# Establishing Confidence in IoT Device Security:

## *How do we get there?*

Katerina N. Megas
Barbara Cuthill
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Sarbari Gupta
*Electrosoft Services, Inc.*
*Reston, VA*

May 14, 2021

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.05142021-draft



National Institute of Standards and Technology
U.S. Department of Commerce

## Abstract

NIST conducted a review of the available alternative approaches for providing confidence in the cybersecurity of Internet of Things (IoT) devices in November 2020 through January 2021, conducting interviews with government and private sector organizations who are experts on these approaches. This white paper describes the available landscape of approaches and draws out themes commonly heard during the interviews.

## Keywords

conformance testing; cybersecurity; Internet of Things; labelling

## Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

## Additional Information

Information on this topic is available on the NIST Cybersecurity for IoT Program homepage. For additional information on NIST's Cybersecurity programs, projects and publications, visit the Computer Security Resource Center. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is also available.

## Public Comment Period: *May 14, 2021 through June 14, 2021*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: iotsec@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

## Note to Reviewers

The purpose of this draft essay is to start a conversation about what it means to have confidence in the cybersecurity of IoT devices used by individuals and organizations and the various ways of gaining that confidence. This essay describes the landscape of confidence mechanisms that are currently available for establishing the security of IoT devices in the marketplace. In preparing this essay, NIST conducted extensive research on initiatives that can help to instill confidence in IoT device security and held a series of meetings with government and industry experts to glean information on the unique aspects and challenges in this space.

NIST seeks comments on this essay and on the topic of confidence mechanisms including comments addressing the following questions:

- While the landscape review wasn't meant to be exhaustive, are there other significant confidence mechanisms that we should include?
- Have we correctly characterized the different mechanisms for providing confidence in the security of IoT products?
- We identified seven themes that emerged from our interviews. Are there other considerations that we missed?

Please provide comments by June 14, 2021 to iotsec@nist.gov with the subject line *IoT Confidence Mechanism Comments.*

## Table of Contents

**1 Introduction ..... 1**
1.1 Background and Purpose ..... 1
1.2 Scope ..... 2
1.3 Intended Audience ..... 3
1.4 Organization ..... 3
**2 Security of IoT Devices ..... 4**
**3 Confidence Mechanisms for IoT Device Security ..... 5**
3.1 Sources of Confidence ..... 5
3.2 Framework for Customer Confidence ..... 6
3.3 Benefits of Confidence in IoT Device Security ..... 7
**4 Landscape of Non-Regulatory Confidence Mechanisms ..... 8**
4.1 Consumer Advocacy Groups ..... 8
4.2 Industry Consortia (Trade Associations and Business Advocacy Groups) ..... 8
4.3 Third Party Confidence Mechanisms ..... 9
**5 Landscape of Policy-Based Confidence Mechanisms ..... 10**
5.1 National Level Efforts ..... 10
5.2 State Government Efforts ..... 11
5.3 International Efforts ..... 12
**6 Confidence Mechanisms - Discussion ..... 14**
6.1 Emerging Themes ..... 14
6.2 The Way Forward ..... 19
**References ..... 20**
**Appendix A— Conformity Assessment ..... 21**
A.1 Requirements ..... 22
A.2 Determination ..... 22
A.3 Attestation ..... 23
A.4 Surveillance ..... 24
A.5 Examples of Existing Conformity Assessment Programs ..... 24

## List of Figures

Figure 1 - Trustworthiness of Cyber Physical Systems ..... 3
Figure 2: Framework for Customer Confidence ..... 6
Figure 3: Conformity Assessment Components ..... 21

# 1 Introduction

## 1.1 Background and Purpose

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT devices are an outcome of combining the worlds of information technology (IT) and operational technology (OT). IoT devices have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution [LTE], Zigbee, Ultra-Wideband [UWB]) for interfacing with the digital world.

There is an explosion of IoT devices in the market – customers of such devices include individual consumers implementing IoT within their home environments as well as organizational customers implementing IoT devices for business use. They purchase and use IoT devices in their environments due to the attractive functionality offered by such devices at a reasonable price point. Many such customers are unaware of the need to ensure that the device is securable and will not create a network risk.

Some groups of IoT device customers are indeed worried about the hazards posed by missing or weak security capabilities of these devices and how these weaknesses can be exploited to bring direct or indirect harm to the customer and their environment. However, these customers may or may not have access to adequate confidence mechanisms for the security of the IoT devices they wish to use. For example, US federal agencies have a large installed base of IoT devices in their environments and are rapidly expanding the use of additional IoT devices to address a variety of functional requirements. Yet, many such agency customers are seeking methods to achieve a higher level of awareness of and confidence in the security capabilities of these IoT devices.

What is a confidence mechanism? Confidence is defined as *the feeling or belief that one can rely on someone or something*. Mechanism is defined as *an established process by which something takes place or is brought about*. For the purposes of this essay, the term confidence mechanism can be defined as "an established process by which the user can rely on someone or something" and addresses the landscape of approaches to achieve assurance about the security capabilities of IoT devices.

In preparing this essay, NIST conducted extensive research on initiatives that can help to instill confidence in IoT device security and held a series of meetings with government and industry experts to glean information on the unique aspects and challenges in this space. This essay describes the landscape of confidence mechanisms that are currently available for establishing the security of IoT devices in the marketplace. Also included (as an appendix) is a summary of existing NIST work in conformity assessment to describe the different approaches that can be used to establish confidence that products meet target standards and specifications.

This essay also identifies a few emergent themes which need to be addressed by existing or evolving confidence mechanisms for IoT device security. These themes are listed below and discussed in further detail in Section 6:

- Theme 1: The diversity and scale of IoT devices precludes having a single approach for establishing security confidence

- Theme 2: The selection of confidence mechanism has to be risk based, with greater risk potentially requiring more rigorous confidence mechanisms
- Theme 3: Confidence mechanisms must be clear about the assumptions and limits of the confidence attestations
- Theme 4: Confidence mechanisms can exacerbate problems of market fragmentation through narrow certifications or can mitigate by providing a certification that is recognized broadly
- Theme 5: Certain categories of customers cannot be expected to take extensive actions with respect to IoT security
- Theme 6: Maintaining appropriate confidence in a device over its lifetime requires IoT device manufacturers and confidence mechanisms to consider additional dimensions
- Theme 7: Customer awareness and training are essential to expanding the recognition of IoT security confidence mechanisms

The next steps will involve collaboration among stakeholders to generate ideas and opportunities for evolving existing mechanisms and developing new mechanisms to encourage a marketplace for secure IoT products.

The purpose of this essay is to start a conversation about what it means to have confidence in the cybersecurity of IoT devices used by individuals and organizations and the various ways of gaining that confidence.

## 1.2 Scope

Security is one dimension of the trustworthiness of a system. The NIST Cyber Physical Systems (CPS) team has done extensive research into the characteristics of systems that interact with both the physical world as well as the cyber world and has developed a notional framework (see Figure 1) for trustworthiness for CPS that incorporates five key dimensions – *security, privacy, safety, reliability, and resilience*.

The CPS trustworthiness framework is directly applicable to the trustworthiness of IoT devices since the fundamental concepts of CPS and IoT are closely aligned. Although all five dimensions of trustworthiness of IoT are important, the security dimension is the primary thrust of this essay. However, it may be noted that a security failure in an IoT device has the potential to undermine all the other trustworthiness dimensions of the device.

This essay is focused on confidence mechanisms for security of IoT devices which is a step in the process of establishing trust in that system.

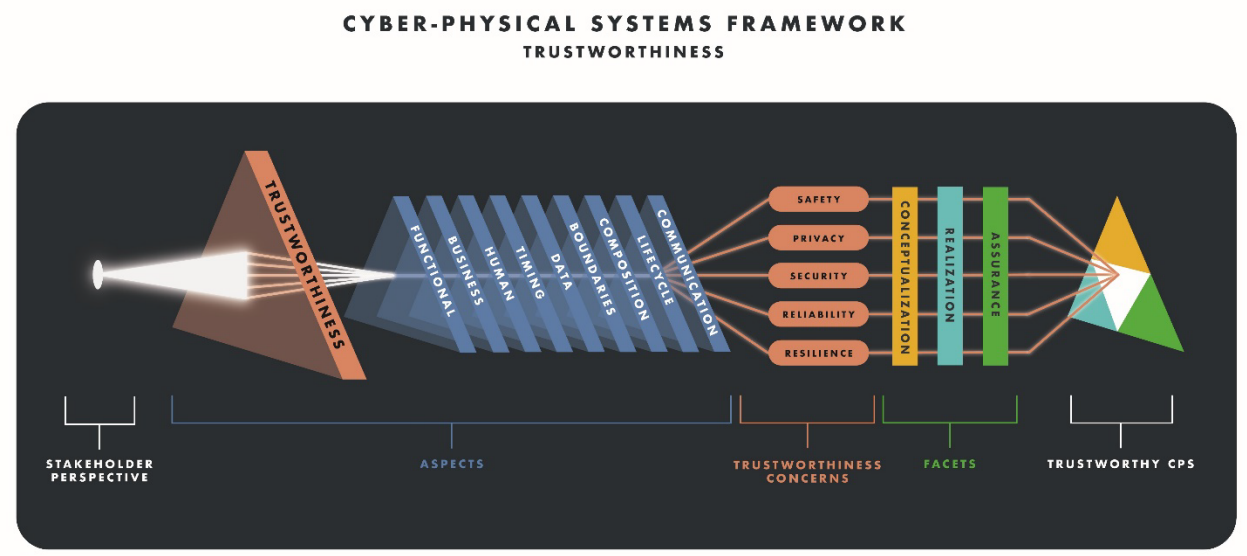


**Figure 1 - Trustworthiness of Cyber Physical Systems**

## 1.3 Intended Audience

The intended audience for this document includes security researchers, federal agency personnel responsible for purchasing and operating IoT devices, IoT manufacturers, consumer advocacy groups, members of standards organizations and third-party certification bodies who have an interest in establishing a marketplace of secure IoT products.

## 1.4 Organization

This essay is organized as follows. Section 2 describes the similarities and dissimilarities between IoT and IT devices with respect to security. Section 3 describes the various types of confidence mechanisms and a general framework for customer confidence. Section 4 provides a high-level survey of the landscape of non-regulatory confidence mechanisms while Section 5 provides examples of policy-based confidence mechanisms. Section 6 summarizes the essay and provides some themes and observations on building confidence mechanisms for IoT device security.

## 2 Security of IoT Devices

IoT devices interact with the physical world through sensors and actuators. However, IoT devices are also Information Technology (IT) devices that collect, store and/or transmit information (data) over network connections. Since they can be viewed as IT assets/systems, IoT devices and the data that they process need to be protected for confidentiality, integrity and availability just like any other IT system. Many of the vulnerabilities that plague other IT systems also affect IoT devices, and the attack methods that target other IT systems may also be used against IoT devices and systems.

Yet, IoT devices are different than conventional IT devices and systems in many ways. Many IoT devices interact with the physical world in ways conventional IT devices do not (and cannot). For example, IoT sensor data, representing measurements of the physical world, have to be effectively managed in order to mitigate physical attacks on sensor technology. IoT devices with actuators have the ability to make changes to physical systems and thus affect the physical world. The potential impact of manipulating these physical actuators needs to be explicitly recognized and addressed. A security compromise could allow an attacker to hijack or control the actuators of an IoT device to endanger human safety, damage or destroy equipment and facilities, or cause major operational disruptions.

Many IoT devices cannot be accessed, managed, or monitored in the same ways conventional IT devices can. Conventional IT devices usually provide authorized people, processes, and devices with hardware and software access, management, and monitoring features. In contrast, many IoT devices are opaque, often referred to as "black boxes." They provide little or no visibility into their state and composition, including the identity of any external services and systems they interact with, and little or no access to and management of their software and configuration.

The availability, efficiency, and effectiveness of security capabilities are often different for IoT devices than conventional IT devices. Many IoT devices do not or cannot support the range of security capabilities typically built into conventional IT devices.

Unlike conventional IT devices/systems, IoT devices possess some **unique characteristics** that make it challenging[1] to implement and maintain a strong security posture. For example:

- The power and computational limitations may make it difficult to implement complex security protections such as cryptography.
- The software/firmware on the devices are often highly configurable – thus, the specific configuration used by a customer may affect the security of the device functionality.
- It is often unclear whether the data handled by the device is sensitive or the possible impacts of data aggregation for unanticipated purposes.
- The mismatch between the expected life of the physical elements of the device versus the IT elements can create long term support challenges.
- The difficulty of communicating with customers (post-market) regarding new security vulnerabilities and the availability of firmware/software updates makes it challenging to maintain the security posture of IoT devices in the operational environment.

[1] https://doi.org/10.6028/NIST.IR.8228

# 3 Confidence Mechanisms for IoT Device Security

As defined earlier, a confidence mechanism is *"an established process by which the user can rely on someone or something."* For the purposes of this essay, NIST is exploring the types of confidence mechanisms that are available to customers of IoT devices with regards to their security capabilities.

## 3.1 Sources of Confidence

Many customers of IoT devices, especially in the consumer market, do not have the expertise to appreciate the potential risks posed by these devices. Other customers understand the need to have confidence in the overall trustworthiness (including resistance to security threats) of the IoT devices they use and are seeking mechanisms to have confidence in the security of IoT that they buy and use.

From the customer's perspective, the available sources of confidence in IoT device security include:

- **User experience** – Customer has had positive experiences related to security mechanisms in the IoT device. The customer believes that the available, configurable security mechanisms meet their needs and are meaningful, relevant, and usable.
- **Reporting by Consumer Groups** – Customer believes that if there was a problem with the IoT device, it would be evident from news media and/or reports published by consumer advocacy groups.
- **Brand Recognition** – Customer has a deep level of trust in the manufacturer or reseller's brand and has confidence in their IoT products.
- **Manufacturer Assertions** – Customer believes that a Manufacturer's assertion (e.g., a label[2] or online assertion) provides confidence in the IoT product.
- **Trade Association Assertions** – Customer believes that an assertion made by a relevant trade association or business advocacy group provides confidence in the IoT product.
- **Third-Party Assertions** – Customer believes that a Third-Party Assertion (e.g., a certification marking or online assertion) provides confidence in the IoT product.
- **Regulations and Enforcement** – Customer believes there are government regulations that protect them from unsafe devices and that enforcement bodies (such as consumer protection agencies) will ensure that violating manufacturers/resellers will be made to recall or ban unsafe products.

[2] Product labels are a well-established mechanism for asserting characteristics and attributes of products. Manufacturers use labels to describe the product, its characteristics, and benefits. Certain labels (such as nutritional information labels on food products, or weight and volume metrics for a product) are mandated by the government and the accuracy of the label is enforced by law. Some other labels indicate assertions about the product by third parties (such as the UL approved label for electrical products or Energy Star label on appliances). A label may be directly affixed to the product packaging. It can also take the form of literature included with the product, QR codes that lead to online statements, manufacturer website claims, etc. Labels are markings that proclaim attributes about a product and can be issued by manufacturers, trade associations or third-party assessment bodies.

## 3.2 Framework for Customer Confidence

The Figure 2 illustrates a general framework for consumer confidence. This framework comprises the following participants:

- **Customers** of a category of product
- **Advocacy Groups** that watch out for the customer's interest
- **Manufacturers** of products
- **Regulators** that mandate requirements for a particular market or category of product and enforce them
- **Standard Development Organizations (SDOs**) and **Industry Consortia** (trade associations and business advocacy groups) that develop specifications and requirements for a category of product and establish consensus or industry standards for that category
- **Conformity Assessment Bodies** (CABs) that measure conformity of products to a selected standard or regulation and provide certifications indicating the level of conformity

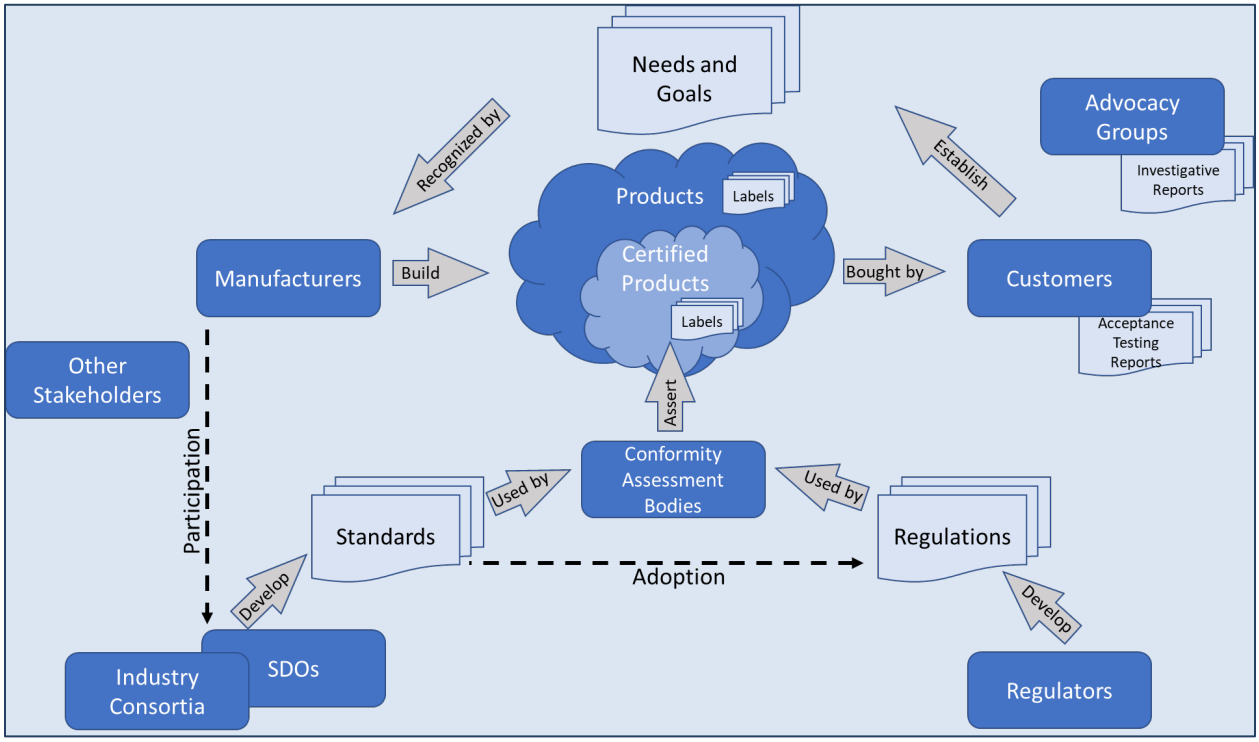


**Figure 2: Framework for Customer Confidence**

Customers have functional needs and goals that need to be met. Manufacturers build products to meet the perceived or articulated functional needs and goals of their target customers. Depending on the criticality of the functions provided by the product, regulatory bodies may enact regulations and establish mandatory requirements for the product category and enforce them through watchdog

organizations. SDOs and Industry Consortia establish standards that are relevant to that product category.

Either because they are driven by regulation or the desire to differentiate their products in the marketplace, manufacturers work to meet applicable sets of regulations or standards. Ultimately the customer determines what standards are important for them and what regulations apply to their market and then seek out ways to obtain confidence that the products they want to purchase meet those regulations/standards. Based on the category of product, there may be various mechanisms available for the Customer (such as consumer reports, manufacturer labels, and certification statements issued by independent CABs) to achieve the desired level of confidence that the product meets the requirements.

## 3.3 Benefits of Confidence in IoT Device Security

With appropriate confidence mechanisms, customers will have a way to distinguish IoT products that have strong security controls from those that have weak or non-existent security controls. This will help customers to determine the value-to-cost tradeoff for secure IoT devices and select more secure devices when appropriate for their risk profile.

The availability of confidence mechanisms also allows manufacturers to differentiate their products from less secure comparable products. This creates is a gradual pressure in the marketplace to build better security within IoT devices. Having confidence mechanisms that are based on standards recognized across many geographies allows manufacturers to build secure IoT devices that can be sold across many regions, which makes it more cost effective to build secure IoT devices. The IoT device marketplace can thus continue to thrive and provide highly sought functionality and services to customers across the globe.

# 4 Landscape of Non-Regulatory Confidence Mechanisms

## 4.1 Consumer Advocacy Groups

Several consumer advocacy groups are focusing their attention on IoT security. Their work serves to drive customer awareness of IoT device cyber risks and advocates for ways to instill higher confidence in these products. Some examples are provided below.

- Consumer Reports (CR) is working to create a new open-source industry criteria-set that can be used to safeguard the security and privacy of consumers of IoT devices[3]. They issued a letter to 25 connected camera manufacturers saying that they will change their rating system to reflect stronger security and privacy standards. They have issued a guide for digital security and privacy to help consumers navigate the complexities, risks, and easy-to-follow tips on using IoT devices[4].
- The Center for Democracy and Technology (CDT) has filed comments with the Consumer Products Safety Commission[5] in response to hearings on IoT and consumer product hazards and have reported on the liability issues surrounding IoT[6].
- Electronic Privacy Information Center (EPIC)[7] pursues a wide range of program activities including policy research, public education, conferences, litigation, publications, and advocacy. They are looking at the security and privacy issues of IoT devices that are connecting to other devices and people over the existing Internet infrastructure.
- Internet Society is a global nonprofit organization empowering people to keep the Internet open, globally connected, secure, and trustworthy. They are investigating the impact of IoT devices[8] and have developed a IoT security and privacy checklist for manufacturers and enterprise users as well as a list of top tips for consumers of IoT.
- Consumers International is a membership organization for consumer groups around the world working to ensure that the voice of the consumer is heard

## 4.2 Industry Consortia (Trade Associations and Business Advocacy Groups)

Various trade organizations and business advocacy groups are working to improve the state of IoT device security through development of relevant requirements and standards and/or shaping the industry's stance on policy issues. While not exhaustive, some examples are provided below.

- The ioXt Alliance[9] comprises over 300 member companies (including Amazon, Google, Comcast, T-Mobile and many others) operating in over 30 countries. Through its Working Groups, ioXt

[3] https://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/
[4] https://www.consumerreports.org/digital-security/online-security-and-privacy-guide/
[5] https://cdt.org/insights/protecting-consumers-in-the-era-of-iot-cdt-comments-to-the-consumer-product-safety-commission/
[6] https://cdt.org/insights/when-iot-kills-preparing-for-digital-products-liability/
[7] https://epic.org/privacy/internet/iot/
[8] https://www.internetsociety.org/iot/
[9] https://www.ioxtalliance.org/

develops security profiles to meet specific product or market security needs and to comply with regulations in the countries where the products are sold. ioXt offers two types of certification: testing of products by accredited third party laboratories and self-attestation by manufacturers. A product that successfully completes the ioXt certification process results in the issuance of a SmartCert, which is a QR code label that links back to the ioXt website and shows if the device is currently "ioXt certified" or not. ioXt also combines researcher rewards for identification of vulnerabilities on all of their certified products. ioXt focuses on the smart home, smart building, cellular IoT, and mobile application markets.

- CTIA represents the U.S. wireless communications industry. CTIA's IoT Cybersecurity Certification Program[10] establishes an industry baseline (developed in collaboration with leading wireless operators, technology companies, security experts, and test labs) for device security on wireless networks. The program is based on technical testing of tangible IoT security features by CTIA Authorized Test Labs (CATLs). The CTIA IoT security certification program was designed to be a framework for OEMs and other device manufacturers to go through rigorous testing and be certified; this certification provides assurances to network operators.
- The Consumer Technology Association[11] (CTA)® is the trade association representing the US consumer technology industry. The CTA® IoT Working Group supports the advancement of the consumer IoT industry through market research, education, standards and policy efforts.

## 4.3 Third Party Confidence Mechanisms

There are several active third-party programs for testing and certification and/or labeling of IoT devices against security requirements. While not meant to be exhaustive, below are some representative examples of such programs. It may be noted that NIST has extensive experience with conformity assessment programs. Appendix A describes the terminology and concepts related to conformity assessment from NIST publications on this topic.

- Underwriters Laboratories (UL) launched its IoT Security Rating in 2019, with the goal of providing assessments against the UL MCV (Marketing Claim Verification) 1376, which is a set of requirements representing industry best practice baseline security capabilities for consumer and commercial IoT devices. Testing against MCV 1376 can be performed at five (5) levels: Bronze, Silver, Gold, Platinum and Diamond – with an increasing set of security capabilities being verified at each level starting with Bronze as the basic level. The UL IoT Security Rating is applicable to the overall consumer and commercial IoT industry. On successful evaluation at a particular level, manufacturers receive a UL Verified Mark (rather than a *certification*) and a security label.
- TIC Council is a global association representing Testing, Inspection and Certification organizations[12]. Members operate 3rd party conformity assessment programs or are conformity assessment scheme owners and must demonstrate ongoing compliance with ISO/IEC 17025 in addition to compliance review against TIC Council's Code of Practice.

[10] https://ctiacertification.org/program/iot-cybersecurity-certification/
[11] https://www.cta.tech/Membership/Member-Groups/IoT-Working-Group
[12] https://www.tic-council.org/about-us

# 5 Landscape of Policy-Based Confidence Mechanisms

With the explosion of IoT devices of various types that are available on the market and the rapid pace at which such devices are being adopted by individual consumers and being integrated into the infrastructure of various organizations, there is significant awareness by governments and industry that the security of these devices requires further attention. This section provides examples of some of the efforts made by governments to drive better security in IoT devices.

## 5.1 National Level Efforts

Executive Order (EO) 13800[13], *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* was issued in May 2017. The focus of EO 13800 is to improve the Nation's cyber posture and capabilities against intensifying cybersecurity threats by modernizing Federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies.

Published in March 2020, the U.S. Cyberspace Solarium Commission report[14] consists of over 80 recommendations organized into 6 pillars, describing a new strategic approach to defending the United States in cyberspace against cyber-attacks of significant consequences. The report makes a recommendation for the creation of a National Cybersecurity Certification and Labeling Authority (NCCLA) to establish and manage a voluntary cybersecurity certification and labeling program for critical information and communication technologies, including IoT devices. The term critical implies that that the product is in use in critical infrastructure sectors supporting national critical functions as determined by DHS. The NCCLA would work in coordination with other Federal government to identify common security standards, frameworks, and benchmarks against which the security of the product can be measured. The certification would result in a label or symbol provided by an accredited certifying agent resulting from a comprehensive evaluation of the product against a set of specified security standards. Three classes of certification would be supported: attestation-based, accreditation-based, and Third-party test-based. The label would be a clear visual and easy to understand symbol or list that conveys a product's security capabilities and features. The labels would be enforced by the Federal Trade Commission for falsely labeled or mislabeled products. It is envisioned that a nonprofit, nongovernmental organization may be suitable to serve as a project manager for centralized certification and labeling efforts in the United States.

Public Law 116-207[15], *IoT Cybersecurity Improvement Act of 2020,* was passed by Congress in December 2020, to establish minimum security standards for IoT devices owned or controlled by the Federal Government. It requires the establishment of security standards and guidelines for agencies on the use and management of IoT devices; establishment of guidelines for and implementation of coordinated disclosure of security vulnerabilities relating to IoT devices; and contractor compliance with the coordinated disclosure of such vulnerabilities. This law specifically addresses the general use of IoT devices within the information technology environment of a federal agency and the security standards

[13] https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure
[14] https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view
[15] https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf

that need to be upheld with such use. It may be noted that IoT cybersecurity is also being addressed by federal agencies that regulate specific classes of consumer IoT devices that pose special hazards (such as FDA for connected medical devices and Department of Transportation for connected cars).

The Consumer Product Safety Commission (CPSC)[16] is charged with protecting the public from unreasonable risks of injury or death associated with the use of the thousands of types of consumer products under the agency's jurisdiction. CPSC has been looking into the safety hazards posed by IoT devices in the consumer space for some time and released *A Framework of Safety for the Internet of Things*[17] in 2019 that provides technology-neutral best practices to incorporate consumer product safety in the design and deployment of devices, software, and systems. In its FY 2021 Operating Plan[18], CPSC includes the following FY 2021 priority activity: "Focus on potential safety issues associated with Internet of Things (IoT)/Connected products."

The Federal Trade Commission (FTC)[19] protects consumers and competition by preventing anticompetitive, deceptive, and unfair business practices. The FTC performs its activities through law enforcement, advocacy, and education. The FTC also advances consumers' interests; develops policy and research tools through hearings, workshops, and conferences; and creates practical and plain-language educational programs for consumers and businesses. It enforces federal laws (such as the FTC Act and others) relating to consumers' privacy and security[20] through cases brought against companies that make claims that they do not substantiate through actions. It has brought legal actions against organizations that have violated consumers' privacy rights, misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury.

## 5.2 State Government Efforts

Various state governments have started work on legislation to regulate the security of connected devices. For example, California[21] and Oregon[22], have formally enacted laws targeted at device manufacturers. Several other states (e.g., Maryland[23], Illinois[24], Virginia[25] and New York[26], Vermont[27] ) have started state level legislation efforts related to connected device security – however, none of these efforts have resulted in state regulation as of this writing.

[16] https://cpsc.gov/About-CPSC
[17] https://www.cpsc.gov/s3fs-public/A_Framework_for_Safety_Across_the_Internet_of_Things_1-31-2019_0.pdf?1KJ.t4Tn04v9OtEBr2s0wyLAP.KsuuQ3
[18] https://www.cpsc.gov/s3fs-public/Fiscal-Year-2021-Operating-Plan.pdf?CKb6Hx.as1gLs3MDCecBUq3Daqo1f5nt
[19] https://www.ftc.gov/about-ftc
[20] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement
[21] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
[22] https://olis.leg.state.or.us/liz/2019R1/Measures/Overview/HB2395
[23] http://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0443?ys=2020RS
[24] https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3391&GAID=15&DocTypeID=HB&LegId=119982&SessionID=108&GA=101
[25] https://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+HB2793&191+ful+HB2793
[26] https://www.nysenate.gov/legislation/bills/2019/s3973
[27] https://legislature.vermont.gov/bill/status/2020/H.157

Since the passing of the *IoT Cybersecurity Improvement Act of 2020*, most states have suspended state level efforts to develop legislation for securing connected devices to avoid fragmentation and suppression of the IoT marketplace with dissimilar state level laws.

## 5.3 International Efforts

Many countries (including the US, UK, Brazil, Taiwan, Australia, Singapore, Japan and others) have been working on laws to regulate the security of IoT devices. While not exhaustive, several examples are provided below.

The European Union (EU) Cybersecurity Act[28], issued in April 2019, aims to achieve a high level of cybersecurity, cyber resilience and trust in the EU by setting (i) objectives, tasks and organizational matters for a strengthened and renamed European Union Agency for Cybersecurity (ENISA), with a new permanent mandate; and (ii) a framework for voluntary European cybersecurity certification schemes for Information and communications technology (ICT) products, services and processes.

The EU Cybersecurity Act establishes the EU Cybersecurity Certification Framework[29] to: (a) improve the functioning of the internal market by increasing the level of cybersecurity in the EU and enabling a harmonized approach at EU level to European cybersecurity certification schemes; and (b) set up a mechanism to establish certification schemes that confirm ICT products, services and processes that have been evaluated in accordance with such schemes comply with specified security requirements to protect the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or functions or services offered by, or accessible via, those products, services and processes throughout their life cycle.

In October 2018, the Government of United Kingdom (UK) has published the *Code of Practice for Consumer IoT Security*[30], which sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. The document describes thirteen guidelines that that are widely considered good security practice and can contribute to protecting consumers' privacy and safety.

In February 2020, the UK government published its *Response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation*[31], advocating a robust and staged approach to enforcing improved IoT security through regulation, starting with ensuring stronger security is built into products. The regulatory proposals set out in the consultation advocated mandating the most important security requirements centered around aspects of the top three guidelines within the Code of Practice for Consumer IoT Security and the ETSI Technical Specification (TS) 103 645, which are: (i) IoT device passwords must be unique and not resettable to any universal factory setting; (ii) Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy; and (iii)

[28] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[29] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[30] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security
[31] https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation

456 Manufacturers of IoT products explicitly state the minimum length of time for which the device will
457 receive security updates. This is the start of the journey and the UK Government will look to increase the
458 baseline and mandate further security requirements as and when appropriate.

459 The Government of Australia published a voluntary *Code of Practice, Securing the Internet of Things for*
460 *Consumers*[32] in 2020. This code of practice comprises 13 principles that are recommended to be
461 followed by industry as a minimum standard for securing IoT devices.

[32] https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

# 6 Confidence Mechanisms - Discussion

As described in this essay, there is an urgent and critical need to improve the security capabilities of IoT devices available in the marketplace. Various organizations have been working on and have issued standards and guidance on security best practices for IoT devices. Several governments are considering regulatory actions or have enacted regulations related to the security of connected devices such as IoT.

To address the demand for confidence in the security capabilities of IoT products, several conformity assessment programs for IoT device security are available and others are evolving. Some of these are based on third-party (independent) assessments of conformity to a specified standard, while others are based on a supplier's (or manufacturer's) self-assessment and declaration of conformity to a standard. Consumer advocacy groups have also been investigating the impact of security compromise of IoT devices.

## 6.1 Emerging Themes

From the research and analysis performed in developing this essay, the following set of themes emerged related to building confidence mechanisms for IoT devices. These are described below.

**Theme 1: The diversity and scale of IoT devices precludes having a single approach for establishing security confidence**

Just as cybersecurity is not "one-size-fits-all" solution, there is no magical "one-size-fits-all" approach for building confidence in IoT device security. The great diversity of IoT devices and the use cases they address make it difficult to create a single set of prescriptive security requirements or confidence mechanism for these devices. Each of the sources of confidence listed in 3.1 could be appropriate depending on the device and requirements involved.

The security posture of an IoT device in an operational environment is often dependent on the specific configuration of the device. While an IoT device may possess excellent security capabilities, it's actual configuration will determine the level of the effective security. Hence, it may be necessary for confidence mechanisms for IoT device security to assert the configurations that were assessed or tested.

The short (expected) life span and low cost of some of these devices make it economically impractical to apply expensive and time-consuming confidence mechanisms. As a result, different types of confidence mechanisms (with varying levels of rigor or complexity) may emerge as being more suitable for different categories of IoT devices.

IoT devices incorporate complex technologies related to actuators, sensors, information technology hardware and software. As a result, manufacturers of these devices often rely on a host of suppliers for the various components. This makes it more difficult for the ultimate integrator/manufacturer to ensure that the components used are free from defects that can have negative impact on the overall security of the device. These supply chains may also be lengthy and span international borders. The risk of inadvertent or intentional security weaknesses in IoT devices can be high as a result. Confidence mechanisms for IoT devices that have complex supply chains may need to check for transparency in the supply chain using techniques such a software-bill-of-materials (SBOM). They may also need to track

changes in the supply chain over the life of the product. For example, a manufacturer might change cloud service providers over the life of an IoT device.

**Theme 2: The selection of confidence mechanism has to be risk based, with greater risk potentially requiring more rigorous confidence schemes**

The risk of insecure IoT varies by context and environment of use. IoT devices span a very wide variety of functional capabilities from smart medical/health devices to smart lighting and appliances. Security weaknesses in these devices can be used as a launching point to impact other elements of trustworthiness (such as *privacy, safety, reliability, and resilience*) of that device.

While all types of risk cannot be captured in a single list, some areas of risk to consider are:

- Risk of compromising device functionality – IoT devices can be used to support critical functions (such as health, safety, transportation, etc.). In addition, some devices can potentially become hazardous through a security compromise, such as a device that generates heat like a stove or coffee pot.
- Risk due to device location – An IoT device that has the capability to collect voice or video data may pose a much higher risk in a sensitive location (such as a lawyer's conference room or a medical exam room) and may need a higher level of assurance regarding its security.
- Risk of compromising the local network – IoT devices with weak security can create a weak point for unauthorized access to the network to which the device is attached. This introduces risk to other systems and devices that are connected to the same network. Bad actors can use weak IoT devices (whether supporting a critical function or not) to launch an attack on other connected systems and devices.
- Risk of using the IoT Device to attack external systems – Compromised IoT devices have been used as "bots" to participate in denial-of-service attacks unbeknownst to the device owner. Maintaining the security of IoT devices has broader benefits in denying malicious actors the ability to use them in attacks.

For high impact environments (such as critical infrastructure installations), the addition and use of IoT devices should always be preceded by a comprehensive risk assessment. The results of the risk assessment can be used to inform the selection of appropriate confidence mechanisms that provides the needed level of assurance in the security of the IoT devices being deployed.

While the security posture of the network environment to which the IoT is connected influences the operational security of the device, this concern exists for any IT device on the same network as well. For example, an IoT device connected to an unsecured wireless network (such as at a hotel lobby, airport or coffee shop) is extremely vulnerable regardless of the security capabilities of the actual IoT device itself. Using a device that boasts a more rigorous security confidence assertion may or may not be helpful. In such cases, compensating security controls may need to be implemented in order to protect the IoT device from compromise.

**Theme 3: Confidence mechanisms have to be clear about the assumptions and limits of the confidence attestations**

While IoT device manufacturers have intended markets and use cases for their products, these devices may often be used across market segments and for unexpected use cases from the original intended use. For example, a smart speaker/microphone that goes through a security certification for use in a home environment may be used in an industrial environment where the threats are quite different than a home environment. The security confidence mechanism that the manufacturer selected for the IoT device may have been based on the expected usage environment and the security threats that exist in such an environment.

It is desirable that the attestations from confidence mechanisms should specify the expected environment of use and any related assumptions so that the customer can understand the limitations of a particular IoT device and make appropriate choices.

Using the same IoT device in an unexpected environment with very different set of threats and threat actors may result in a much higher level of risk. As mentioned earlier, a risk assessment should ideally be performed for the use of IoT in the specific target environment prior to selecting a particular IoT device with a known set of security capabilities and security confidence mechanisms.

**Theme 4: Confidence mechanisms can exacerbate problems of market fragmentation through narrow certifications or can mitigate by providing a certification that is recognized broadly**

Many National as well as local governments have been analyzing the impacts of insecure IoT devices within their jurisdictions and developing legislation and/or guidance to protect their constituents from the negative impacts of such devices. Several have passed legislation and/or guidance on minimum security requirements for IoT devices; others are still working on developing such legislation or guidance. Similarly, many standards bodies, consumer advocacy groups and industry consortia have been working to develop standards, guidelines and best practices for IoT device security. As a result, there are multiple (and potentially conflicting) IoT device security requirements and standards issued by various interested stakeholders. Confidence schemes (such as certifications) for IoT device security are typically based on standards and/or regulations that are applicable to the IoT market segment.

Regulators recognize that multiple jurisdictional regulations can fragment the marketplace and have been working on ways to harmonize the requirements they establish. There have also been efforts to establish mutual recognition of IoT device security standards across jurisdictions and markets.

From a manufacturer's perspective, the existence of multiple certification schemes for their IoT products and the lack of reciprocity between various types of existing certifications drive up the cost of product manufacture. Additionally, for manufacturers that sell products in multiple regulatory jurisdictions, the existence of disparate confidence schemes that are not mutually recognized make it economically unsustainable to develop IoT products that can be sold in these different jurisdictions.

Several IoT device security confidence schemes may be available in certain markets. For IoT customers, the existence of multiple confidence schemes within a given market offers advantages as well as disadvantages. When a customer needs to select a confidence scheme based on the risk level of their use case, it is good to have options to select from. However, for other customers, having multiple confidence schemes makes it is difficult to select one for their particular use case.

In some cases, a single certification could meet the requirements of multiple markets or standards thereby mitigating market fragmentation.

**Theme 5: Certain categories of customers cannot be expected to take extensive actions with respect to IoT security**

Security for IoT devices cannot be achieved through technology alone. Many IoT devices are designed and built with technical security capabilities - however, in many instances, the security capabilities must be enabled or selected within the environment of use to become operational. To assist the customer to make the right choices in operating these devices, manufacturers may provide guidance/instructions explaining secure configurations, software updates to address discovered vulnerabilities, and security best practices for their products. The customer is assumed to be a partner in ensuring adequate security of these IoT devices.

Certain categories of customers may be more or less prepared to assume this responsibility. There is a significant difference between organizational customers versus individual (and small business) customers of IoT. The former set can be presumed to have a higher level of security awareness as well as resources to address security of the IoT devices they use within their environments. Organizational customers may be capable of implementing IoT devices in accordance with manufacturer instructions, ensuring devices have connectivity to receive updates (when available), and monitoring devices to ensure continued security. Organizational customers often have established policies/processes to manage the additional risks introduced through the use of IoT devices in their environment to achieve compliance with regulations that apply to their industry segment.

Individual consumers or small business customers of IoT devices are often unaware of the security concerns related to IoT and do not have the sophistication to understand and implement security measures needed to secure their IoT devices. For this group, it may be difficult or impossible to engage the customer to enable the needed configurations for secure operation of IoT devices. IoT devices targeted at this group of customers may need to have stronger default security configurations and simpler sets of instructions to enable security.

**Theme 6: Maintaining appropriate confidence in a device over its lifetime requires IoT device manufacturers and confidence mechanisms to consider additional dimensions**

Like all other IT devices, the threat environment for IoT devices is continuously evolving, with the identification of new vulnerabilities and emergence of new attack methods. Over the years, IT manufacturers have evolved an infrastructure of vulnerability disclosure policies, vulnerability reporting mechanisms, vulnerability databases, and software patching and updates. Organizational and individual customers receive notifications of updates, and those updates have become routine. While not all organizations and individuals perform updates, the processes for updating are at least well-established and available to organizations and individuals who take advantage of them.

However, vulnerability disclosure and remediation are not routine practices for IoT devices. Many IoT manufacturers are still building this type of infrastructure and not yet providing routine software updates. With the variety of IoT devices available in the market, the customer's role in installing updates may vary by type of device and customer. IoT customers are often unaware of the security risks of such devices and the importance of being vigilant about installing and applying security updates. Customers

having to cope with different software update cycles for a larger and larger number of devices can be overwhelmed. IoT manufacturers have to develop effective strategies to deal with the current maturity state of the IoT customer base and their awareness of and ability to deal with security issues.

Another related challenge is that there is a mismatch between the life span of the IT components and the mechanical components of an IoT device. Manufacturers may establish a product support period for the IoT device based on the expected lifetime of the IT components. During the support period, the manufacturer may implement an effective vulnerability disclosure and remediation program for the product. Yet, the IoT device may be quite functional beyond the manufacturer's support period and the customer may continue to use it. The device may be insecure at that point of its life. Many customers choose to use devices after support ends but need to recognize the risk involved.

A core focus of confidence mechanisms is to assess and attest that a product meets the stated requirements for a given environment of use prior to the product becoming available on the market. However, as pointed out in Appendix A, Section 7.3, confidence programs often provide assurance on an on-going basis through surveillance activities focused on maintaining the validity of the initial confidence attestation. IoT devices that received certification may need strong surveillance methods to ensure they continue to be secure.

**Theme 7: Customer awareness and training are essential to expanding the recognition of IoT security confidence mechanisms**

Many customers of IoT devices are unaware of the security implications of their use. Even if IoT device security information is available to target customers, the extent to which customers can use the information is open to question. Various participants gathered from the October 2020 NIST workshop entitled *Workshop on Cybersecurity Risks in Consumer Home IoT Products* highlighted research on IoT device customer behavior with respect to security. The lack of easily accessible and reliable security information in product information precludes most consumers from using security as a factor in selecting IoT devices. While various participants highlighted studies suggesting that consumers want, and may be willing to pay somewhat more for, secure IoT devices, those consumers do not have the background to evaluate detailed information about security or to perform complex security functions. In the individual consumer space, the buyer's assumption generally is that if a product is on the market, its safety and security can be assumed[33].

Modern day consumers recognize the value of a variety of other confidence mechanisms (such as food labels, gas mileage ratings or energy usage ratings) based on awareness campaigns launched by advocacy groups, industry groups and government organizations. It is difficult to gain customer recognition and acceptance of the value of new certifications/labels.

More awareness programs are needed to help customers understand the importance of IoT device security and the value of confidence mechanisms that attest to the security of IoT devices in the market. Such awareness campaigns may need to focus on individual consumers and small business customers who are much less prepared to deal with IoT device security than customers within larger, more mature organizations. If an IoT device security certification is widely recognized as valuable, it can be an

[33] https://doi.org/10.6028/NIST.IR.8322

important tool for communicating with customers.

In workshops on IoT held in 2020, NIST received feedback that reinforces these themes:

As identified in the summary report from NIST's October, 2020 *Cybersecurity Risks in Consumer Home Internet of Things (IoT) Devices Virtual Workshop*, "Consumers do not have a mechanism for recognizing which devices meet security baselines and which do not. Customers expect devices to be initially secure, but confidence mechanisms for establishing that security are not available." [NISTIR 8333]

One of the themes identified in the summary report of NIST's July, 2020 *Building the Federal Profile for IoT Device Cybersecurity Virtual Workshop* was: "*Evaluate Approaches for Establishing Confidence in IoT Device Cybersecurity*. Workshop participants indicated a desire for greater specificity regarding the use of conformance assessments and other confidence mechanisms such as labels and self-certification. These confidence mechanisms can be an important component of the IoT cybersecurity solution space. The program will begin exploring, in concert with interested government and industry organizations, approaches for gaining confidence in the cybersecurity capabilities of IoT devices that address the needs of both IoT device users and manufacturers." [NISTIR 8322]

Developing and making customers aware of confidence mechanisms could fill an important market gap.

## 6.2 The Way Forward

There is a need to strengthen the available ecosystem for confidence mechanisms for IoT device security. The size and diversity of the IoT device marketplace demonstrates the need for a variety of confidence mechanisms depending on the type of IoT device, use case, and risks involved in its operation. Different confidence mechanisms will be the best choice for different situations.

Bringing together communities of interest around particular device types and market segments and identifying the best confidence mechanisms will need to be worked through a variety of forums. As with many areas of security, no one size fits all and risk must be considered in its broadest context.

The themes that emerged in the process of developing this essay suggest that there are many topics that remain to be further discussed. NIST invites feedback on this essay as well as additional discussion on possible approaches to improve confidence in the security of IoT devices in the marketplace.

## References

[ISO/IEC 17000] International Organization for Standardization / International Electrotechnical Commission, *Conformity assessment — Vocabulary and general principles,* 2020.

[ISO/IEC 17020] International Organization for Standardization / International Electrotechnical Commission, *Conformity assessment — Requirements for the operation of various types of bodies performing inspection,* 2012.

[ISO/IEC 17021] International Organization for Standardization / International Electrotechnical Commission, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*, 2015.

[ISO/IEC 17024] International Organization for Standardization / International Electrotechnical Commission, *Conformity assessment — General requirements for bodies operating certification of persons*, 2012.

[ISO/IEC 17025] International Organization for Standardization / International Electrotechnical Commission, *General requirements for the competence of testing and calibration laboratories*, 2017.

[NISTIR 8322] Megas KN, Fagan M, Lemire D (2021) Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8322. https://doi.org/10.6028/NIST.IR.8322

[NISTIR 8333] Megas KN, Fagan M, Cuthill B, Raguso M, Wiltberger J (2021) Workshop Summary Report for "Cybersecurity Risks in Consumer Home Internet of Things (IoT) Products" Virtual Workshop. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8333. https://doi.org/10.6028/NIST.IR.8333

# Appendix A—Conformity Assessment

NIST serves as the focal point for federal government standards and conformity assessment coordination and is a key information source for United States industry on standards-related market access issues. Standards allow technology to work seamlessly and establish trust so that markets can operate smoothly. They:

- provide a common language to measure and evaluate performance,
- make interoperability of components made by different companies possible, and
- protect consumers by ensuring safety, durability, and market equity.

Under the National Technology Transfer and Advancement Act (NTTAA), NIST is assigned responsibility to coordinate federal, state, and local documentary standards and conformity assessment activities.

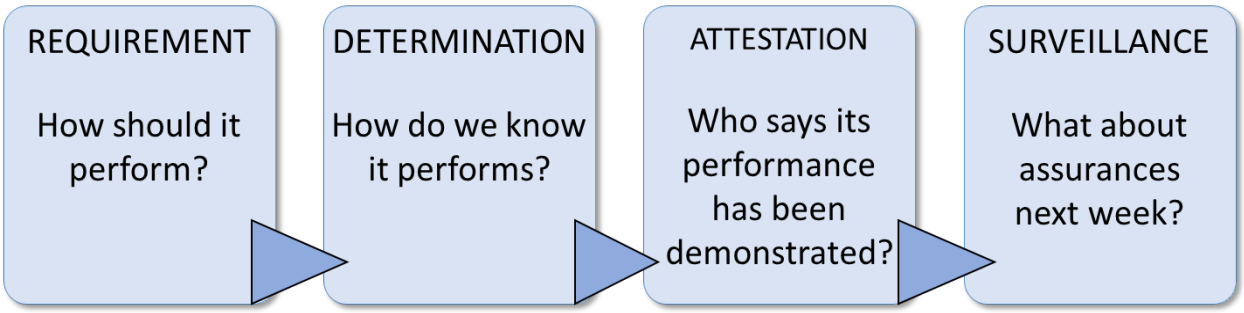


**Figure 3: Conformity Assessment Components**

Conformity Assessment is the demonstration that specified requirements relating to a product, process, system, person or body are fulfilled [ISO/IEC 17000]. NIST Special Publications 2000-1[34] and 2000-2[35] describe core concepts and terminology related to Conformity assessments. A conceptual view of conformity assessments includes four essential components (see Figure 3). These components are:

1. Requirements – representation of how the product or service should perform
2. Determination – methodology establishing how it performs
3. Attestation – an assertion that performance has been demonstrated
4. Surveillance – methodology establishing continuing assurance about the performance

Conformity assessment can assure that a particular product, service, or system meets a given level of quality or safety, and provide explicit or implicit information about its characteristics, the consistency of those characteristics, performance, and/or adherence to regulatory requirements. Conformity assessment can also increase ***confidence***, furnish useful information, and help to substantiate a company's advertising and labeling claims. Therefore, conformity assessment is an important marketplace communication mechanism providing a means of information exchange.

It is vital for interested parties to understand the conformity assessment process to competently judge

[34] http://doi.org/10.6028/NIST.SP.2000-01
[35] http://doi.org/10.6028/NIST.SP.2000-02

the value of a conformity assessment program and to use the information resulting from that program to make intelligent choices that can achieve the desired goals.

Various parties participate in such an ecosystem. These are the types of organizations and individuals that can participate in conformity assessment activities for a specified product or service include:

- First Party – the seller, manufacturer or supplier
- Second Party – the purchaser or user
- Third Party – individuals and organizations whose interests are independent of transactions between the first and second parties

## A.1 Requirements

Standards often contain the requirements for performance that are used as the basis for conformity assessments. Standards are a vital tool of industry and commerce promoting market understanding between buyers, and sellers thus enabling mutually beneficial commercial transactions. A standard is defined as a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

Standards can cover many aspects of the conformity assessment process. They can describe characteristics of the product for which conformity is sought; the methodology used to assess that conformity; or even the conformity assessment process itself (e.g., how a certification program should be operated). Standards used in conformity assessment should be clearly and concisely written, readily understood, precise, and technically credible, as well as contain requirements for objective verification.

## A.2 Determination

The Determination component comprises the activities that may be used to examine an object of conformity to specified requirements. A variety of conformity assessment activities may be used to provide evidence of conformity including:

- Testing – the determination of one or more characteristics of an object of assessment, according to a specified way to carry out an activity [ISO/IEC 17000]. Testing activity is used to develop information about the object's fulfillment of requirements. ISO/IEC 17025 is used to demonstrate that testing and calibration laboratories are competent and capable of generating valid results. Testing laboratories use a test method (often a set of procedures) to conduct tests on received samples and report data. Testing can be performed by first, second, or third-party laboratories. Test reports issued by testing laboratories may be used for evidence of conformance in support of other conformity assessment activities.
- Inspection - examination of a product design, product, process, or installation and determination of its conformity with specific requirements or, on the basis of professional judgement, with general requirements [ISO/IEC 17000]. Inspection is an activity to develop information about the object's fulfillment of requirements. ISO/IEC 17020 defines requirements for the operation of various types of bodies performing inspection. an inspection body uses an inspection method (often a set of procedures) to examine a product design, product, or

installation to determine conformity with requirements and produce an inspection report. Inspection can be performed by first, second, or third parties.

- Audit – a systematic, independent, documented process for obtaining records, statements of fact or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled [ISO/IEC 17000]. ISO/IEC 17021 outlines requirements for certification bodies to ensure that management system certifications are performed in a consistent, competent, and impartial manner. The audit activity may provide assurance of a credible management system certification.

## A.3 Attestation

Information obtained from a conformity assessment activity about the object's fulfillment of requirements is used as the basis of an attestation. An attestation is an issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated [ISO/IEC 17000]. The attestation intends to convey assurance about the conformity of the object to consumers, regulators, buyers, or other interested parties. Types of attestation are described in the subsections below.

### A.3.1 Supplier Declaration of Conformity

This is a declaration by the supplier that requirements have been met based on the results of testing, inspection, or audits undertaken by the manufacturer or other parties on its behalf. A declaration is generally used when the consequences associated with nonconformity are low, there are suitable penalties for placing nonconforming products on the market, and/or there are suitable mechanisms in place to remove nonconforming products from the market.

### A.3.2 Certification

This is a third-party attestation related to products, processes, systems or persons with the goal to provide confidence to interested parties that objects of assessment meet specified requirements. Certification may provide a higher level of confidence since the third-party's certification decision is required to be impartial and free of commercial, financial or other pressures. Certification programs often include surveillance and/or ongoing renewal process to ensure continued conformity.

Certification programs are usually designed for mass-produced products to provide assurance of continued conformity to applicable standards throughout the manufacturer's production process. There are many organizations that operate third-party certification programs, such as:

- Conformity assessment bodies
- Other organizations, such as nonprofit organizations
- Professional or technical societies
- Trade associations

The Federal government as well as State and Local governments also administer certification programs that cover a diversity of products from meat inspection to ensuring the health and safety of amusement rides on its population.

### A.3.3 Management System Certification

Management system certification is third-party attestation related to systems within an organization. A management system is the way in which an organization manages the interrelated parts of its business to achieve its objectives. Certification of management systems is generally used as a demonstration of fulfillment of quality, security, and environmental management system standards.

### A.3.4 Personnel Certification

Personnel certification provides confidence that individuals have skills needed to perform their work competently. ISO/IEC 17024 specifies requirements to ensure certification bodies for persons operate personnel certification schemes with competence, consistency, and impartiality.

## A.4 Surveillance

Conformity assessment programs may require assurance on an on-going basis. Surveillance comprises a group of activities conducted to maintain the validity of the attestation. Per ISO/IEC 17000, surveillance is defined as “systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.” Post-market surveillance involves the evaluation of certified products taken from the marketplace to determine if product requirements continue to be met. Pre-market surveillance is the checking of products before they reach the market and may include audits of the supplier's process control systems and/or inspection of the production.

## A.5 Examples of Existing Conformity Assessment Programs

The Environmental Protection Agency (EPA) ENERGY STAR16 program is a voluntary public-private partnership that relies on independent third-party certification to ensure ongoing compliance and the integrity of the ENERGY STAR label. Reliance on third-party certification helps maintain consumer trust and improve oversight of the program while allowing the agency to utilize the private sector to conduct evaluation and additional market surveillance activities.

The National Registry of Food Safety Professionals develops and maintains an accredited certification examination program in the areas of food safety as well as Hazard Analysis Critical Control Point (HACCP) for workers in food manufacturing facilities, plants, packaging facilities, and warehouses.

There are many additional examples of existing, successful conformity assessment programs that have promoted safety, security, interoperability and commerce. For example, UL certification for electrical devices ensures consumer safety and nutritional labels enable food purchasing decisions. Examples of programs that enhance security and interoperability include the FIPS 140 certification for cryptographic modules, FICAM certification for identity management products, and the FedRAMP certification of cloud services. Programs that enable commerce include testing of gasoline pumps and weight scales.