ETSI
The Standards People

Security Conference

Small “s” Standards: NIST’s Role In IoT Cybersecurity

Presented by: Katerina Megas, NIST

17/10/2023

Small “s” Standards: NIST’s Role In IoT Cybersecurity

Katerina Megas, NIST

17 October2023

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

Background on NIST ITL Mission: Cultivating Trust

NIST is the technical arm of the US 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 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

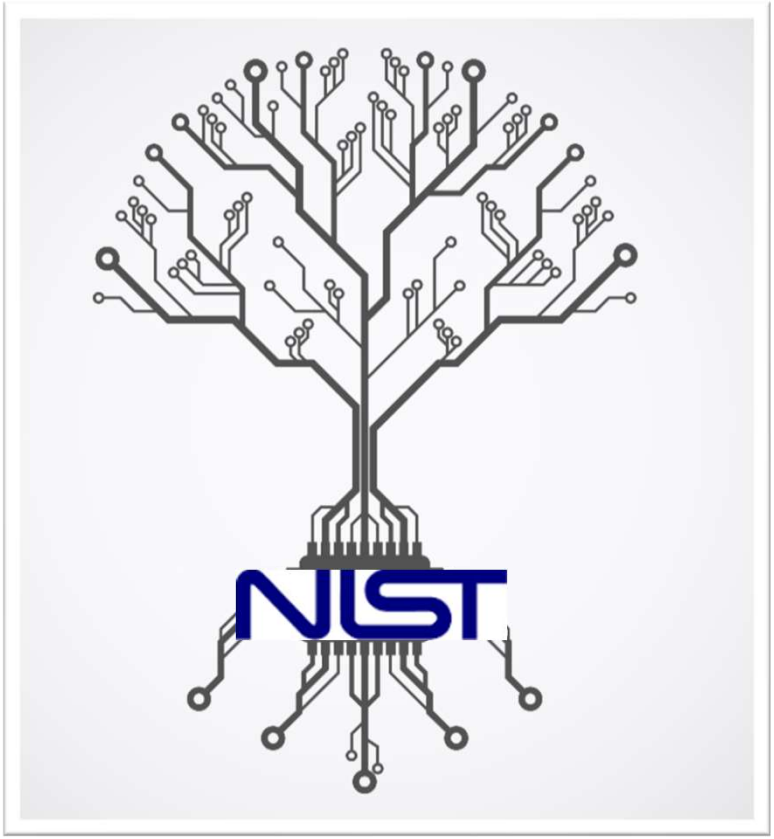


Photo credit: Shutterstock

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**

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

Much of the NIST pre-standardization research informs our standards engagement

Why We Engage In Standards:

- NIST and the USG play many roles in the standards ecosystem: User, Specifier, Participant, Facilitator, Advocate, Technical Advisor/Leader, Convener, Provides Funding
- Our Engagement Supports Regulation, Procurement And Policy Activities, and Incorporates into Voluntary Programs

- **The Background on policy drivers:**
  - National Technology Transfer and Advancement Act (NTTAA) - 1996
  - OMB Circular A-119 – Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities – 2016
  - Trade Agreements Act of 1979 & WTO Technical Barriers to Trade Agreement

Clear policy guidance for Federal Agencies to:

- Participate in voluntary consensus standards development
- Use voluntary consensus standards and consider other standards in lieu of Government developed standards.
- Consider reasonable availability of standards
- Consider private sector conformity assessment mechanisms
- Be aware of international obligations in choosing standards and conformity assessment.

A recent example of NIST research work in IoT Cybersecurity was under Executive Order 14028 signed by President Biden

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

NIST was directed to pilot a cybersecurity label for consumer IoT products:

Criteria

- *What criteria are products assessed against?*

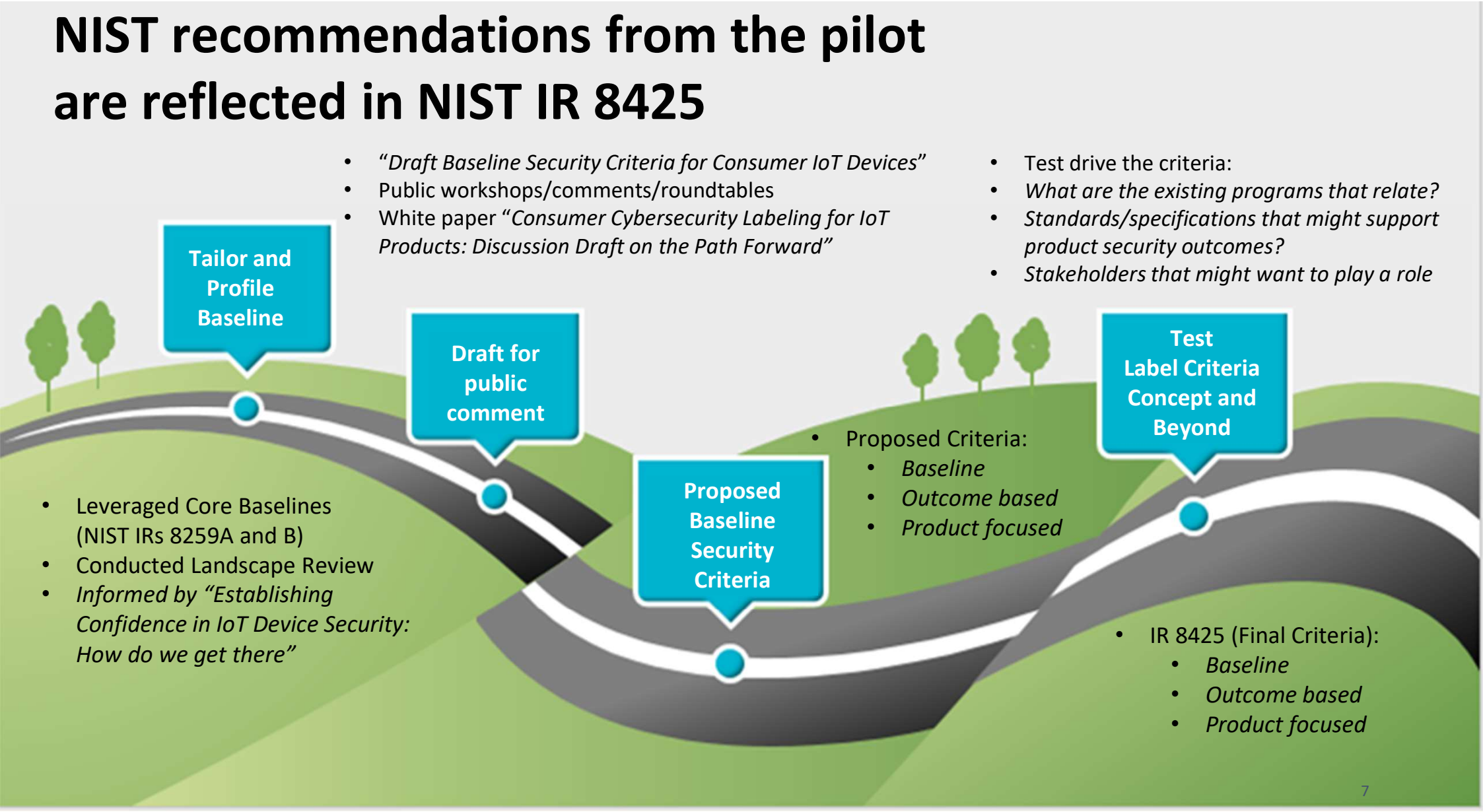
Label

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

Conformity

- *How is conformity with criteria demonstrated?*

NIST recommendations from the pilot are reflected in NIST IR 8425



These 10 cybersecurity outcomes and 65 sub-outcomes aim to identify a ‘good’ set of minimum criteria for IoT products

NIST

Asset Identification

Product Configuration

Data Protection

Interface Access Control

Software Update

Cybersecurity State Awareness

Documentation

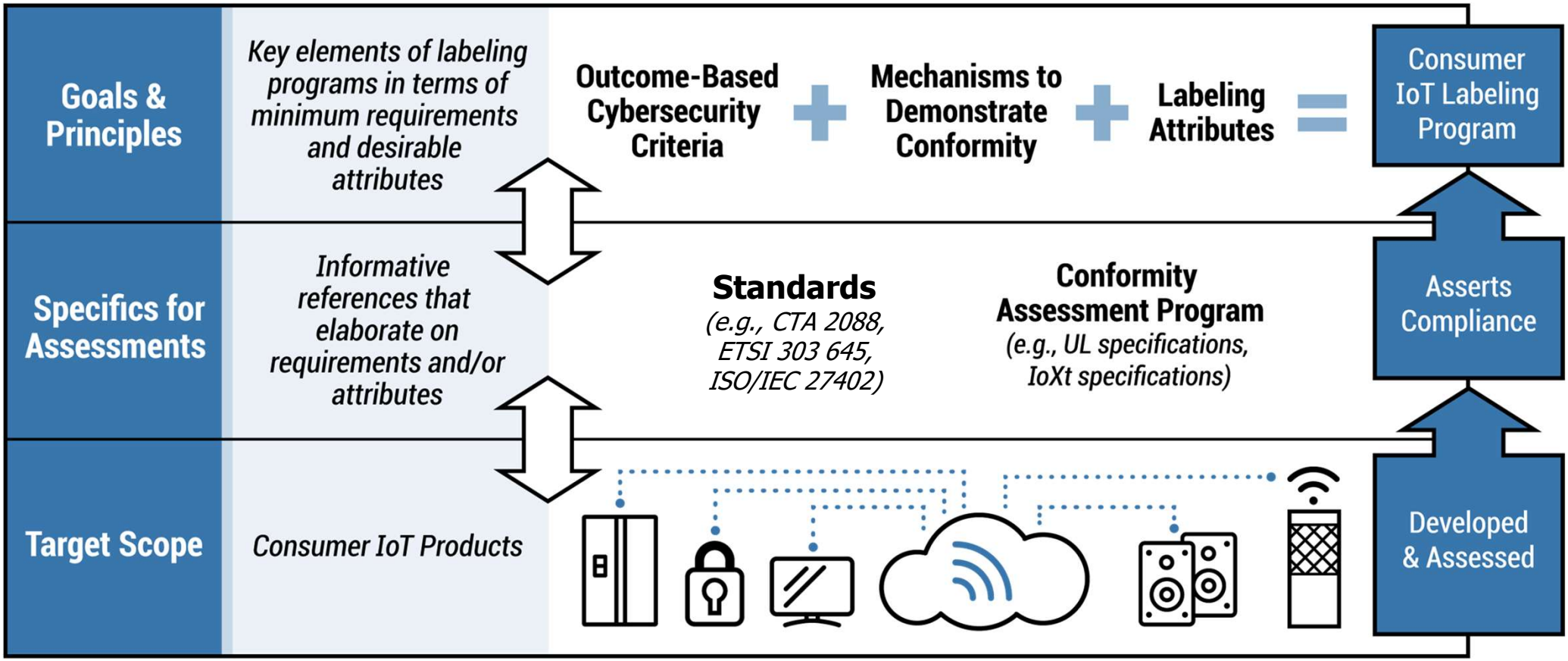
Information & Query Reception

Information Dissemination

Product Education & Awareness

NIST IR 8425

The NIST product cybersecurity criteria in 8425 aim to identify the desired outcomes and rely on standards to identify the 'how'



In addition to the 10 criteria NIST delivered a report to the APNSA with a number of recommendations for the strategy going forward

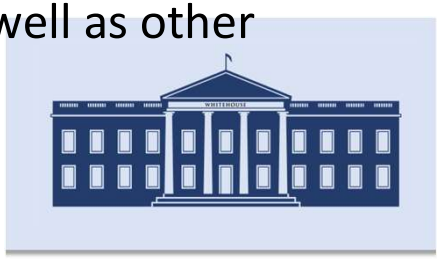
- Consistent layered label design
- Consumer education critical but large undertaking and investment
- Flexibility for wide range of products
- Multiple scheme owners / third party authority to coordinate across
- Liability considerations and incentives
- Outcome-based criteria, updated over time as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

Report for the APNSA on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software (May 10, 2022)

Examples of how NIST publications such as 8425 get put into practice

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

- In August the FCC released a notice of proposed rulemaking (NPRM) announcing their intent to use the NIST criteria, but inviting feedback on the criteria as well as other considerations such as:
  - does the definition they propose work?
  - could this program also be extended to include industrial devices?
  - understanding that the scope of the FCC authorizations might be device focused, would a more product view as proposed by NIST address better the needs of the final consumer?



- California IoT Security Law (SB-327) Amended: Effective January 1, 2023, connected device manufacturers may elect to comply with existing reasonable security features requirements by satisfying the criteria of a labeling scheme that conforms with National Institute of Standards and Technology (NIST) criteria

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

THANK YOU

CONTACT US

NIST.gov/cybersecurity

@NISTcyber

NIST Cybersecurity for IoT Program Home Page