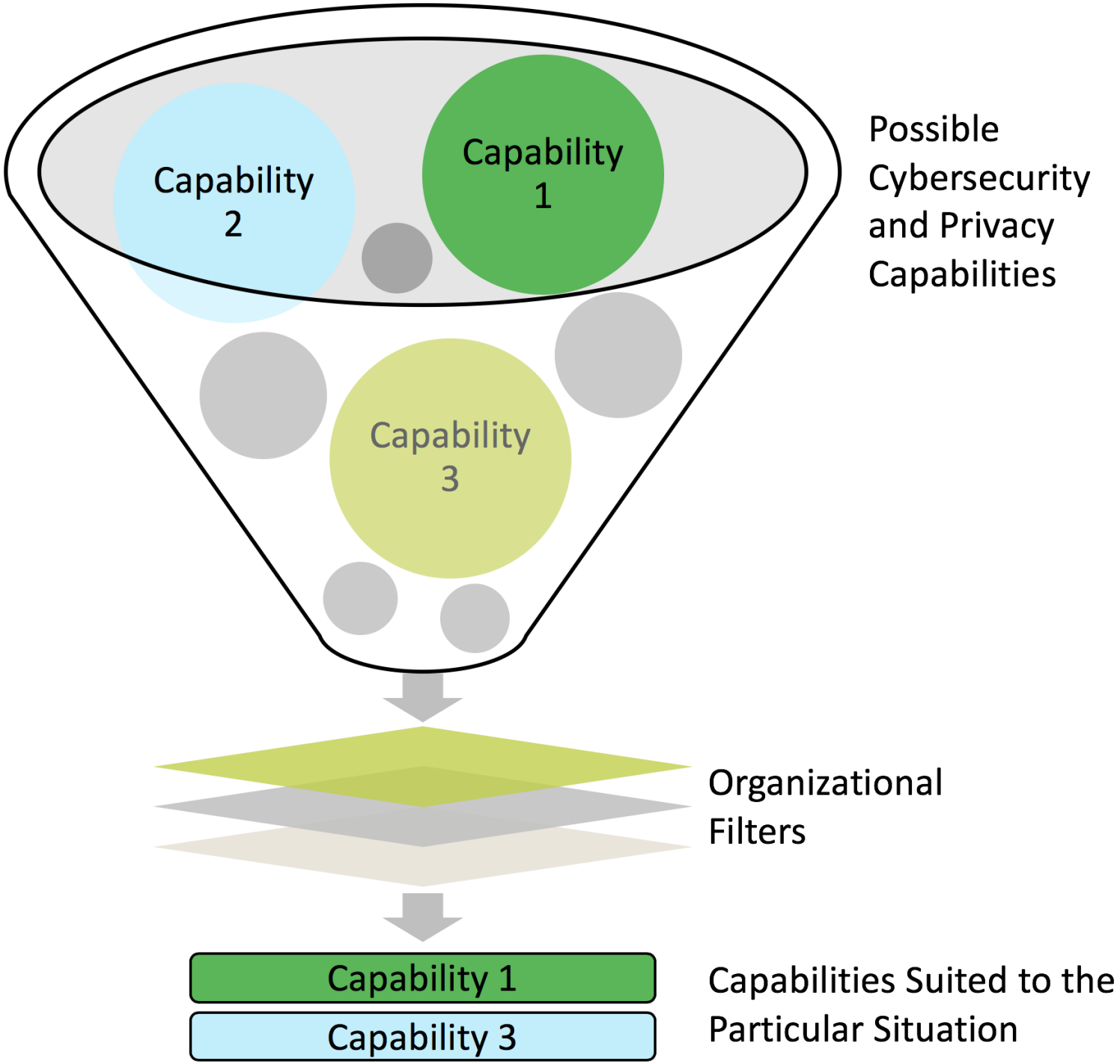




Recommendations for Addressing Risk Mitigation Challenges

1. Understand the IoT device risk considerations and the challenges they may cause to mitigating cybersecurity and privacy risks for IoT devices in the appropriate risk mitigation areas.
2. Adjust organizational policies and processes to address the cybersecurity and privacy risk mitigation challenges throughout the IoT device lifecycle.
3. Implement updated mitigation practices for the organization's IoT devices as you would any other changes to practices.

Filtering Capabilities within the Context and Risk of a Particular Situation



Examples Based on Selected IoT Guidance Documents

- Broadband Internet Technical Advisory Group (BITAG), "Internet of Things (IoT) Security and Privacy Recommendations"
- Cloud Security Alliance (CSA) Mobile Working Group, "Security Guidance for Early Adopters of the Internet of Things (IoT)"
- CSA IoT Working Group, "Identity and Access Management for the Internet of Things"
- CTIA, "CTIA Cybersecurity Certification Test Plan for IoT Devices, Version 1.0"
- European Union Agency for Network and Information Security (ENISA), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures"
- Groupe Spéciale Mobile Association (GSMA), "GSMA IoT Security Assessment"
- Industrial Internet Consortium (IIC), "Industrial Internet of Things Volume G4: Security Framework"
- IoT Security Foundation (IoTSF), "IoT Security Compliance Framework, Release 1.1"
- Online Trust Alliance (OTA), "IoT Security & Privacy Trust Framework v2.5"
- United Kingdom Government Department for Digital, Culture, Media & Sport (DCMS), "Secure by Design: Improving the cyber security of consumer Internet of Things"

Example of Possible Cybersecurity Capabilities for IoT Devices

Possible Capabilities	Cybersecurity Framework Subcategories	Draft SP 800-53 Revision 5 Controls	References to Selected IoT Guidance Documents
Protect Device Security—Asset Management			
1. The IoT device can be identified both logically and physically. **Expectation 1**	• ID.AM-1: Physical devices and systems within the organization are inventoried • ID.AM-2: Software platforms and applications within the organization are inventoried • PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes • PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition • PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools • PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	• CM-8 • IA-3 • PE-20	• BITAG: 7.2, 7.6 • CSA1: 5.2.1.1, 5.3.1, 5.3.4 • CSA2: 11, 14 • CTIA: 4.13 • ENISA: PS-10, TM-21 • GSMA: CLP11_5.2.1, CLP13_6.6.2, 6.8.1, 6.20.1, 8.11.1 • IIC: 7.3, 8.5 • IoTSF: 2.4.14.3-4, 2.4.8.1 • UKDDCMS: 4

Examples of Possible Capabilities for Goals 1 and 2 by Area

- Goal 1, Asset Management
  1. The IoT device can be identified both logically and physically.
  2. Information confirming the sources of all the IoT device's software, firmware, hardware, and services is disclosed and accessible.
  3. An inventory of the IoT device's current internal software and firmware, including versions and patch status, is disclosed and accessible.
- Goal 1, Vulnerability Management
  4. The IoT device's software and firmware can be updated using a secure, controlled, and configurable mechanism.
  5. 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.
  6. The IoT device can enforce the principle of least functionality through its design and configuration.

Examples of Possible Capabilities for Goals 1 and 2 by Area

- Goal 1, Access Management
  7. Local and remote access to the IoT device and its interfaces can be controlled.
  8. The IoT device is designed to allow physical access to it to be controlled.
- Goal 2, Data Protection
  9. The IoT device can use cryptography to secure its stored and transmitted data.
  10. The IoT device can use well-known and standardized protocols for all layers of the device's data transmissions.
- Goals 1 and 2, Incident Detection
  11. The IoT device can log the pertinent details of its security events and make them accessible to authorized users and systems.

Recap of Public Comments on IR 8228

- NIST received hundreds of comments total from approximately 30 organizations and individuals.
- Nearly all commenters were positive about the document.
- Most commenters offered suggestions for small improvements to or expansions of the material.
- Several commenters also shared their thoughts about additional aspects of IoT cybersecurity and privacy risk management NIST should consider addressing in the future.

Some Suggestions for Improving IR 8228

1. Define "Internet of Things" (and don't define it)
2. Add safety risks to the scope of the document
3. Include recommendations for mitigating supply chain risks
4. Add a fourth risk mitigation goal on system protection
5. Add considerations for risk avoidance
6. Provide the Appendix A content in additional formats
7. Provide more details on how risk can be mitigated
8. Talk about risk and risk mitigation in terms of IoT devices and their environments, systems, etc.
9. Add references to the General Data Protection Regulation (GDPR) and use Personal Information (PI), not just PII
10. Emphasize making IoT devices secure by design

Suggestions for Future NIST Work

- Address risk management for other components of the IoT ecosystem, not just the IoT devices themselves
- Provide mitigation recommendations for more specific groups of IoT devices and for particular sectors
- Continue development of Appendix A examples into a capabilities baseline, then create versions of this baseline specific to particular sectors, uses, etc.

Next Steps

- Refine IR 8228 based on public feedback
  - Contact us at iotsecurity@nist.gov
- Continue work on capabilities baselines, with Appendix A content as a starting point
- Post a blog entry or short essay on our thoughts on IoT baselines, and solicit feedback on our approach
- Continue to review new IoT standards, guidelines, etc. and learn from them

Thank you! Questions?

- karen@scarfonecybersecurity.com