A U.S. Perspective on IoT security certification activities

Katerina Megas, NIST Cybersecurity for IoT Program Manager

About the NIST Cybersecurity for IoT Program

NIST's Cybersecurity for IoT Program develops & applies standards, guidelines, and related tools to **improve the cybersecurity of connected devices and the environments in which they are deployed**.

By **collaborating with stakeholders** across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables **innovation on a global scale**.

Introduction to managing IoT cybersecurity and privacy risk in Federal Systems

NIST is preparing a document on **managing IoT security and privacy risks for federal systems**. This effort is aimed at considering a practical approach to IoT security and privacy risk management.

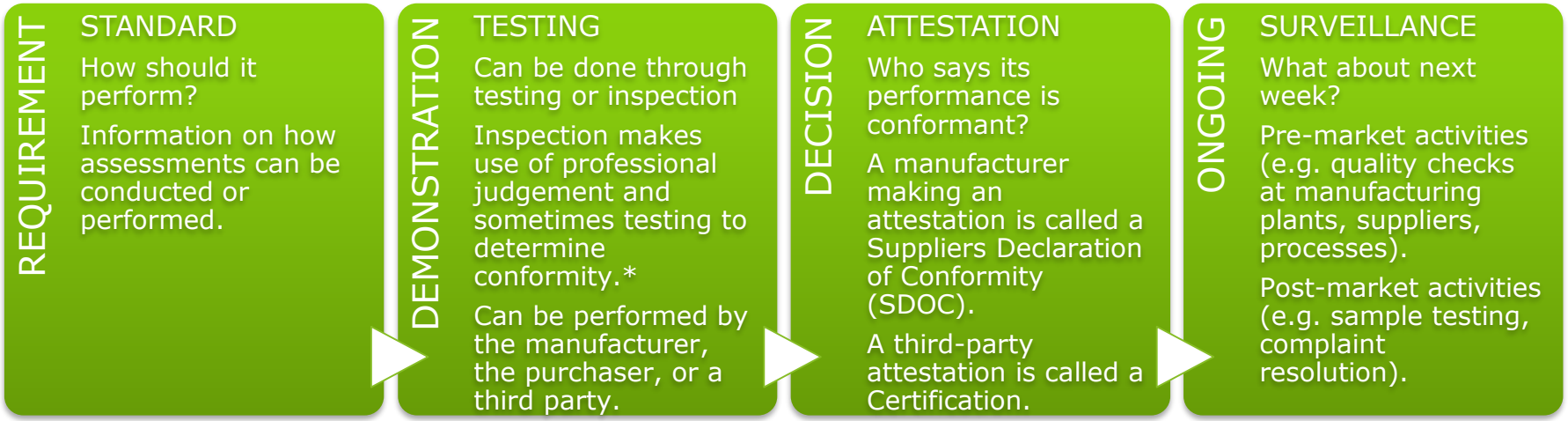
Next steps

- Attending roundtables to gather industry feedback throughout the development process.
- Collecting input on discussion draft at iotsecurity@nist.gov

Conformity comprises a range of methods: from self-declaration to third party certification

Conformity assessment is the **demonstration** that specified **requirements** relating to a product, process, system person or body are **fulfilled**.*

Conformity assessments can include a broad range of assessment methods based on agreed-upon industry practices and standards.



ISO/IEC 17000 Conformity assessment – Vocabulary and general principles

Conformity assessment design based on risk

Consider risks associated with non-compliance when determining the necessary rigor of a system.

- Over-design can be costly and may delay products to market.
- Under-design reduces confidence and may prevent market acceptance of the product.

Marketplace consequences, regulatory penalties and effective recall processes may be considered in determining needed level of rigor in conformity assessment systems.

Conformity assessment in the US is different than elsewhere

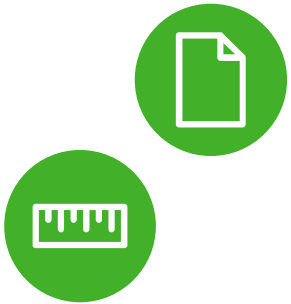
- There is no national-level coordinating organization.
- Multiple accreditation bodies, differing in size and scope.
- Sector-developed approaches.
- Overlaps in coverage.
- Conformity assessment programs are tailored to meet specific private and public sector needs.

This results in:

- Opportunity for effective, cost-efficient conformity assessment programs.

White House Office of Management and Budget Circular A-119 provides guidance to agencies

- Using private sector conformity assessment mechanisms.
- Considering international obligations in using standards and conformity assessment.
- Preference for leveraging existing voluntary consensus standards over creating unique government standards.
- A-119 also permits agencies to consider other types of standards (e.g., market or sector) to meet the agency's missions and priorities.



Challenges for certification of cybersecurity and IoT

- IoT comprises a very broad range of devices and systems for use by consumers, businesses, and public entities. As such, there is a large range of risk profiles and challenges to address.
  - There is no single set of stakeholders requiring certification, therefore the financial incentives around certification are difficult to codify.
  - The liability for configuring, implementing, and updating IoT devices is diverse – so there is not a "penalty" for lack of certification.
- The range of IoT device types means the prototypical basis definitions for systems are hard, making it difficult to define a target of evaluation for a certification scheme. There would be a lot of different ways to define the "testable widget."
  - Diverse set of considerations by sector, such as automotive, medical, consumer, industrial, public buildings, etc.
  - Devices are often used beyond their intended purpose, creating a challenge to consensus-based standards as these uses are often unforeseen.

Challenges for certification of cybersecurity and IoT, continued

- Some devices are frequently updated – often without notification - and each may introduce new risks or considerations.
  - This makes standardization and assessments difficult, especially as conformity is considered as point-in-time.
- Some IoT devices, such as medical devices, operate as part of an ecosystem and cannot be removed from the environment without negatively impacting other vital parts of the system.
  - Certification of individual devices outside of their operating environment does not necessarily achieve desired risk mitigation effect. Certifying them within the operating environment is typically not viable.
- Challenge of where the certification badges would go.
  - For example, energy efficiency is an attribute of the washer/dryer. How would someone know that there is an IoT device in their fridge? How would it be displayed? How would it be revoked if updated?
- Difficulties in communicating the meaning of conformance. How secure is secure? What is sufficient for the purpose?
  - Does conformity necessarily mean security?
  - Challenge of whether consumers understand and value conformance

Possible approaches to IoT conformity assessments

- Different assessments can be created based on device type and function.
- Industry can lead on best practices for creating necessary requirements and assessment approaches.
- Can design assessments to enable the flexibility needed to meet market demand.
- Leverage different conformity assessment approaches (e.g,. self-attestation, third party attestation) based on risk associated with device type or environment.
- Focus on the capabilities, not the use.

Understanding the current standards landscape that might support conformance testing

The Interagency International Cybersecurity Standardization Working Group (IICS WG)

- NIST co-chaired an IoT Task Group stood up under the IICS WG, coordinating with 13 agencies on a report todetermine the present state of international cybersecurity standards development for IoT.
- The Draft NISTIR 8200 is now online at https://csrc.nist.gov/publications/detail/nistir/8200/draft. There is a 60 day comment period.
- Private industry input is key to providing a more complete view of the current state of IoT standards, especially in areas such as industry adoption or implementation barriers.

Preliminary Takeways:

- One size likely does not fit all. We anticipate that IoT will need a variety of standards, and public input is needed to complete the inventory.
- No single comprehensive unifying standard for IoT Cybersecurity but many areas of specialized focus.

There remains a need for incentives for certification and improved security

As *A Report to the President on Enhancing Resilience Against Botnets* points out, market incentives are misaligned.

- "Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products."

Draft US legislation *The Internet of Things (IoT) Cybersecurity Improvement Act of 2017* proposes minimum security requirements for IoT devices purchased by US government.

- Would require IoT vendors selling to agencies ensure that devices can be patched.
- Calls for vendors to ensure that software used for communications, encryption, and other critical functions are supported by the software vendor.
- Creates standard vulnerability disclosure polices for federal contractors.

The draft has a provision that agencies waive the requirements if "Industry develops third-party device certification standards that provide equivalent, or more rigorous, device security requirements (as determined by NIST)"*

***https://www.warner.senate.gov/public/index.cfm/2017/8/senators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices**

Example industry efforts to assess cybersecurity in IoT devices

Underwriter's Laboratory (UL) is conducting conformity assessment on the cybersecurity of IoT devices.

Consumer Reports is evaluating products and services for their privacy and data security.

Open Connectivity Foundation's certification program includes conformance testing to ensure secure connectivity.

ICSA Labs, a division of Verizon, has introduced an IoT security testing Program.

Red Alert Labs provides cybersecurity consulting and evaluation services to organizations deploying IoT devices.

Contact – NIST wants to hear from you!

#IoTSecurityNIST

iotsecurity@nist.gov

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Attributes of a Voluntary Consensus Process

A-119 focuses on the PROCESS used to develop the standard.

Standards developed in a process that does not include all of these attributes are referred to merely as other standards.