

Welcome to

***Considerations for
Consumer Router
Cybersecurity:***

NIST Discussion Forum

Agenda (all times are EST)

1:00-1:05pm – Welcome, Barbara Cuthill (NIST)

1:05-1:50pm – Router Profile Update and Presentation, Mike Fagan (NIST)

Reference: Preliminary Draft: IoT Cybersecurity Profile for Consumer Grade Routers

1:50-2:35pm – Q&A and Discussion

2:35-2:45pm – Coffee Break

2:45-3:30pm – Products and Product Components, Mike Fagan

Reference: Discussion Essay: IoT Product Component Requirements

3:30-4:15pm – Q&A and Discussion

4:15-4:30pm – Recap and Closing Fireside Chat, Barbara Cuthill/Mike Fagan



NIST's Consumer Router Cybersecurity Profile

Michael Fagan, NIST
7 December 2023

Motivations to develop a consumer router cybersecurity profile

- Routers are “a higher-risk type of product that, if compromised, can be used to eavesdrop, steal passwords, and attack other devices and high value networks” – *W.H. Statement – 7/18/23*
 - Nexus for all home products, including consumer IoT products
- NIST to “define cybersecurity requirements for consumer-grade routers”
- Linked to Cyber Trade Mark announcement:
 - Program could be expanded to include routers

Starting Point for developing a consumer router cybersecurity profile



- Consumer Profile came from EO 14028 (May 2021):
 - *NIST will “identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law”*
- Approach:
 - Build from IR 8259A / 8259B Core Baselines
 - Tailor to consumer IoT needs and product orientation
 - Finalized in Consumer Profile (IR 8425)
- Consumer profile scoped to apply to all consumer-grade IoT products

Path for developing a consumer router cybersecurity profile



- Consumer-grade routers build on that scope:
 - “Consumer-grade routers are defined as networking devices that forward data packets, most commonly Internet Protocol (IP) packets, between networked systems which are primarily intended for residential use and can be installed by the customer.”
- Consumer-grade routers have risks and vulnerabilities specific to the product type:
 - Central to home network, helps transmit data from many other products
 - Broad deployment, most homes have one







- **Baselines & Profiles**
 - *Background on Cybersecurity for IoT guidance*
- **Consumer-Grade Router Profile Objectives & Scope**
 - *Which products and parts of products are intended to be covered by the consumer-grade router profile*
- **Applying Industry Standards**
 - *How the consumer-grade router profile was developed using existing industry standards*
- **Consumer-Grade Router Profile Draft**
 - *Status of the consumer-grade router profile draft and discussion of content*
- **Next Steps**
 - *What NIST is planning next and other opportunities for engagement*



Baselines & Profiles





- Baseline: a set of device capabilities / manufacturer non-technical supporting capabilities generally needed to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems (NIST IR 8259A/B)
 - A “starting point” for identifying needed capabilities
- Profile: the application of sector- and/or use case-specific information to select capabilities most applicable to the needs of customers (NIST IR 8425)
 - Somewhat akin to a Cybersecurity Framework Profile

We begin from our IoT Cybersecurity Capability Core Baseline . . .

	Asset Identification	Products are uniquely identified and all components inventoried
	Product Configuration	Product can be configured for security by authorized users
	Data Protection	Data is protected during storage and transmission
	Interface Access Control	Interface access is restricted to authorized individuals, services, and product components
	Software Update	Product components can receive, verify, and install software updates
	Cybersecurity State Awareness	Product captures and records information about its cybersecurity state

... and Our IoT Non-Technical Supporting Capability Core Baseline



 Documentation	Product developers create, gather, and store information relevant to the cybersecurity of the product
 Information & Query Reception	Product developers can receive information and answer queries regarding the cybersecurity of the product
 Information Dissemination	Product developers provide cybersecurity-relevant information via various channels
 Product Education & Awareness	Product developers create awareness and educate customers regarding product

We have developed 3 profiles to-date

- Federal Profile (SP 800-213A, Appendix A)
 - Based on the RMF low-impact baseline
 - Starting point for Federal agencies integrating IoT
 - Extended 8259A baseline with Device Security category
- Consumer IoT Product Profile (NIST IR 8425)
 - Starting point for businesses building consumer IoT products
 - Expanded baseline applicability to IoT *Products*
- Consumer-Grade Router Cybersecurity Profile
 - Subject of today's discussions

The background of the slide features a complex network diagram. It consists of numerous interconnected nodes, represented by small circles in shades of blue, green, and orange. These nodes are linked by thin, light-colored lines, creating a dense web of connections. The overall aesthetic is technical and digital, with a dark blue color palette.

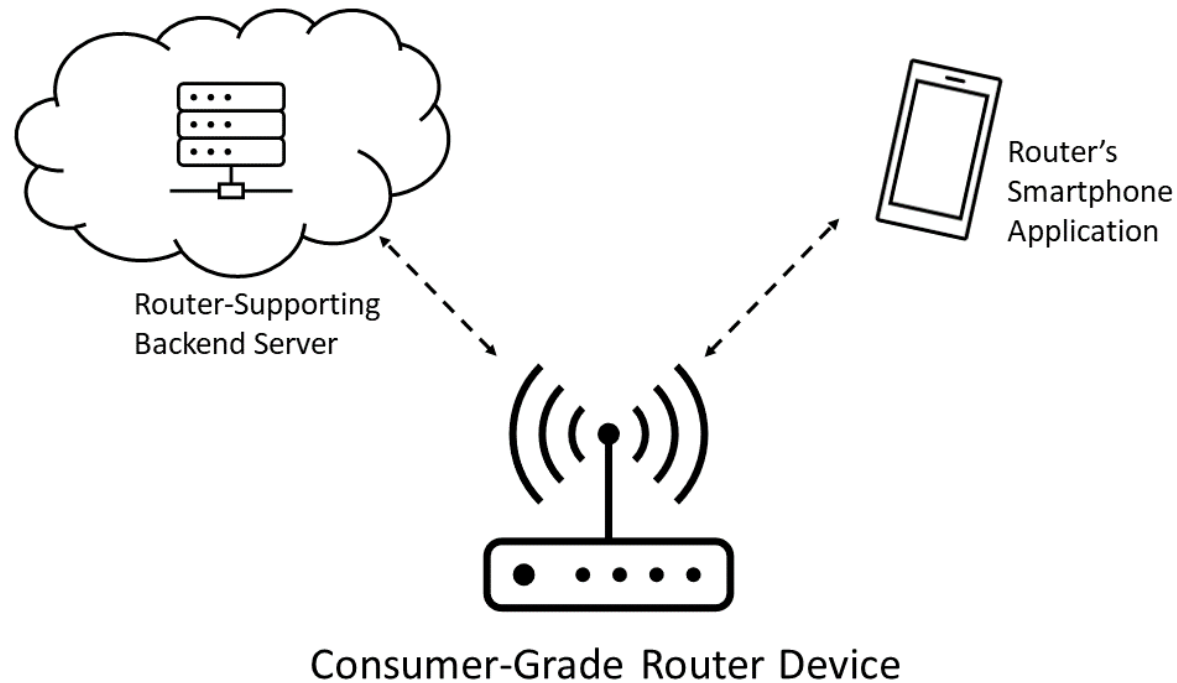
Consumer-Grade Router Profile Objectives & Scope

Why IoT *Product* Scope?

- Complex IoT products may contain multiple physical IoT devices, contain other kinds of equipment, or connect to multiple backends or companion applications as components.
 - Specialty Networking Hardware
 - Companion Application Software
 - Backend Services
- Product components have access to the IoT device and its data
 - Become attack vectors that impact the IoT device, customer, and others (e.g., via attacks on systems or the Internet at large)
- The entire IoT product, including auxiliary components, must be securable

Why IoT *Product* Scope?

Example Additional Router Product Components



- **The entire IoT product, including auxiliary components, must be securable**

- Traffic Processing
 - Routing Between Private (LAN) and Public (Internet)
 - Port and Address Translation
- Auxiliary Functions
 - DHCP, DNS, Network Time, ...
- Control & Configuration ← Focal Point for Cybersecurity
 - May have app-based and/or cloud-based management tools

- Consumer-grade routers can be:
 - Owned by the consumer, generally purchased at retail
 - Rented by the consumer, generally from their Internet Service Provider
- Technical Product Cybersecurity Seems Consistent for Retail Purchased vs. Service Provider Leased Routers
 - But how technical cybersecurity capabilities are used and more importantly by whom may have implications for non-technical cybersecurity



Applying Industry Standards

- Consumer-Grade Router Device Cybersecurity Capabilities:
 - Broadband Forum TR-124 Issue 8 – *Functional Requirements for Broadband Residential Gateway Devices (Cybersecurity Requirements Only)*
 - CableLabs *Security Gateway Device Security Best Common Practices*
 - BSI TR-03148: *Secure Broadband Router - Requirements for secure Broadband Routers*
 - Infocomm Media Development Authority (IMDA) *Technical Specification Security Requirements for Residential Gateways*
- Gap: Standards for other Consumer-Grade Router Components and Non-Technical Supporting Capabilities

We applied a consistent analysis process

- **Group** requirements into their applicable Consumer IoT Product Profile outcome or sub-outcome.
 - Identify any additional outcomes or sub-outcomes needed
- **Define** SHALLs and SHOULDs, starting from the source documents' designations
- **Consolidate** For each outcome, determine if the set of extracted requirements are complementary or if any are contradictory.
 - **Complementary requirements** are those that can be used together without conflict
 - **Contradictory requirements** cannot be used together because of a conflict or some other issue.
- **Expand:** consider tailoring the profile to include a new outcome or sub-outcome that reflects the requirements.
- **Tailor:** Use the grouped and pruned requirements to, if necessary, tailor the outcomes of the Consumer IoT Product Profile outcomes by adjusting or amending the language to more directly identify concepts reflected in the source document's requirements.

Example Requirement Grouping and Consolidation



- Sub-outcome: Data Protection 1 -- Each IoT product component protects data it stores via secure means.
- Extracted associated requirements

Data Protection	-
Data Protection 1 <i>Data at rest is protected.</i>	BBF SEC.FIRMWARE.2 CL DRP-001, KEY-001, KEY-002, KEY-003, HR-003, HR-004, SB-005, OOB-002 BSI (4.1.1)[7] IMDA 4.5

- Identified four groups of concepts in requirements:
 - Data protection with encryption or hashing
 - Data storage capabilities
 - Cryptographic algorithm agility
 - Physical security of the product
- No conflicts identified between any requirements

Crosswalk Essay, 25 October 2023

New Cybersecurity Sub-Outcomes that Expand on NISTIR 8425



- **Software Update 3:** Integrity of data, including configuration is preserved when an update is applied.
 - *Related Standards Requirements:*
 - **BBF GEN.OPS.15, GEN.OPS.24**
 - **CL SU-004**
- **Cybersecurity State Awareness 2:** The consumer-grade router product can inform authorized entities about or respond directly to changes in cybersecurity information.
 - *Related Standards Requirements:*
 - **BBF GEN.OPS.6**
 - **CL AR-002**

Cybersecurity Outcomes Tailored for Consumer-Grade Routers



The IoT product protects data stored across all IoT product components and transmitted both between IoT product components and outside the IoT product from unauthorized access, disclosure, and modification.

Cybersecurity Outcomes Tailored for Consumer-Grade Routers

The IoT product protects data stored across all IoT product components and transmitted both between IoT product components and outside the IoT product from unauthorized access, disclosure, and modification.



The **consumer-grade router** product protects data stored across all **consumer-grade router** product components and transmitted both between **consumer-grade router** product components and outside the **consumer-grade router** product from unauthorized access, disclosure, and modification.

- **Software Update 1:** Each consumer-grade router product component can receive, verify, and apply verified software updates.
 - *Related Standards Requirements:*
 - **BBF** GEN.OPS.22, GEN.OPS.23
 - **CL** KEY-004, KEY-005, SB-001, SU-001, SU-005, SBOM-009, SB-002, SU-003
 - **BSI** (4.2)[1], (4.2)[3], (4.2)[3], (4.2)[6]
 - **IMDA** 4.3

Verification of updates is required by all of the standards. All four standards either imply or explicitly state that devices be updateable

- **Software Update 1:** Each consumer-grade router product component can receive, verify, and apply verified software

BBF recommends
and CL requires
signing updates.

Standards Requirements:

- **BBF** GEN.OPS.22, GEN.OPS.23
- **CL** KEY-004, KEY-005, SB-001, SU-001, SU-005, SBOM-009, SB-002, SU-003
- **BSI** (4.2)[1], (4.2)[3], (4.2)[3], (4.2)[6]
- **IMDA** 4.3

- **Software Update 1:** Each consumer-grade router product component can receive, verify, and apply verified software updates.
 - *Related Standards Requirements:*
 - **BBF** GEN.OPS.22, GEN.OPS.23
 - **CL** KEY-004, KEY-005, SB-001, SU-001, SU-005, SBOM-009, SB-002, SU-003
 - **BSI** (4.2)[1], (4.2)[3], (4.2)[3], (4.2)[6]
 - **IMDA** 4.3

BSI recommends redundant storage.

The background features a complex network diagram with various nodes and connecting lines in shades of blue, green, and orange. The nodes are represented by small circles and triangles, some of which are highlighted in green. The lines represent connections between these nodes, creating a web-like structure. The overall aesthetic is technical and digital.

Consumer-Grade Router Profile Draft

How the Outcomes are Defined in Full

Consumer-grade router...	Technical Outcomes	Non-technical Outcomes
Device	Sections 3.1.1-3.1.7	Section 3.1.8 + TBD
Additional Product Components	TBD	TBD

- Consumer-grade router devices could meet the technical cybersecurity outcomes using all four standards
- Additional consumer-grade router components would need additional guidance to meet technical cybersecurity outcomes when included in a consumer-grade router product
- Additional guidance will be needed to completely meet the non-technical cybersecurity outcomes for a consumer-grade router product

Technical Cybersecurity Outcomes and Consumer-grade Router Devices



- Our analysis revealed no conflicting requirements among the four standards within each grouping
- Standards represent current recommended practice but with varying scope and details
- All four existing consumer-grade router standards analyzed define the technical cybersecurity outcomes from consumer-grade route *devices*

Additional Consumer-Grade Router Product Components



- Many consumer-grade routers need additional product components
- Existing standards define router device requirements, and do not address additional components
- Additional product components are less tailored to the specific use case (i.e., consumer-grade router)
 - Ex: Mobile app cybersecurity approaches are similar for most mobile apps
- An approach specific to the additional components is suitable
- To be addressed more thoroughly in Forum Part 2

- Non-technical supporting outcomes are largely decoupled from device / product / sector / customer specifics
- A general approach is suitable
- Standards for non-technical outcomes aren't numerous
- Some NIST standards apply
 - Cybersecurity Framework
 - Secure Software Development Framework
- To be addressed more thoroughly in Forum Part 2



Next Steps

The Months Ahead...

December 2023

Continue to gather feedback, engage with community, and iterate on the draft consumer-grade router profile

Milestone: Comment Close on 12/21

January 2024

Socialize newest draft, gather additional feedback, work towards finalizing the consumer-grade router profile

Milestone: Next Router Profile Draft

February 2024

Gather final feedback, develop the final draft of consumer-grade router profile for publication

THANK YOU

CONTACT US



[NIST.gov/cybersecurity](https://www.nist.gov/cybersecurity)



[@NISTcyber](https://twitter.com/NISTcyber)



NIST Cybersecurity for IoT
Program Home Page

Agenda (all times are EST)

1:00-1:05pm – Welcome, Barbara Cuthill (NIST)

1:05-1:50pm – Router Profile Update and Presentation, Mike Fagan (NIST)

Reference: Preliminary Draft: IoT Cybersecurity Profile for Consumer Grade Routers

1:50-2:35pm – Q&A and Discussion

2:35-2:45pm – Coffee Break

2:45-3:30pm – Products and Product Components, Mike Fagan

Reference: Discussion Essay: IoT Product Component Requirements

3:30-4:15pm – Q&A and Discussion

4:15-4:30pm – Recap and Closing Fireside Chat, Barbara Cuthill/Mike Fagan

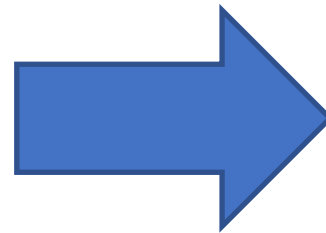
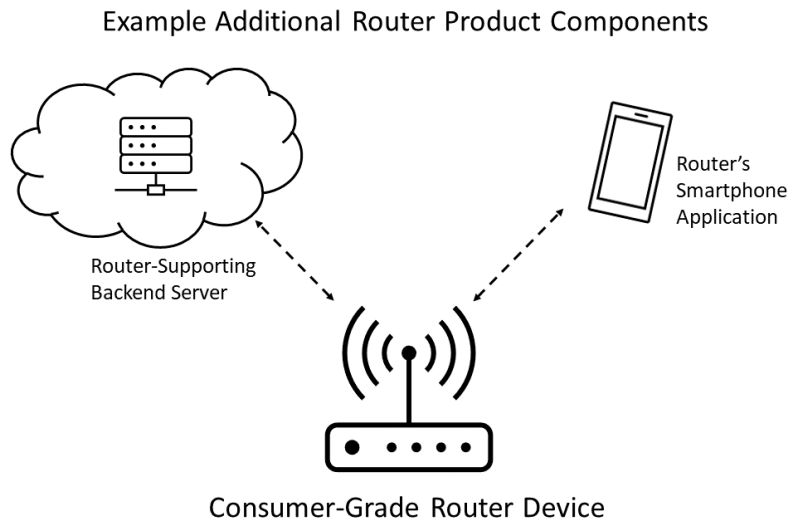


Standards & Guidance for a Consumer IoT Product Development Handbook

Michael Fagan, NIST
7 December 2023

A Shift In Focus

From: Consumer Grade Routers

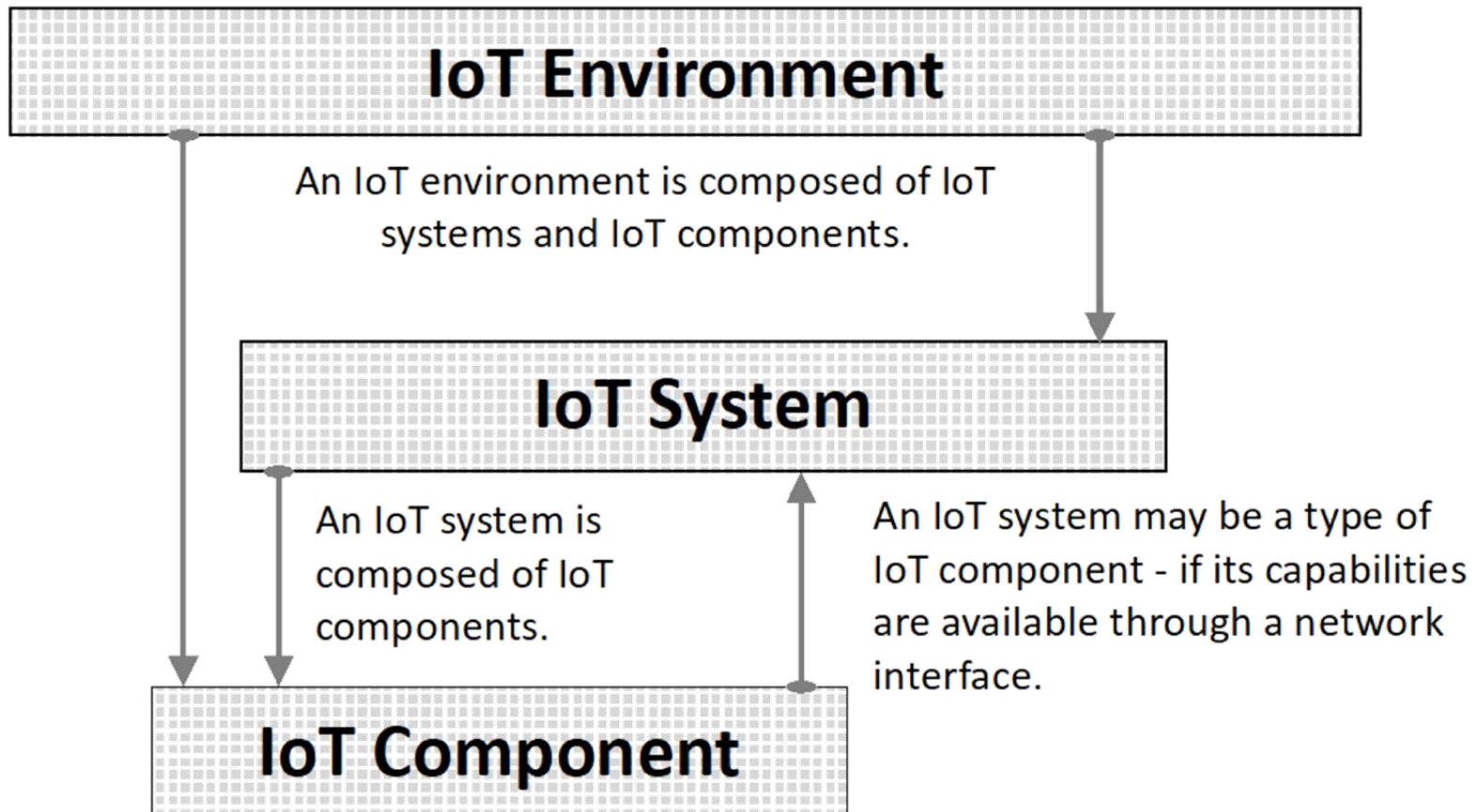


To: Consumer IoT Products

Cybersecurity of IoT devices, though critical, is incomplete if cybersecurity of other IoT product components is not considered as well since the IoT device and other IoT product components will be a system.

- Additional components = additional attack surface
 - More interfaces, more access to data: more risk
- Technical And Non-technical Outcomes Apply Product-wide
- Guidance addressing products assists developers toward securability

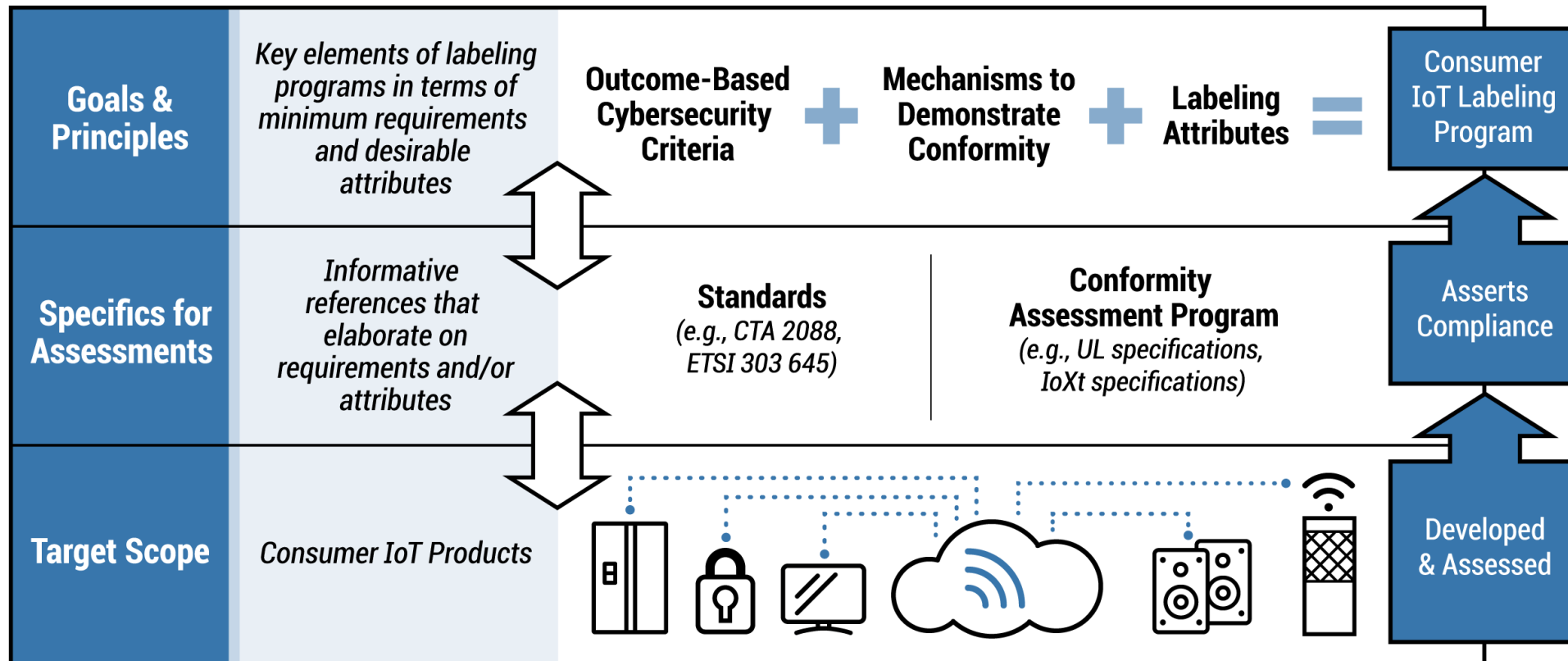
IoT Product Are Systems and Components Of Systems



Product components include:

- IoT device(s)
- Mobile & desktop management applications
- Specialty hardware
- Cloud storage backends
- Any SW or HW/SW element essential to product function

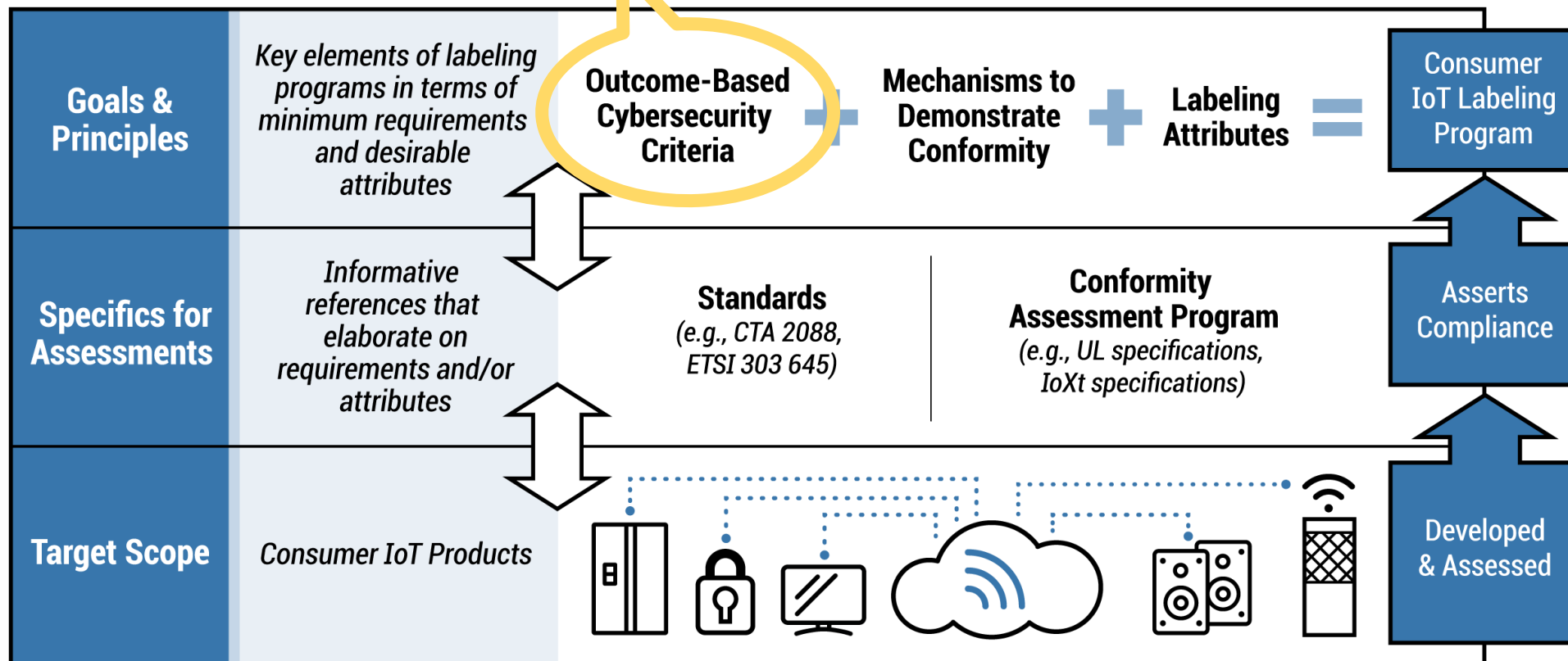
Outcomes vs. Requirements



Outcomes vs. Requirements

Outcomes: Guidelines describing *what* is expected; e.g.,

- Data Protection
- Verifiable Software Updates



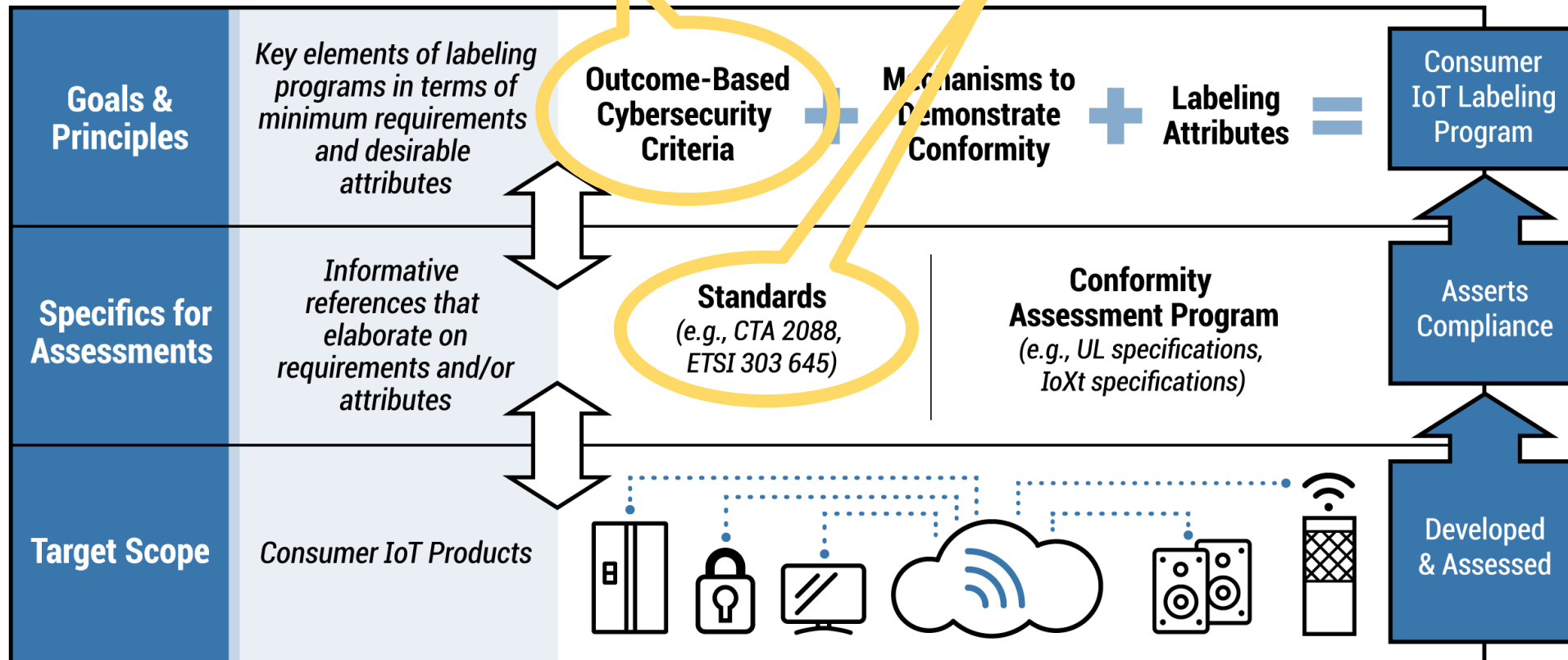
Outcomes vs. Requirements

Outcomes: Guidelines describing *what* is expected; e.g.,

- Data Protection
- Verifiable Software Updates

Requirements: Statements of *how* to achieve an outcome; e.g.,

- Encryption, tamper-proof storage
- Signed update packages



- **Discuss Example Standards And Guidance To Address**
 - Technical cybersecurity
 - Non-Technical cybersecurity
- **NIST Has Identified Example Standards; Consider**
 - Applicability, Value
 - Other Candidate Standards
- **Next Steps**
 - *What NIST is planning next and other opportunities for engagement*

Technical Cybersecurity







The image features a dark blue background with a faint, abstract network of interconnected nodes and lines in shades of green, blue, and orange. A white rectangular border frames the central text area. The text 'Technical Cybersecurity' is written in a large, bold, white sans-serif font, centered horizontally and vertically within the frame.

... the measures taken in the hardware and software of the IoT product's components to address and reduce risks

- Outcomes for *IoT Devices* can be satisfied by applying both general & product- / sector- / use case-oriented standards
 - e.g., four standards identified for routers
- Outcomes for other *IoT Product Components* often rely on more general standards

Technical Cybersecurity Outcomes (NIST IR 8529A)



	Asset Identification	Products are uniquely identified and all components inventoried
	Product Configuration	Product can be configured for security by authorized users
	Data Protection	Data is protected during storage and transmission
	Interface Access Control	Interface access is restricted to authorized individuals, services, and product components
	Software Update	Product components can receive, verify, and install software updates
	Cybersecurity State Awareness	Product captures and records information about its cybersecurity state

Identified Standards for IoT Device Technical Cybersecurity



- [ISO/IEC 27402](#) (Cybersecurity – IoT security and privacy – Device baseline requirements)
- [ANSI/CTA-2088-A](#) - Baseline Cybersecurity Standard for Devices and Device Systems
- [ETSI 303-645](#) - Cyber Security for Consumer Internet of Things: Baseline Requirements
- All tiers of Singapore's [Cyber Security Agency's Cybersecurity Labeling Scheme](#)

- IoT product components can be implemented in:
 - Software (that is installed or hosted)
 - Hardware and Software (packaged in equipment)
- Software can be hosted on Platforms (e.g., cloud backend)
 - It may also be installed on customer's systems (e.g., smartphone)

Identified Standards IoT Product Component Technical Cybersecurity



- NIST's [Recommended Criteria for Cybersecurity Labeling of Consumer Software](#)
 - This document provides clear, testable claims for software cybersecurity.
- OWASP's [Application Security Verification Standard](#), [Mobile Application Security Testing Guide](#), and [Web Security Testing Guide](#)
 - These standards and guidance documents provide extensive requirements for different types of software.
- [ISO 9001](#) (Quality management systems — Requirements)
 - Hardware development quality management
- Cloud Security Alliance's Security, Trust, Assurance and Risk ([STAR](#)) Program
 - Cloud Platforms







Non-Technical Cybersecurity

... the measures an organization takes to support cybersecurity over a product's lifecycle

- Non-technical cybersecurity is less product-specific
- Not generally addressed in product- / sector- / use case-oriented standards
- Non-technical cybersecurity outcomes would be the same for many digital products and services
- Apply broadly-applicable cybersecurity standards to the product *as a whole*

Non-Technical Cybersecurity Outcomes (NIST IR 8529B)

 Documentation	Product developers create, gather, and store information relevant to the cybersecurity of the product
 Information & Query Reception	Product developers can receive information and answer queries regarding the cybersecurity of the product
 Information Dissemination	Product developers provide cybersecurity-relevant information via various channels
 Product Education & Awareness	Product developers create awareness and educate customers regarding product

Identified Standards for Documentation 1a-d



Cybersecurity Outcome	Potential References
Documentation 1a. Assumptions made during the development process and other expectations related to the IoT product.	ISO 9001 (Quality management systems — Requirements) ISO/IEC TS 19249 (Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications)
Documentation 1b. All IoT components, including but not limited to the IoT device, that are part of the IoT product.	Software Bill of Materials (SBOM) Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management
Documentation 1c. How the baseline product outcomes are met by the IoT product across its product components.	<i>On risk management:</i> ISO 31000 (Risk management — Guidelines) NIST SP 800-37 Rev. 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
Documentation 1d. Product design and support considerations related to the IoT product.	ISO/IEC 27036 (Cybersecurity — Supplier relationships) ISO/IEC 27034 (Information technology — Security techniques — Application security) ISO/IEC 5055 (Information technology — Software measurement — Software quality measurement — Automated source code quality measures) NIST Cybersecurity Supply Chain Risk Management (CSCRM)

Identified Standards for Documentation 1e-g



Cybersecurity Outcome	Potential References
Documentation 1e. Maintenance requirements for the IoT product.	ISO/IEC/IEEE 14764 (Software engineering — Software life cycle processes — Maintenance)
Documentation 1f. The secure system lifecycle policies and processes associated with the IoT product.	ISO/IEC 15288 (Systems and software engineering — System life cycle processes) ISO/IEC 12207 (Systems and software engineering — Software life cycle processes) ISO/IEC 15408 (Information security, cybersecurity and privacy protection — Evaluation criteria for IT security) ISO/IEC 27001 (Information security management systems — Requirements) ISO/IEC 27002 (Information security, cybersecurity and privacy protection — Information security controls) ISO/IEC 27005 (Information security, cybersecurity and privacy protection — Guidance on managing information security risks) NIST Secure Software Development Framework (SSDF) Cybersecurity and Infrastructure Security Agency (CISA)'s Secure by Design
Documentation 1g. The vulnerability management policies and processes associated with the IoT product.	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO/IEC 30111 (Information technology — Security techniques — Vulnerability handling processes)

Identified Standards for Information & Query Reception



Cybersecurity Outcome	Potential References
<p>Information and Query Reception 1a. The ability of the IoT product developer to identify a point of contact to receive maintenance and vulnerability information (e.g., bug reporting capabilities and bug bounty programs) from customers and others in the IoT product ecosystem (e.g., repair technician acting on behalf of the customer).</p>	<p>ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO 10004 (Quality management — Customer satisfaction — Guidelines for monitoring and measuring)</p>
<p>Information and Query Reception 1b. The ability of the IoT product developer to receive queries from and respond to customers and others in the IoT product ecosystem about the cybersecurity of the IoT product and/or its components.</p>	<p>ISO 10004 (Quality management — Customer satisfaction — Guidelines for monitoring and measuring) ISO/IEC 27035-1 (Information technology — Information security incident management — Part 1: Principles and process)</p>

Identified Standards for Information Dissemination 1



Cybersecurity Outcome	Potential References
Information Dissemination 1a. Updated terms of support (e.g., frequency of updates and mechanism(s) of application) and notice of availability and/or application of software updates.	[No standards currently identified]
Information Dissemination 1b. End of term of support or functionality for the IoT product.	ETSI 303-645 (Cyber Security for Consumer Internet of Things: Baseline Requirements): Provision 5.3-13
Information Dissemination 1c. Needed maintenance operations.	ISO/IEC/IEEE 14764 (Software engineering — Software life cycle processes — Maintenance)
Information Dissemination 1d. New IoT device vulnerabilities, associated details, and mitigation actions needed from the customer.	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO/IEC 27035-1 (Information technology — Information security incident management — Part 1: Principles and process)
Information Dissemination 1e. Breach discovery related to an IoT product and its product components used by the customers, associated details, and mitigation actions needed from the customer (if any).	ISO/IEC 29147 (Information technology — Security techniques — Vulnerability disclosure) ISO/IEC 27035-1 (Information technology — Information security incident management — Part 1: Principles and process)

Identified Standards for Information Dissemination 2



- Information Dissemination 2: The IoT product developer can distribute information relevant to cybersecurity of the IoT product and its product components to alert appropriate ecosystem entities (e.g., IoT product component manufactures and/or supporting entities, common vulnerability tracking authorities, accreditors and certifiers, third-party support and maintenance organizations) about cybersecurity relevant information.
 - This outcomes and its sub-outcomes will generally be guided by standards mapped to other outcomes (e.g., ISO/IEC 29147)

Identified Standards for Education & Awareness



- Five minimum criteria:
 - 1. The presence and use of IoT product cybersecurity capabilities.
 - 2. How to maintain the IoT product and its product components during its lifetime, including after the period of security support (e.g., delivery of software updates and patches) from the IoT product developer.
 - 3. How an IoT product and its product components can be securely reprovisioned or disposed of.
 - 4. Vulnerability management options (e.g., configuration and patch management and anti-malware) available for the IoT product or its product components that could be used by customers.
 - 5. Additional information customers can use to make informed purchasing decisions about the security of the IoT product (e.g., the duration and scope of product support via software upgrades and patches).
- Identified Standards:
 - [ISO/IEC/IEEE 26512](#) (Systems and software engineering - Requirements for acquirers and suppliers of information for users)
 - [ISO/IEC/IEEE 26514](#) (Systems and software engineering — Design and development of information for users)



Next Steps

NIST seeks specific feedback on:

1. Potential standards discussed throughout this essay that are appropriate to the IoT product components and cybersecurity outcomes they're paired with.
2. Gaps in the coverage by standards of particular IoT product components or cybersecurity outcomes and possible solutions for the gap(s).
3. Additional standards that can be used to inform requirements for IoT products, IoT product components, and cybersecurity outcomes.
4. Feasibility of applying multiple standards of different focus related to cybersecurity to reflect the total scope of the IoT product.

Plotting the path from here...

- Path forward from here still TBD
 - Feedback welcome!
- Goal is to provide additional information about ways the cybersecurity outcomes may be specifically defined
 - Standards are being utilized as a path, are there other possible paths?

THANK YOU

CONTACT US



[NIST.gov/cybersecurity](https://www.nist.gov/cybersecurity)



[@NISTcyber](https://twitter.com/NISTcyber)



NIST Cybersecurity for IoT
Program Home Page