IoT Cybersecurity: Strategies, Laws, Guidance, Labels, and some Working Group updates too…

Kat Megas, NIST

12 September2023

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

The National Cybersecurity Strategy released in March advances both Federal as well as non-Federal IoT cybersecurity

Strategic Objective 3.2: Drive the Development of Secure IoT Devices

The Administration will continue to improve IoT cybersecurity through Federal research and development (R&D), procurement, and risk management efforts, as directed in the IoT Cybersecurity Improvement Act of 2020. In addition, the Administration will continue to advance the development of IoT security labeling programs, as directed under EO 14028, "Improving the Nation's Cybersecurity." Through the expansion of IoT security labels, consumers will be able to compare the cybersecurity protections offered by different IoT products, thus creating a market incentive for greater security across the entire IoT ecosystem.

– National Cybersecurity Strategy, March 2023

P.L. 116-207 IoT Cybersecurity Improvement Act of 2020 established minimum requirements for Federal Agencies

- Requires NIST to publish standards and guidelines on the use and management of IoT devices by the federal government
- NIST must publish minimum information security requirements for managing cybersecurity risks associated with IoT devices including
    - (i) Secure Development.
    - (ii) Identity management
    - (iii) Patching.
    - (iv) Configuration management.
- Federal agency procurement of IoT devices will have to comply with NIST guidelines
- Require NIST to publish guidelines for reporting security vulnerabilities relating to federal agency information systems, including IoT devices.
- Require contractors providing IoT devices to the U.S. government to adopt coordinated vulnerability disclosure policies, so that if a vulnerability is uncovered, that information is disseminated.

These requirements for Federal Agencies went into force in December 2022

Federal agencies must use NIST publications 800-213 and 800-213A when procuring IoT as of December 2022

OMB Memo -23-03 Specifies that the agency CIO must review and approve all contracts and “if the CIO conducts such a review of a contract for an IoT device, and determines during that review that using the device would prevent the agency from complying with NIST’s IoT standards and guidelines, then the agency is prohibited from using the device, procuring or obtaining the device, or renewing a contract to procure or obtain the device.

SP 800-213:
Determining Requirements

- Relationship to Risk Management Framework Process
- Evaluating IoT Device Risk
- Selecting Requirements

SP 800-213A:
Capabilities Catalog

- Builds from NISTIR 8259A/B Baselines
- Detailed Technical & Supporting Capabilities
- Incorporates Federal Profile

- 11 Capabilities
- 53 Associated Sub-Capabilities

The Device Cybersecurity Capability Catalog Categories covers 11 areas technical and non-technical

- Device Identification (DI)
- Device Configuration (DC)
- Data Protection (DP)
- Logical Access to Interfaces (LA)
- Software Update (SU)
- Cybersecurity State Awareness (CS)
- Device Security (DS)
- Documentation (DO)
- Information & Query Reception (IQ)
- Information Dissemination (ID)
- Education & Awareness (EA)

The documentation category in SP 800-213 includes a number of requirements related to supply chain

- Generally the requirements in Capability DO (Documentation) require that the manufacturer have documented their policies and processes ranging from secure software development to vulnerability management.
- The baseline requirement in subcapabilty DO-13. are requirements for the manufacturer of IoT products for the US Federal Government Market
- *Establish communications that describes the manufacturer's third party, contractor, and vendor IoT device security oversight, and for including security and privacy requirements within contractual agreements. Information that may be necessary to provide to explain supply chain risk management include details and actions.*
- *Sections DO-13.a thought DO-13.f describe what minimum information should be included*

E.O. 14028 directed NIST to pilot a Consumer IoT Cybersecurity Label

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?*

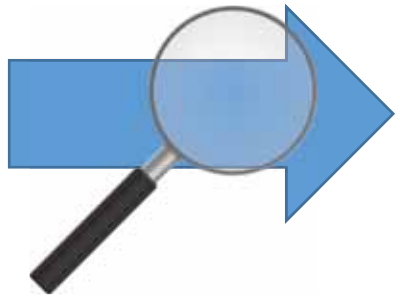
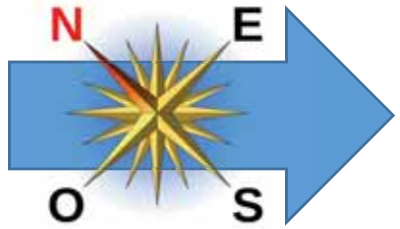
Label

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

Conformity

- *How is conformity with criteria demonstrated?*

For the criteria that would underpin the cybersecurity label, NIST made two major shifts from the core cybersecurity baselines

Focus	Device		Product
Orientation	Defined Cybersecurity Capabilities		Identifies Cybersecurity Outcomes

Asset Identification / Product Configuration / Data Protection / Interface Access Control / Software Update / Cybersecurity State Awareness

Documentation / Information and Query Reception / Information Dissemination / Product Education and Awareness

NIST IR 8425 publishes the NIST recommendations for minimum cybersecurity outcomes for IoT products as part of the labeling program

Profile of the IoT Core Baseline for Consumer IoT Products (September 2022)

- Defines Consumer IoT product scope:

Product Definition

  - IoT Device(s), plus any mix of:
  - Specialty hardware (e.g., gateway)
  - Companion applications (e.g., mobile app)
  - Backend support (e.g., cloud services)

- Profiles IR 8259A/B Core Baselines
- Provides supporting information regarding source materials, common IoT vulnerabilities, insights & takeaways from profiling process


NIST Internal Report
NIST IR 8425

Profile of the IoT Core Baseline for Consumer IoT Products

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425

September 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

In the report to the APNSA 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 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?

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

The NDAA'21 Directed the Secretary of Commerce to deliver a Report to Congress on IoT adoption

The NDAA 2021 directed the Secretary of Commerce to stand up an IoT interagency group and an advisory board consisting of non-governmental stakeholders recognizing that the Internet of Things will—

(A) be vital in furthering innovation and the development of emerging technologies; and

(B) play a key role in developing artificial intelligence and advanced computing capabilities;

- The scope of the Report to Congress covers use of IoT across almost every market sector, including healthcare, agriculture, transportation, logistics and many others

Supply Chain is a theme that is heard in many discussions of the IoT AB and will likely result in recommendations for actions that the USG should take to enable IoT adoption:

- IoT enabled logistics in a key use case identified that can bring significant benefits to the US economy
- Ensuring that the US has a resilient and secure supply chain to support IoT manufacturers
- In addition they identify opportunities to:

Digitize product data across the supply chain to be able to answer questions:

How is the product made: Implement digital threads to trace products from chip design through manufacturing of components and assembly

What does the product consist of: Implement infrastructure for traceable HBOM, SBOM and DBOM

Where is the product (or components of the product during production): Leverage IoT and analytics and track assets across the supply chain

Comments on the public draft of the FACA and Federal Working Group update are welcome!!i

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

THANK YOU

CONTACT US

NIST.gov/cybersecurity

@NISTcyber