DLWG Research and Evaluation of Existing Labeling Formats and Standards

The sections that follow provide the research and information that was identified over the course of the project. These details were discussed and reviewed for applicability to Canada and as discussion points at the meetings that were held over the project period. They are included here as a summary review and consideration for labeling requirements.

In order to provide more insight into the relative merits of the different types of labeling, it is useful to refer to critical research performed on well-established labeling schemes, particularly on the food labels and the energy efficiency labels.

Food and energy labels serve as particularly effective models for labeling schemes.[74] [75]

74 PETRAS IoT Hub, Rapid evidence assessment on labeling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

75 UCL Jill Dando Institute of Security and Crime Science, "Developing a consumer security index for domestic IOT devices (CSI), "17 January 2019.

Refrigerating appliances, as EEI									
A+++	A++	A+	A	B	C	D	E	F	G
<22	<33	<42/44	<55	<75	<95	<110	<125	<150	>150

FIGURE 1. ENERGY EFFICIENCY LABEL

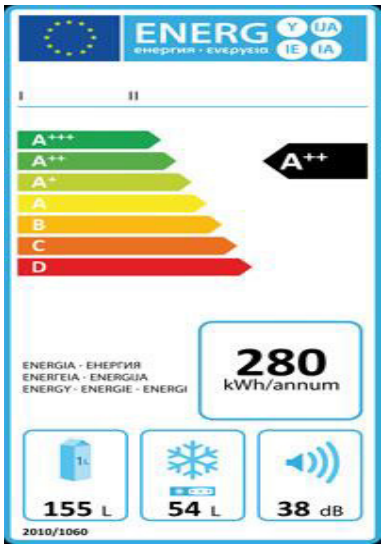


FIGURE 2. LABEL CATEGORIZATION FOR REFRIGERATORS

Energy Efficiency Labels

In 1995, the EU introduced the Directive 92/75/EC that was updated as Directive 2010/30/EU, outlining an energy consumption labeling scheme to be displayed on electronic products (Figure 1). In 2010, a grading scheme (A+, A++, and A+++) was introduced, following developments in energy efficiency standards. It is mandatory for manufacturers to display energy efficiency labels for certain classes of product, including refrigerators, televisions, and dryers.

The EU directive requires manufacturers to provide the labels for free to dealers, and include a performance table in brochures and associated documents.

A challenge for consumers in dealing with the energy efficiency label A+++ to G is that it is quite product dependent and not standardized. For example, television labels encompass from A+ to F, but coffee machines use a scheme from A to G. In 2010, all washing machines that were in label category A were prohibited. Then in order to drive market shift, all future washing machines needed to be in the A+ to A+++ range. These distinctions are generally invisible to the consumer and lead to confusion among product lines.

Also, the introduction of A+ to A+++ grading has undermined the efficacy of the label as it became difficult for consumers to differentiate between A+ to A+++ and A to G. Consumers are generally not willing to make the additional investment to buy an A+ or A++ rated product, and settle for an A product as good enough.

GDA LABEL

GDA LABEL WITH TRAFFIC LIGHT SYSTEM

Food Labels

As per the PETRAS report, food labeling enables consumers to make healthier food choices and reduce levels of obesity in the general public. The European Commission regulates the provision of food labeling, requiring pre-packaged foods to label their nutritional content (EC No. 1169/2011). Labeling on the back of a food package is mandatory for manufacturers, while labeling on the front-of-pack (FOP) is optional. FOP labels must display portion values for key risk areas (sugars, salt, fat, and saturates).

There are three types of FOP labels. The first is the Guideline Daily Amount[76] (GDA) shown below. The other figure shows the GDA scheme with colored traffic light system and is approved by the UK Food Standards Agency.[77] The third FOP type is a health logo, which is a "seal of approval" scheme, granted to a food product that is proven to meet particular nutritional requirements and/or standards (see below). This also shows the European Union organic food logo,[78] which came into effect in 2012, and is compulsory on all pre-packaged organic food products produced in the EU that meet specific standards.

76 https://www.foodlabel.org.uk
77 https://www.food.gov.uk
78 https://www.foodnavigator.com

EUROPEAN UNION ORGANIC FOOD LOGO

European Union organic food logo

Research has shown that the display of FOP labels has increased healthy product choice by eighteen per cent.[79] Little consensus exists on the most effective FOP labeling scheme. Research on GDA has shown that consumers find it difficult to identify the nutrient content, while more recent research has indicated that it helps consumers identify healthier products. On the other hand, a number of studies have shown that the traffic light FOP scheme facilitates more healthy food choices, compared to other FOP labeling schemes.[80] Health "seal of approval" logos are preferred by consumers due to their simplicity[81] and intuitive format, and have been found to reduce the time consumers spend in examining food packages.

In summary, there are clear benefits to a FOP label in aiding consumer choice, with each format offering its own strengths and limitations. Consumers tend to prefer a binary label; however, this may lead to poor decision-making, and research indicates that traffic light systems help consumers make better judgments and are marginally more effective in driving a healthier product choice.

The success of any of the food label schemes will be limited by the consumer's attention at the point of sale. Often, consumers are rushed and focus on trading off the brand, costs, convenience, and taste when making product choices.[82]

79 Cecchini M, Warin L. Impact of food labeling systems on food choices and eating behaviours: a systematic review and meta-analysis of randomized studies. Obes Rev. 2016;17:201–10. doi:10.1111/obr.12364

80 Id.

81 Id.

82 Szanyi JM. Brain food: Bringing psychological insights to bear on modern nutrition labeling efforts. Food and Drug Law Journal. 2010;65. http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/foodlj65&section=9. Accessed 24 May 2018.

QR CODES USED BY HP

STAPLES MOBILE MARKETING CAMPAIGN USING QR CODES

Relevant Use Cases for QR Codes

The use cases of QR Codes vary widely and cover different areas from marketing, product packaging, advertising, special causes, customer surveys, and much more. Below, three use cases of QR Codes are presented that focus on providing product information particularly in the ICT (information and communications technology) domain.[83]

HP Use Case

HP sought a practical and interactive way for customers to receive details on their products right from the package. They wanted potential customers to more easily understand what they were purchasing, and what accessories, like ink packages, were required for each.

HP used ScanLife activated codes extensively on most of their consumer printer line around the world. The codes told customers more about the products and gave them details on accessories which made it easier for shoppers to buy products, especially during the busy holiday season when retail associates were difficult to find.

Staples Use Case

Staples had a variety of goals for its mobile marketing campaign, including demonstrating value for the consumer while also helping the business achieve key sales milestones. The ultimate objective, however, was to increase overall conversions through the use of an effective in-store campaign. Staples incorporated QR Codes into its in-store displays.

83 Scanbuy, QR Codes Use Cases, http://www.scanlife.com/case-studies/

SELECTING KEURIG COFFEE MACHINES UTILIZING QR CODES

Keurig Use Case

Keurig wanted to give customers more dynamic information on all of their products, from K-Cup brewers to K-Cup flavours. Keurig used QR Codes as a flexible tool and centralized code management platform to work across multiple divisions within the organization. Dynamic codes were generated for Keurig products allowing the experiences to be adapted in real-time. Once scanned, the codes educate consumers on the product of interest: product information, a video tutorial of how the product works, and an explanation of why everyone should have a Keurig in their home or office. The campaign helps shoppers decide which Keurig brewing machine was best for them without interacting with sales associates.

Selecting Keurig coffee machines utilizing QR Codes

Standards and Best Practices

As multiple groups develop standards, the scope and jurisdiction of these documents may create confusion for consumers. Buyers must consider how they will use this product and the potential risks involved before determining the best documents to purchase. Currently, fragmentation and lack of industry wide collaboration on security and privacy across standards development organizations (SDOs) and trade associations is a problem not just in North America, but globally.

In the following table, we have included the key referenced standards by the DCMS report "Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security".[84] They are provided here for reference only as users will need a means to determine risks prior to purchase.[85]

84 Department of Digital, Culture, Media and Sport (DCMS), Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

85 Other recommendations and standards include NIST's definition of baseline IoT security recommendations, with conclusion expected out by the fall of 2019: https://www.nist.gov/sites/default/files/documents/2019/02/01/final_core_iot_cybers ecurity_capabilities_baseline_considerations.pdf, and the legislation passed by California and other states in the United States, most of which are focused on minimum guidelines.

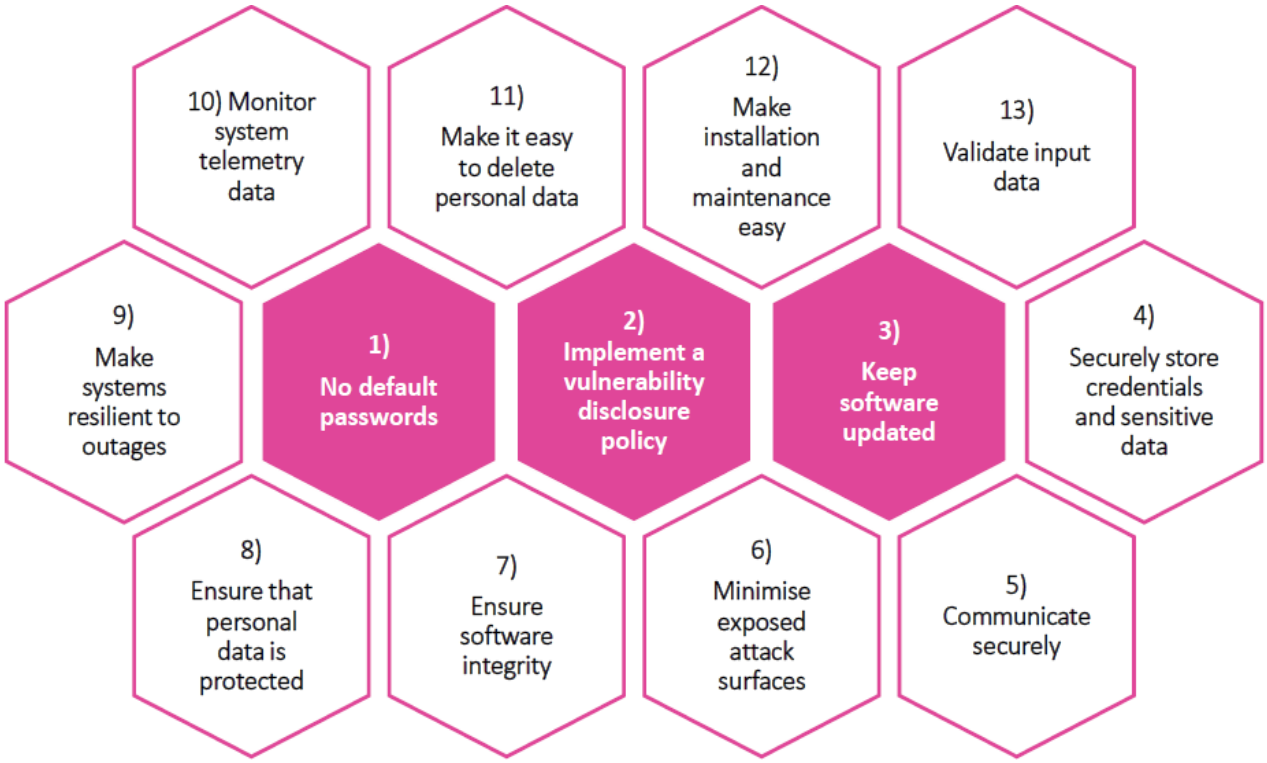
Organization	Standard/Recommendation
ETSI Technical Specification	Globally-applicable industry standard containing normative provisions for consumer IoT
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT
GSMA	IoT Security Guidelines for Service Ecosystems
IEEE	IoT Security Principles and Best Practices
Internet Engineering Task Force (IETF)	Best Current Practices (BCP) for IoT Devices
IoT Security Foundation	IoT Security Compliance Framework 1.1
IoT Security Initiative	Security Design Best Practices
Online Trust Alliance (OTA)	IoT Security & Privacy Trust Framework v2.5
U.S. Department of Homeland Security	Strategic Principles for Securing the Internet of Things (IoT)
U.S. House of Representatives	HR 1668 – Internet of Things (IoT) Cybersecurity Improvement Act of 2019 (Bill)
Alliance for Internet of Things Innovation (AIOTI)	Report on Workshop on Security and Privacy in the Hyper connected World
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations
CableLabs	A Vision for Secure IoT
IoT Security Foundation	Vulnerability Disclosure Best Practice Guidelines, IoT Security Compliance Framework 1.1
Broadband Internet Technical Advisory Group (BITAG)	Internet of Things (IoT) Security and Privacy Recommendations

Organization	Standard/Recommendation
Cloud Safety Alliance	Future-proofing the connected world: thirteen steps to Developing Secure IoT
European Commission and AIOTI	Report on Workshop on Security & Privacy in IoT
European Union Agency for Network and Information Security (ENISA)	Baseline Security Recommendations for IoT
Cloud Security Alliance (CSA)	Security Guidance for Early Adopters of the Internet of Things (IoT)
Industrial Internet Consortium (IIC)	Industrial Internet of Things Volume G4: Security Framework v1.0
IoT Security Initiative	CyberSecurity Principles of IoT
Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG)	State-of-the-Art and Challenges for the Internet of Things Security
Microsoft	IoT Security Best Practices
Open Connectivity Foundation (OCF)	OIC Security Specification v1.1.1
Open Web Application Security Project (OWASP)	IoT Security Guidance
Symantec	Strategic Principles for Securing the Internet of Things (IoT)
oneM2M	TR-0008-V2.0.1 Security (Technical Report)

The principles identified in the Code of Practice for Consumer IoT Security[86] are shown below.

Similar guidelines have been provided by the U.S. Department of Homeland Security in the "Strategic Principles for Securing the Internet of Things" report.[87] The IoT Alliance Australia (IoTAA) published a comprehensive report titled "Internet of Things Security Guidelines".[88] The IoTAA report identifies "the Trust Framework," whose requirements form the basis for evaluating an IoT system for best practices in security and privacy, and the basis of the IoTAA Security and Privacy Trustmark.

UK IOT CONSUMER CODE OF PRACTICE



86 Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

87 [17] U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

88 IoT Alliance Australia, Internet of Things Security Guideline, 2017, http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

BSI Kitemark for IoT Devices in the United Kingdom

In March 2018, the United Kingdom Government's Secure by Design review announced a series of measures to make connected devices safer to use.[89] The British Standards Institution (BSI) Kitemark builds on these guidelines by providing ongoing rigorous and independent assessments to make sure the device both functions and communicates as it should, and that it has the appropriate security controls in place. Manufacturers of Internet connected devices will be able to reassure consumers by displaying the Kitemark on their product and in their marketing materials.

There are three different types of BSI Kitemark for IoT Devices, which will be awarded following assessment according to the device's intended use: residential, for use in residential applications; commercial, for use in commercial applications; and enhanced, for use in residential or commercial high value and high-risk applications.[90]

The assessment process involves a series of tests that help ensure the device is fully compliant to the requirements. Before being awarded the Kitemark, the manufacturer is assessed against ISO 9001, and the product is required to pass both an assessment of functionality and interoperability, as well as penetration testing that scans for vulnerabilities and security flaws. Once the BSI Kitemark is achieved, the product will undergo regular monitoring and assessment including functional and interoperability testing, further penetration testing, and an audit to review any necessary remedial action. Importantly, if security levels and product quality are not maintained, the BSI Kitemark will be revoked until any flaws are rectified.

BSI Kitemark[91] provides comfort and confidence to users of products or services across a whole range of sectors. Recognition of the BSI Kitemark is high. Two thirds of all UK consumers associate it with quality, assurance, reliability, and trust. Ninety-three per cent of adults believe BSI Kitemark products are safer and seventy-five per cent say the BSI Kitemark will help make choosing between products easier.

Other Labeling Programs

It should be noted that other labeling programs are currently in development, such as Trustable Technology Mark a self-asserted mark covering broad aspects of IoT security and privacy.[92] The DLWG's research is not meant to be exhaustive, but rather to paint a picture of the existing IoT security labeling market.

89 UCL Jill Dando Institute of Security and Crime Science, "Developing a consumer security index for domestic IOT devices (CSI), "17 January 2019
90 British Standards Institution. BSI launches Kitemark for Internet of Things devices, 2018. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-Internet-of-things-devices/.
91 Id.
92 https://trustabletech.org/

IoT Product Testing in Australia

Another example of IoT product testing and certification is the process identified in Australia. IoT product manufacturers may wish to submit their products for testing by an accredited test laboratory, either under the National Association of Testing Authority (NATA) scheme or under the Australian Government in the Australasian Information Security Evaluation Program (AISEP). Formal testing will, if successful, result in the award of a test certificate and provide evidence of independent security assurance to customers.

Currently, there is no mandated requirement for security testing, but the high profile of cyber-attacks involving IoT devices makes this a key area of consideration for users. Having evidence that a device has been security tested will be a competitive advantage.

In order to provide security and privacy confidence in IoT devices designed, manufactured, or deployed in Australia, the IoTAA will release a security testing procedure based on the Online Trust Alliance Framework[93] which will be available for accredited organizations to use to recommend the issue of an IoTAA Security and Privacy Trustmark. There are currently three sets of published criteria that can be used for testing IoT devices:

1. The IoT Security Foundation has proposed a compliance scheme based on evaluation against their Security Compliance Framework. This is based on the DCMS code of practice. In addition, the IoT Security Foundation has proposed a compliance regime for demonstrating security in IoT devices and systems. This categorizes an IoT product into one of five classes: Class 0 to Class 4. Additionally, the ETSI TS 103 645 has been written so that manufacturers can test against the thirteen steps.

Class	Impact of Compromise	Confidentiality	Integrity	Availability
0	Minimal	Basic	Basic	Basic
1	Limited impact on an individual or organization	Basic	Medium	Medium
2	Significant impact on one or more individuals or organizations	Medium	Medium	High
3	Significant impact to sensitive data	High	Medium	High
4	Personal injury or damage to critical infrastructure	High	High	High

2. The Open Web Application Security Project (OWASP)[94] has developed a testing guide for IoT products. It covers sixteen IoT Principles of Security and provides a framework for testing ten different vulnerabilities.
3. The Online Trust Alliance (OTA) framework provides measurable requirements, which can be used as a starting point for selecting security-testing requirements.[95] The framework consists of eight categories of actionable principles: authentication, encryption, security, updates, privacy, disclosures, control, and communications. It also considers stakeholders who will have a collective responsibility for developing a secure solution.

IoT device manufacturers could select the relevant criteria for their device from these three documents, in addition to any device specific functionality not otherwise covered. These criteria will then form the Initial Claims Document for the security testing.

93 https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

94 Open Web Application Security Project (OWASP), Principles of Security, www.owasp.org/index.php/Principles_of_IoT_Security

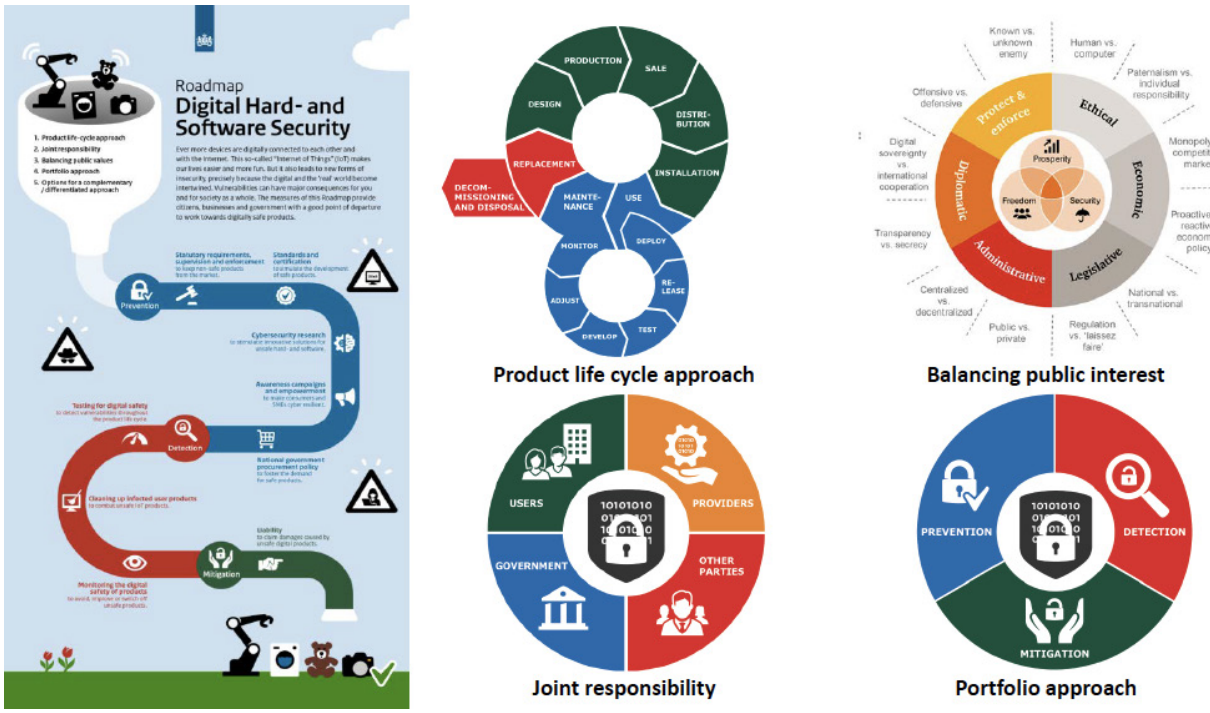
95 Online Trust Alliance (OAT), IoT Trust Framework, https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

IoT Product Certification in The Netherlands/European Union

As part of EU negotiations, the Netherlands is strongly promoting the rapid adoption of the Cybersecurity Act (CSA) and the active development of a European Cybersecurity Certification framework for ICT products and services.[96]

Moreover, the Dutch government supports the swift adoption of mandatory certification for specific product groups, i.e. products that present the greatest risk or the most problems in practice. In the long term, mandatory certification or compliance with a CE marking for all products with Internet connectivity should be implemented through gradual expansion.

ROADMAP FOR HARDWARE AND SOFTWARE SECURITY – THE NETHERLANDS



EU Framework: Security Certification of ICT Products and Services

The proposed Cybersecurity Act (CSA) is the European Commission's attempt to create, amongst others, a harmonized framework for the cybersecurity certification of ICT products and services within the EU. The absence of reciprocal agreements on standards and certification systems forms a barrier to creating a European market for cybersecurity products and services because it limits the scale for providers, reduces choice, and creates increasing uncertainty for procurers.

Common European certification of products and services will indicate that they are resilient (at a specified security level) to threats to their availability, authenticity, integrity, and reliability of data or of the functionalities and services being offered. The CSA aims to target fragmentation and foster the harmonization and mutual acknowledgment of cybersecurity certification at the European level.

Once a European certification framework has been adopted for a product or service, national government schemes will become redundant, and the Member States will no longer need to develop their own certification programs.

96 Ministry of Economic Affairs and Climate Policy, The Netherlands, Roadmap for Digital Hard-and Software Security, 2018, https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digital-hard--and-software-security

ETSI Cyber Security for Consumer Internet of Things Standard

The European Telecommunications Standards Institute (ETSI) published the "Cyber Security for Consumer Internet of Things" or the TS 103 645 V1.1.1 standard, in Feb. 2019.[97] This is certainly a major development into the direction of specifying globally applicable high-level provisions for the security of consumer devices that are connected network infrastructure such as the Internet or home network.

The standard document provides basic guidance for manufacturers involved in the development and manufacturing of consumer IoT on how to implement those provisions.

The thirteen high-level provisions identified in the standard document closely follow the principles identified in the Code of Practice for Consumer IoT Security.[98]

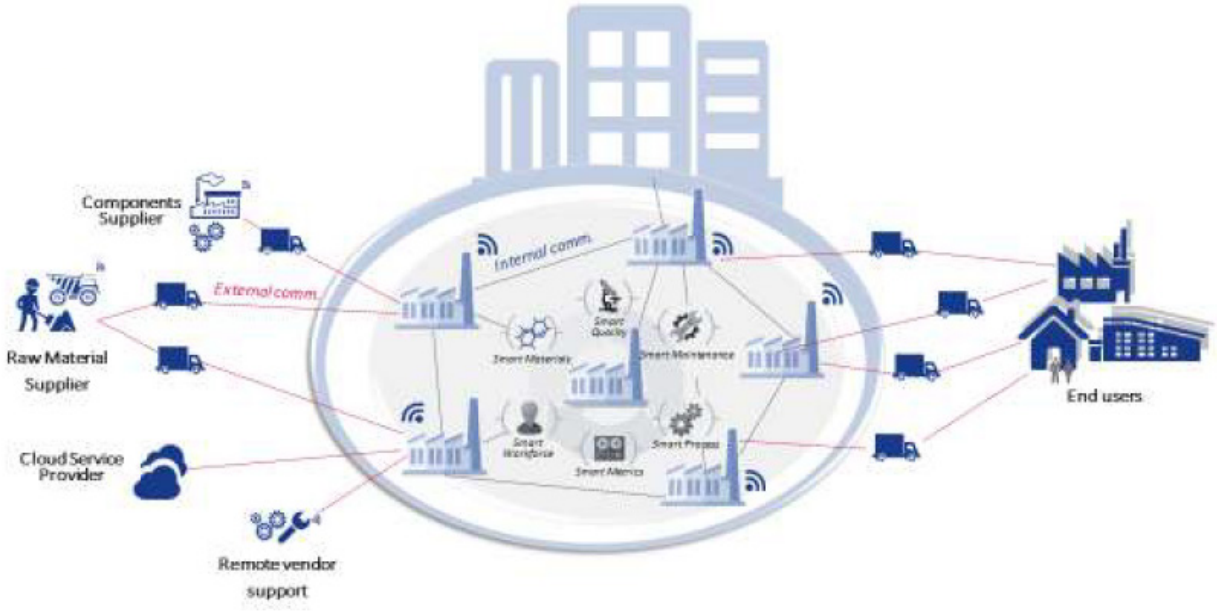
ENISA "Good Practices for Security of Internet of Things"

Towards the end of 2018, the European Union Agency for Network and Information Security (ENISA), which is a center of network and information security expertise for the EU, published a comprehensive report on "Good Practices for Security of Internet of Things," focusing on the context of Smart Manufacturing (Industry 4.0.).[99]

ENISA defines Industry 4.0 as "a paradigm shift towards digitalized, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT".

Industry 4.0 is gaining acceptance and is rapidly becoming a reality, making use of intelligent, interconnected cyber-physical systems to automate all phases of industrial operations. This evolution is spanning phases of design, manufacturing, and operations, with a great impact on consumers' and citizens' safety, security, and privacy due the extremely wide threat landscape, resulting from the cyber-nature and the inherent autonomy of Industry 4.0 and IoT.

COMMUNICATIONS RELATIONSHIPS IN INDUSTRY 4.0



97 ETSI, Cyber Security for Consumer Internet of Things, TS 103 645 V1.1.1, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

98 Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, https://www.gov.uk/government/publications/secure-by-design

99 ENISA, Good Practices for Security of Internet of Things, 2018, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

A key focal point of the ENISA report is the development of Security Measures for IoT in Smart manufacturing. The approach is to provide guidelines and recommendations for Operators, Manufacturers, and Users of Industrial IoT (IIoT). Applying these guidelines can help prevent or properly respond to potential cyber-attacks and ensure overall security and safety of the industrial IoT environment.

The recommendations and guidelines are classified into three main groups: Policies, Organizational Practices, and Technical Practices.

GOOD PRACTICES OVERVIEW

CTIA Cybersecurity Certification for IoT Devices in the U.S.

In 2018, the U.S. Cellular and Telecommunications and Internet Association (CTIA) published its Cybersecurity test Plan for IoT Devices.[100] This plan identifies testing requirements for CTIA Cybersecurity Certification of managed Internet of Things devices. In this case, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications module supporting either LTE or WiFi connectivity.

The test plan defines the Cybersecurity test that will be conducted by CTIA Authorized test labs (CATLs) on devices submitted for CTIA Cybersecurity Certification. An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. The device might include hardware, software, sensors, actuators, and network connectivity.

CTIA Cybersecurity Certification is defined in three categories. The first category identifies core IoT device security features, and the second and third categories identify security elements of increasing sophistication, complexity, and manageability.

While the test plan aims at ensuring compatibility across Cybersecurity systems through using the most widely adopted standards, it mandates a number of critical standards including: AES key size standards, end-to-end encryption standards, syslog standards, etc. An AES with a minimum of 128-bit key is expected by the test plan, to ensure interoperable cryptographic capability among all devices tested. However, devices may also support other algorithms and key sizes that provide the same or more cryptographic security.

100 CTIA, CTIA Cyber Security Certification Test Plan for IoT Devices, 2018, https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf

The table below provides an overview of the cybersecurity test cases per IoT device category:

CTIA IOT CYBERSECURITY TEST CASES

CATEGORY 1 IoT security features	Terms of Service and Privacy Policies
	Password Management
	Authentication
	Access Controls
	Patch Management
	Software Updates
CATEGORY 2 IoT security features	Cat. 1 IoT security features
	Audit Log
	Encryption of Data in Transit
	Multifactor Authentication
	Remote Deactivation
	Secure Boot
	Threat Monitoring
	IoT Device Identity
CATEGORY 3 IoT security features	Cat. 1 and Cat. 2 IoT security features
	Encryption of Data at Rest
	Digital Signature Generation and Validation
	Tamper Evidence
	Design-in Features

Canadian Standards Association (CSA) Group Cyber Verification Program

The CSA Group is currently developing a program and national standard that is aiming to address the product and organization security aspects. The Cyber Certification Program (CVP) consists of several aspects including a self-assessment, onsite audit, and formal product testing and evaluation. This program is built on the premise that an insecure organization cannot build a secure product. Security practices must be embedded into the organization's operations and development processes.

The assessment aspects consider six domains and eighteen practice areas within these domains. The current self-assessment consists of 198 binary questions that, once completed in connection with an audit, will provide a maturity rating for the organization.

The program has been field testing and has resulted in filing of a bi-national standard under Standards Council of Canada and the American National Standards Institute. This standard currently titled T-200 in Canada is currently under development. This will include the ability for vendor organizations to perform an attestation to this standard and as a maturity-based model it can use any recognized standard or best practice as the control for assessment.

Underwriters Laboratories (UL) 2900

UL has a series of standards that will formally evaluate a product against specific criteria to determine that the vendor is following and has correctly implemented the list of controls. These currently include medical products and devices. The testing and evaluation process is stringent and will provide buyers the assurance that formal testing, including penetration testing, has been conducted against a product.

ISO/IEC Standards

There are several standards that may be considered for products and organizations to determine their security posture. These may not necessary result in a label but a certificate of product or organizational testing and evaluation.

ISO/IEC 27001: A standard and certification process that will indicate that an organization has formally implemented and maintains an information security management system or ISMS. An ISMS is a formal system of process, procedures, and controls that identify and mitigate the risks associated with the organization. The controls are defined in the standard and guidance is provided on how to implement the necessary risk management framework within an organization.

ISO/IEC 9001: A standard and certification process that will indicate the process maturity of an organization in order to deliver a product or service. This includes an approach that states what they do, do what they say, and be able to prove it by creating process artifacts.

ISO/IEC 15408: Common Criteria is a formal product assessment methodology that provides assurance to product based on confidentiality, integrity, and availability. It can assess both hardware and software and is typically a requirement for government and higher security technology deployments. Objective testing uses an evaluation process that considers either the Evaluation Assurance Level (EAL) or Security Assurance Requirements (SAR) to provide the buyer with a rating that indicates whether the vendor meets a specific target level.

ISO/IEC 62443: This family of standards is focused on industrial and embedded systems. Organizations can target either assessing their products individually or having their entire SDLC program certified for any product/service being developed. With global recognition it does provide a means for a single level of assessment for a vendor to provide assurance of the security design practices. Given the complexity of this standard it is not necessary positioned for SMBs or start-ups but for more mature organizations with products. Due to the inherent costs of implementation and the required expertise it might be very difficult for SMBs to consider this standard.

CyberNB Cyber Essentials: This program is built on the UK program with the same title and objectives. The province of New Brunswick and several partners have adopted this framework as a means to validate that organizations have a minimum set of security requirements that they can demonstrate have been deployed. The focus is on IT controls within the organization and targets SMBs for deployment of these controls.

Potential labels by function

The list that follows provides some product categories and product labels that currently exist. While not foolproof, the labeling does provide a level of assurance that the vendor takes assessment and evaluation seriously. As such, these vendors have decided to obtain formal certification which indicates a level of business, process, and product maturity. These certifications are not a guarantee of security and privacy safety, but that the product has undergone a certain level of evaluation.

1. Home appliances
    a. Electrical certification: multiple CAN, US, and IEC standards.
    b. Security testing and evaluation: UL 2900 or equivalent.
    c. Attestation to CSA, CVP, or equivalent.
    d. Consumer Reports, BSI Kitemark, or equivalent.
    e. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.
2. Security and safety
    a. Functional safety certification to IEC 61508.
    b. Security testing to ISO 15408 *for mission critical environments.
    c. Security testing and evaluation UL 2900 or equivalent.
    d. Attestation to CSA, CVP, or equivalent.
    e. Consumer Reports, BSI Kitemark, or equivalent.
3. Lighting
    a. Electrical certification: multiple CAN, US, and IEC standards.
    b. Security testing and evaluation UL 2900 or equivalent.
    c. Attestation to CSA, CVP, or equivalent.
    d. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.
4. Entertainment
    a. Electrical certification: multiple CAN, US, and IEC standards.
    b. Security testing and evaluation UL 2900 or equivalent.
    c. Attestation to CSA, CVP, or equivalent.
    d. Consumer Reports, BSI Kitemark, or equivalent.
5. HVAC
    a. Electrical certification multiple CAN, US, and IEC standards.
    b. Functional safety certification to IEC 61508.
    c. Security testing and evaluation UL 2900 or similar.
    d. Attestation to CSA, CVP, or similar.
    e. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.

6. Utility
    a. Functional safety certification to IEC 61508.
    b. Electrical certification: multiple CAN, US, and IEC standards.
    c. Security testing and evaluation UL 2900 or similar.
    d. Attestation to CSA, CVP, or similar.
    e. 62443-3-1 or 62443-4-1 for embedded systems and vendor SDLC.

Regardless of the sector or product, there are two standards that an organization can target which will provide a level of process maturity for product quality and security management. These are ISO 9001 for a quality management system and ISO 27001 for an information security management system. A vendor that has one or both of these standards provides a higher level of assurance to a product with the necessary security controls deployed. An organization will have to balance business decisions and ensure full understanding of options and benefits to each standard.

Enforcement of Standards

Certification is neither a guarantee of product security nor privacy. Certification of any product or organization is based on a standard, usually international in context, which is used to conduct formal testing on a product or organization.

While under development, no standard for IoT controls currently exists that can be used to definitively address IoT security and privacy issues. As a result, other aspects can be evaluated under formal audit and product testing to validate whether both a company and product are being securely developed.

In addition, a company can falsify a label, and therefore buyers need to determine if a label has been counterfeited. This issue might be a bigger problem for consumers who are now being educated to trust labeling as an accepted means to determine assurance. The motivations for counterfeiting include costs, attempting to gain market share, or grey market goods. To better protect the buyer, labeling requirements should include a "live" portion to allow a potential buyer to determine the following:

1. A machine-readable code that will redirect the user to a live Internet portal (i.e. QR Code).
2. The Internet portal should contain the following as a minimum:
    a. Company name.
    b. Product.
    c. Current model version.
    d. Current firmware version.
    e. Current MUD file or equivalent version.
    f. Certifying company.
    g. Date of certification or last assessment.