NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST IoT for Cybersecurity Program and Contributions to Labeling

March 26, 2024

Are you building a securable connected product?

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Background on NIST ITL Mission: Cultivating Trust

NIST is the technical arm of the US Department of Commerce and a non-regulatory agency

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 Information Technology Labs mission is to cultivate trust in technology

In support of the above mission, NIST engages in both pre-standardization research as well as standards development

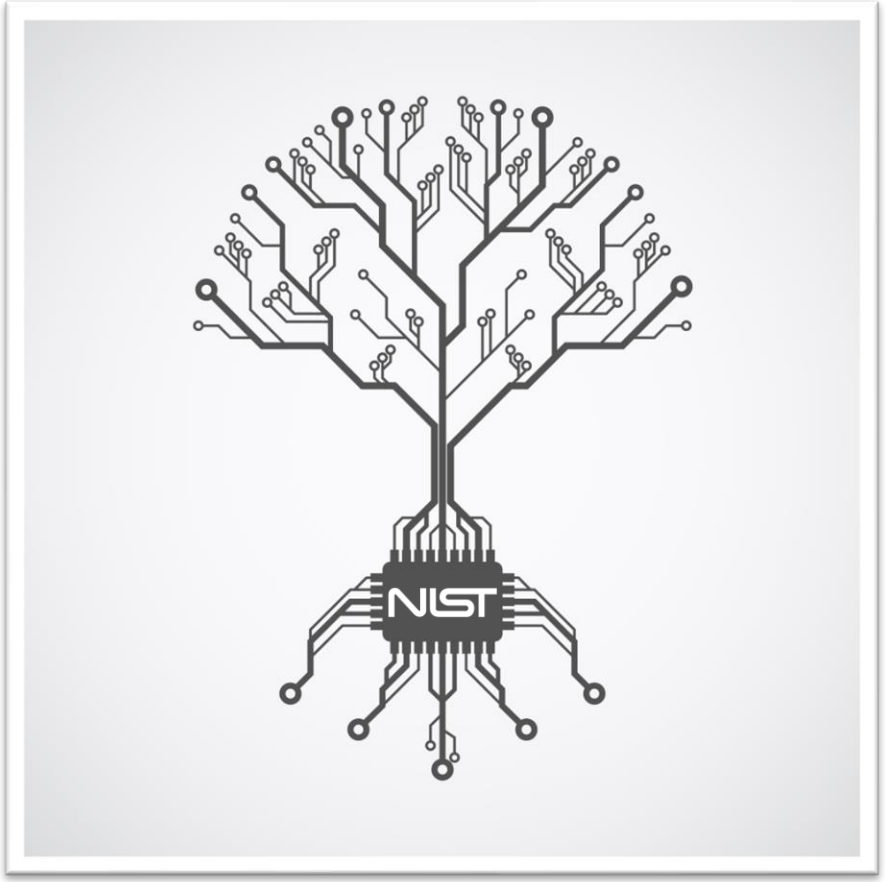


Photo credit: Shutterstock

Federal Drivers Toward Enhanced IoT Cybersecurity

EO 13800 (May 2017)

- Goal: dramatically reduce threats perpetrated by automated and distributed attacks (e.g., botnets)

Botnet Report (May 2018)

- Guide to government and private sector actions – 5 Goals
  - Path to sustainable, secure technology marketplace
  - Infrastructure innovation for dynamic adaptation
  - Network edge innovation for mitigation
  - Coalition approach, domestic & international
  - Increased awareness & education

Botnet Roadmap (Nov 2018)

- Five Lines of Effort:
  - IoT
  - Enterprise
  - Internet Infrastructure
  - Technology Development
  - Awareness & Education

Botnet Report Update (July 2020)

- Progress & Impact
- Looking Ahead

IoT Cybersecurity Improvement Act PL 116-207 (Dec 2020)

- Establishes mandate to define federal IoT cybersecurity requirements

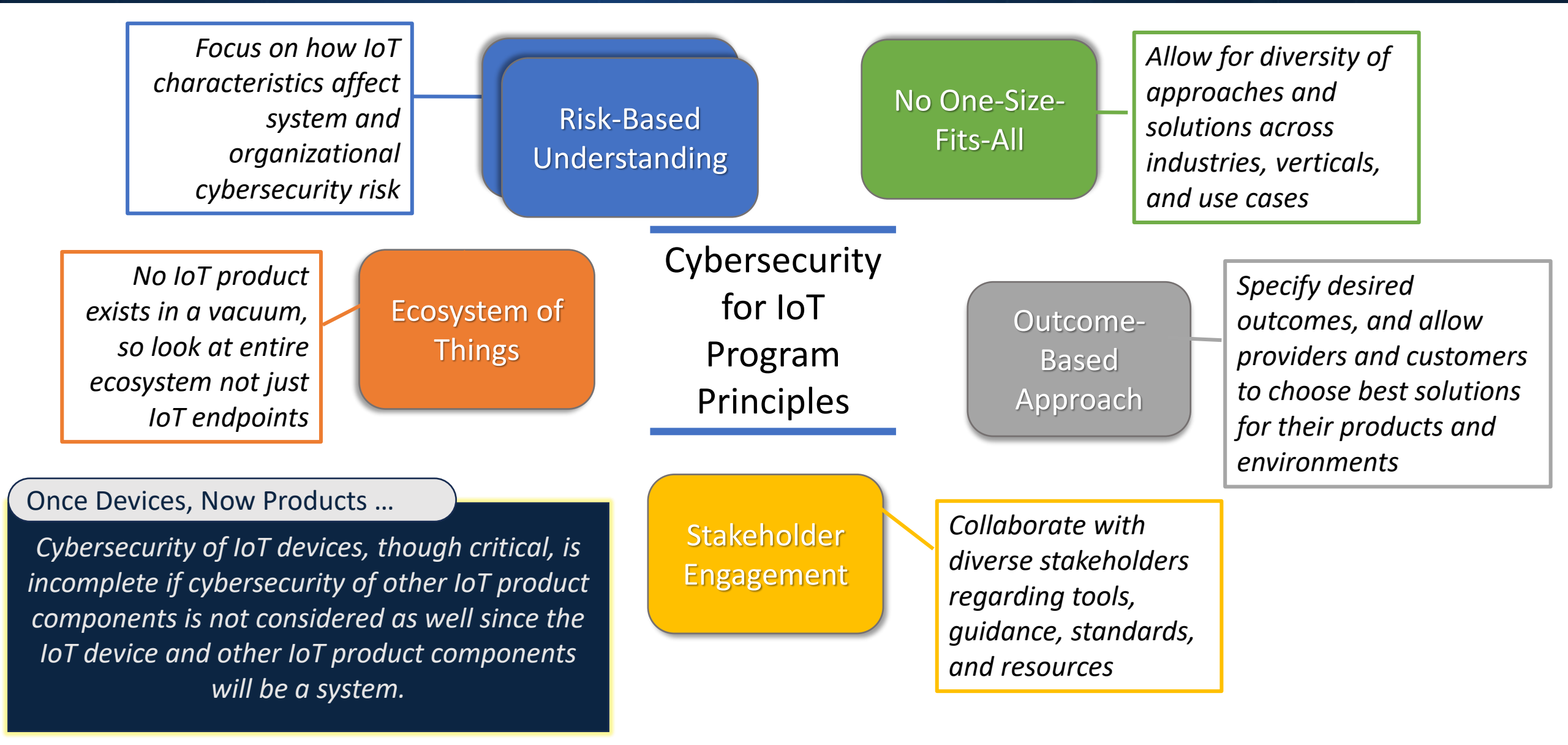
EO 14028 (May 2021)

- Title: Improving the Nation's Cybersecurity
- Included assignment for NIST to develop criteria for IoT consumer product cybersecurity labeling program

IoT Cyber Trust Mark Program (July 2023)

- Program lead: Federal Communications Commission
- Uses NIST IR 8425 criteria

Five principles guide how we approach solutions and program direction



The NIST IoT cybersecurity program engages in pre-standardization research across a number of areas

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

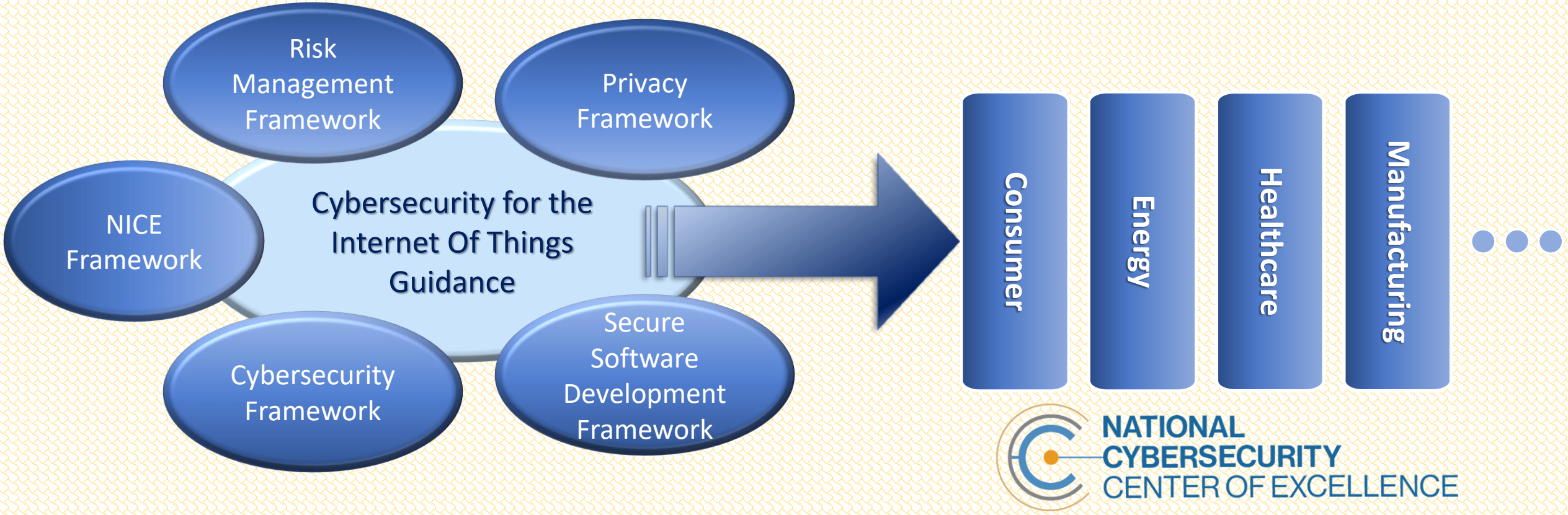
Applied

- 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

How do these guidelines get used?

- **Some cybersecurity guidelines are mandatory for federal agencies and their suppliers**
- **Often NIST will engage in standards development efforts to advance the results of our research within standards**
- **Some of our guidelines are adopted by regulators**
- **Much of our guidelines are voluntary for everyone else**

The Cybersecurity for IoT Program connects with and integrates guidance from other NIST efforts



There Are Many Participants In The IoT Ecosystem

Information Security Officers

Role: Manage security of business operations and infrastructure

Use NIST guidance as a framework to:

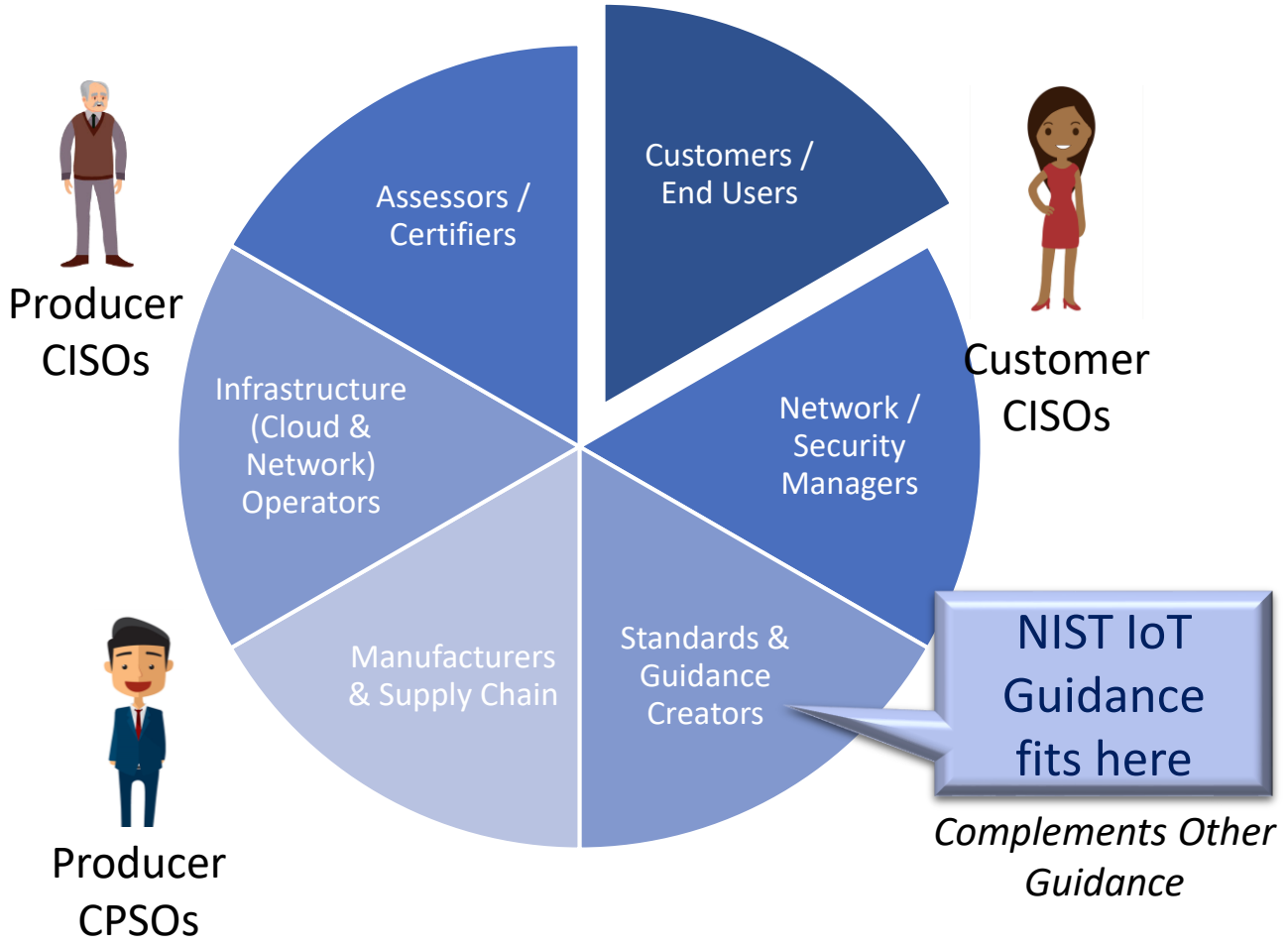
- Establish IoT procurement security requirements
- Evaluate risk implications of IoT product integration
- Identify additional or enhanced security control needs

Product Security Officers

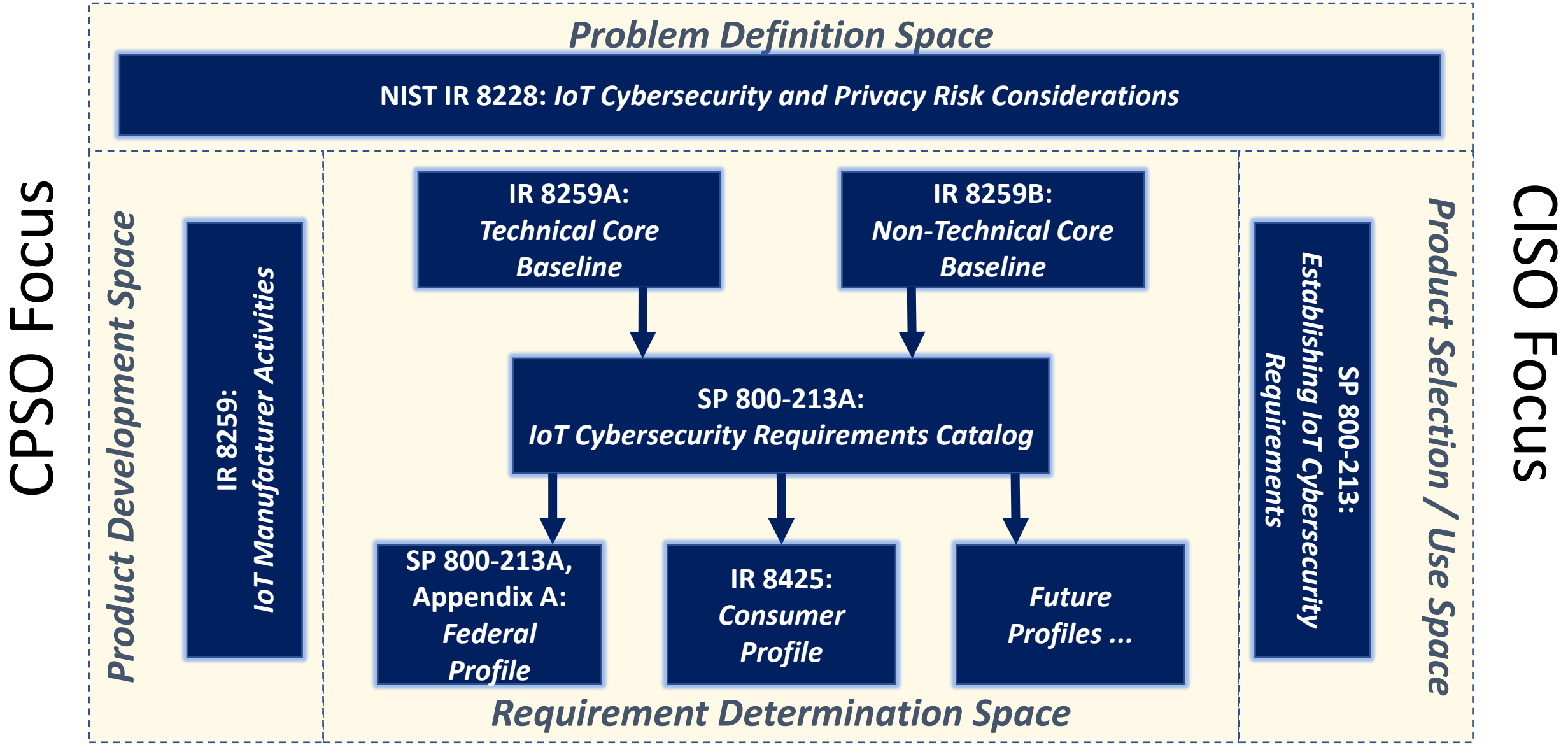
Role: Guide vendor development of securable IoT devices & products

Use NIST guidance as a framework to:

- Evaluate customer use cases and security risks
- Determine required product technical capabilities
- Select applicable industry & international standards
- Scope product support infrastructures and activities
- Establish sound, security-informed development processes



A 50K Foot View of NIST's IoT Cybersecurity Guidance



May 2021 E.O. directed NIST to identify IoT Cybersecurity criteria and pilot labeling approach

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply

Criteria

- *What criteria are products assessed against?*

Label

- *What should the label look like and what should it contain?*

Conformity

- *How is conformity with criteria demonstrated?*

To build out the criteria NIST looked to build on the existing non-sector specific IoT product security baselines and guidance

Program Inception: (2017)

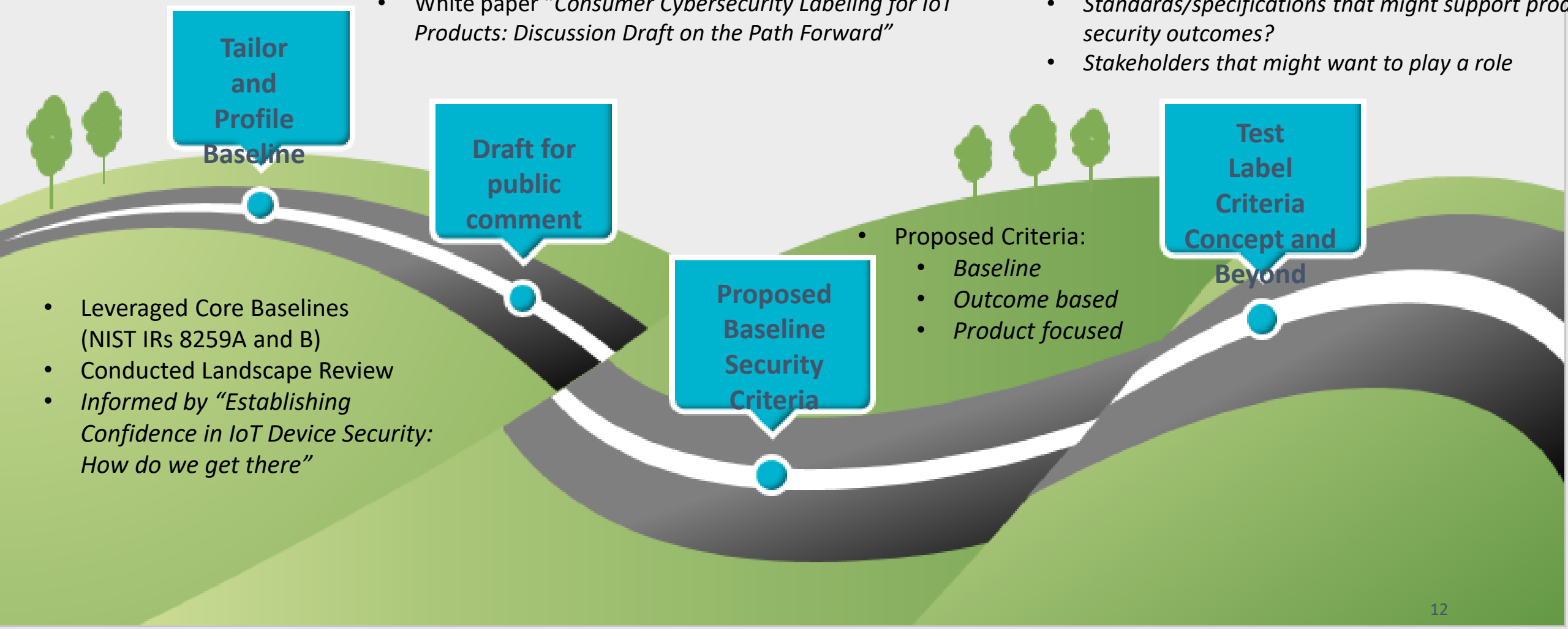
Cybersecurity guidance for adopters of IoT technology (2019)

Cybersecurity guidance for manufacturers of IoT products (May 2020)

Adapting guidance to specific product use case/sectors (Nov 2021)

- Considerations for organizations adopting IoT technology towards managing Cybersecurity and Privacy Risks (NIST IR 8228)
- Foundational Cybersecurity Activities for IoT Device Manufacturers (IR 8259)
  - IoT Device Cybersecurity Capability Core Baseline (IR 8259A)
  - IoT Non-Technical Support Capability Core Baseline (IR 8259B)
- SP 800-213 – IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements (Nov 2021)
  - SP 800-213A – IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog / Federal Profile (Nov 2021)

Roadmap to criteria for IoT product cybersecurity label



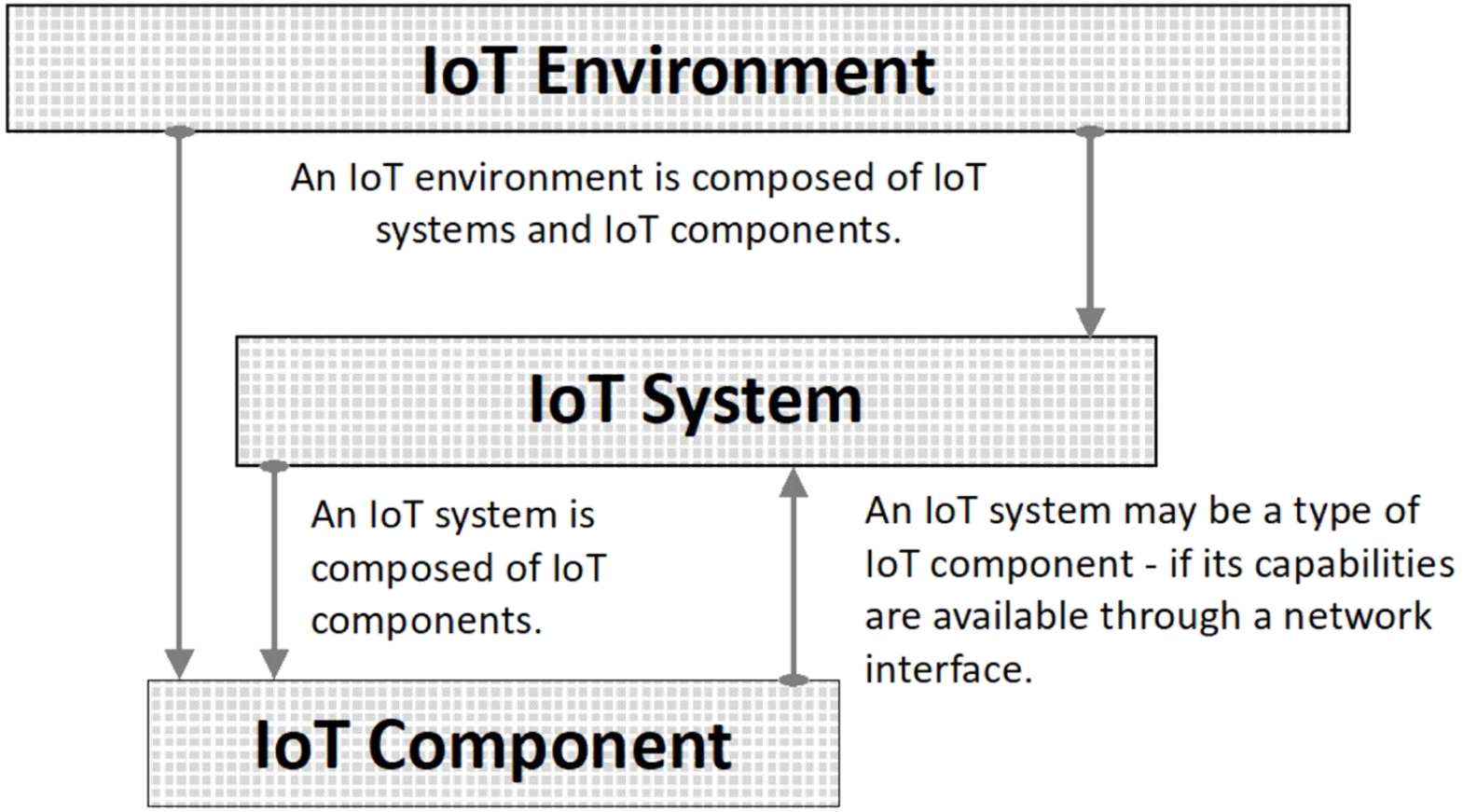
- Leveraged Core Baselines (NIST IRs 8259A and B)
- Conducted Landscape Review
- *Informed by "Establishing Confidence in IoT Device Security: How do we get there"*

- *"Draft Baseline Security Criteria for Consumer IoT Devices"*
- Public workshops/comments/roundtables
- White paper "*Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward*"

- Proposed Criteria:
  - *Baseline*
  - *Outcome based*
  - *Product focused*

- Test drive the criteria:
- *What are the existing programs that relate?*
- *Standards/specifications that might support prod security outcomes?*
- *Stakeholders that might want to play a role*

IoT Product Are Systems and Components Of Systems

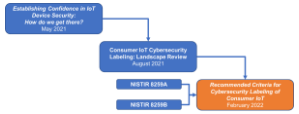


Product components include:

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

From: *Internet of Things (IoT) Component Capability Model for Research Testbed*, NISTIR 8316

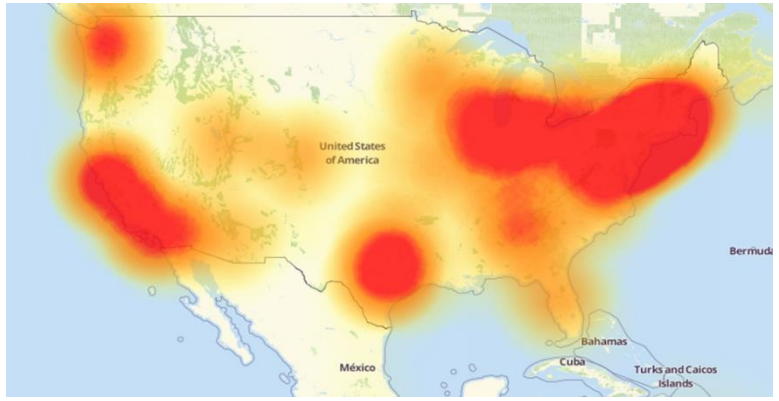
Consumer IoT Product Scope



- Consumers buy products and do not distinguish the device's cybersecurity from that of the other product components
- For Consumer IoT broadened scope to IoT Products, which include at least one (possibly multiple) IoT Device, plus:
  - Specialty networking/gateway hardware (e.g., a hub within the system where the IoT device is used).
  - Companion application software (e.g., a mobile app for communicating with the IoT device).
  - Backends (e.g., a cloud service, or multiple services, that may store, process data and/or provide functionality from the IoT device).

Proposed Baseline IoT Product Criteria Informed by Real-world Incidents

Unauthorized access to data and views of the inside and outside of buildings occurred with multiple brands of security cameras.



Use of weak authentication to enable the loading of malware onto the device and use that device in DDOS and other attacks.

Unauthorized individuals exploiting weak authentication to access data and microphones in baby monitors in multiple brands. In some cases, product developers failed to respond to vulnerability reports.

Proposed Baseline IoT Product Criteria Informed by Real-world Incidents

Fitness tracker location data for military personnel was publicly posted even when product was configured for privacy.

Unauthorized access to the fish tank thermometer enabled hackers to reach sensitive database and exfiltrate data.

Secondhand IoT devices can put previous owners at risk.

Technical requirements establish connected product securability

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

NIST IR 8425

Supporting requirements ensure users are supported

 **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

Focus on Outcomes in Criteria

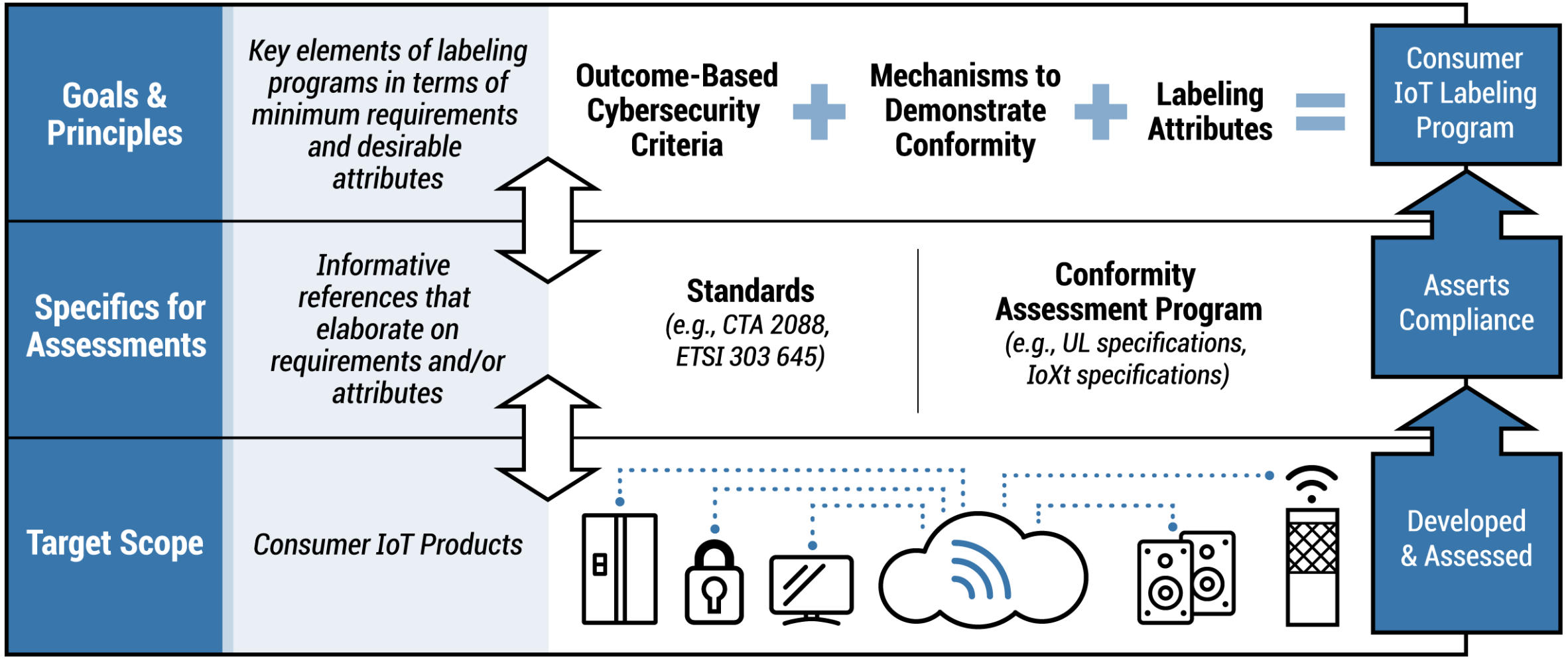
Flexibility in meeting the criteria to support different approaches to cybersecurity

Allows for a vibrant IoT product conformity and labeling landscape

Easy adaptability as technologies and risks change over time

Outcomes speak to the risks they are intended to mitigate

Desired outcome approach can allow for flexibility in how outcomes are achieved but requires governance



Results from piloted concept as well as observations were summarized in the final report

- About 20 responses were received and reviewed
- Overall we observed from the effort:
  - Support for product focus, however: recognition that will present some challenges in actual execution
  - Support for outcome-based, but recognition that it will require governance to ensure consistency
  - Varied responses with respect to the role of government, ranging from need to undertake public awareness, enforcement, incentives through potential liability protections and potential governance
  - Unclear whether the drivers are there to change market behavior through labeling

In the final report under the E.O. NIST provided a number of recommendations for the strategy going forward

- Consistent layered label design
- Consumer education critical but large undertaking and investment
- Flexibility for wide range of products
- Multiple scheme owners / third party authority to coordinate across
- Liability considerations and incentives
- Outcome-based criteria, updated over time as threat landscape evolves
- Robust marketplace of standards to support assessment
- International considerations and mutual recognition
- Include both 3rd part certification and self attestation

In July of 2023 the White House held a launch event announcing that the FCC would operate the US Cyber Trust Mark

In August 2023 the FCC released a notice of proposed rulemaking (NPRM) announcing their intent to use the NIST criteria in a Cyber Trust Mark program and inviting feedback.

In February, 2024 the FCC released a Report and Order (R&O) on the proposed operation of the Cyber Trust Mark including basing it on the NIST criteria and definition of IoT products.

On March 14, 2024 the FCC adopted the R&O and is moving forward on the Cyber Trust Mark program

Our Partner: National Cybersecurity Center of Excellence (NCCoE)

- NIST created NCCoE to provide a collaborative hub for industry, government, academia, and others.
- Example NCCoE projects address IoT Cybersecurity
  - 5G - show how the components of 5G architectures can securely mitigate risks and meet industry sectors' compliance requirements for several 5G use case scenarios
  - Securing the Industrial Internet of Things (IIoT) with the goal of documenting an approach for improving the overall security of IIoT in a distributed energy resources (DER) environment

NCCoE Focuses On Applied Solutions

DEFINE + ARTICULATE Describe the business problem	ORGANIZE + ENGAGE Partner with innovators	IMPLEMENT + TEST Build a usable solution	TRANSFER + LEARN Help people adopt a solution
ACTION	ACTION	ACTION	ACTION
Identify and describe business problem	Publish project use cases and solicit responses	Build solution	Collect Solution documents
Conduct market research	Select partners and collaborators	Test solution	Tech transfer
Vet project and use case descriptions	Sign CRADA	Identify solution gaps	Document lessons learned and archive
OUTCOME	OUTCOME	OUTCOME	OUTCOME
Well-defined business problems and project descriptions, refined through specific use cases	Collaboration with partners from industry, government, academia and the IT community to design solutions	Practical, usable, repeatable and secure solution that addresses the business problem	Set of all material necessary to implement and easily adopt the secure solution

References: IoT Cybersecurity Program

NIST Cybersecurity for IoT Program
https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

NIST Cybersecurity for IoT Program Publications
https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/publications

IoT projects at NIST's National Cybersecurity Center of Excellence
https://www.nccoe.nist.gov/iot