Draft NISTIR 8200

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Prepared by the Interagency International Cybersecurity Standardization Working Group.

The Interagency International Cybersecurity Standardization Working Group (IICS WG) has developed this draft report based upon the information available to the participating agencies. Comments are being solicited in order to augment that information, especially on the information about the state of cybersecurity standardization for IoT that is found in Sections 8, 9, 10, and Annex D.

Reviewers are requested to submit comments to NISTIR-8200@nist.gov using the comment template at https://csrc.nist.gov/publications/detail/nistir/8200/draft. Comments will be posted at https://www.nist.gov/itl/comments-draft-nistir-8200 as they are received.

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

Draft NISTIR 8200

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Prepared by the Interagency International Cybersecurity Standardization Working Group.

NIST Editors:
Mike Hogan
Ben Piccarreta
Information Technology Laboratory

February 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency Report 8200
187 pages (February 2018)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *February 14, 2018* through *April 18, 2018*

National Institute of Standards and Technology
Attn: Information Technology Laboratory
100 Bureau Drive (Mail Stop 8900) Gaithersburg, MD 20899-8900
Email: NISTIR-8200@nist.gov

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

Reviewers are encouraged to use the comment template available at https://csrc.nist.gov/publications/detail/nistir/8200/draft. Comments will be posted at https://www.nist.gov/itl/comments-draft-nistir-8200 as they are received.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

The Interagency International Cybersecurity Standardization Working Group (IICS WG) was established in December 2015 by the National Security Council's Cyber Interagency Policy Committee (NSC Cyber IPC). Its purpose is to coordinate on major issues in international cybersecurity standardization and thereby enhance U.S. federal agency participation in international cybersecurity standardization.

Effective U.S. government participation involves coordinating across the U.S. government and working with the U.S. private sector. There is a much greater reliance in the U.S. on the private sector for standards development than in many other countries. Companies and industry groups, academic institutions, professional societies, consumer groups, and other interested parties are major contributors. Further, the many Standards Developing Organizations (SDOs) who provide the infrastructure for the standards development are overwhelmingly private sector organizations.

On April 25, 2107, the IICS WG established an Internet of Things (IoT) Task Group to determine the current state of international cybersecurity standards development for IoT. This Report is intended for use by the IICS WG member agencies to assist them in their standards planning and to help to coordinate U.S. government participation in international cybersecurity standardization for IoT. Other organizations may also find this useful in their planning.

Keywords

cybersecurity; cybersecurity objectives; cybersecurity risks; cybersecurity threats; IT; information technology; IoT; Internet of Things; IoT components; IoT systems; SDO; standards developing organizations; standards; standards gaps

Executive Summary

The Interagency International Cyber Security Working Group (IICS WG) was created in response to recommendations from NISTIR 8074 Volume 1 [1]. The IICS WG coordinates on major issues in international cybersecurity standardization. The IICS WG established an Internet of Things (IoT) Task Group to develop this Report on the status of international cybersecurity standards that are relevant to IoT.

The Internet of Things (IoT) consists of network connected devices, systems, and resulting services. The adoption of IoT and its applications is rapidly growing and the ensuing opportunities and benefits are significant. However, to reap the substantial benefits and to minimize the potentially significant risks, IoT security and resiliency are critical.

The timely availability of international cybersecurity standards is a dynamic and critical component for the cybersecurity and resilience of all information and communications systems and supporting infrastructures. The intended audience is both the government and public. The purpose is to inform and enable policymakers, managers, and standards participants as they seek timely development of and use of such standards in IoT components, systems, and services.

The Report relies upon terms and definitions that are defined in Annex A – Terms and Definitions of NISTIR 8074 Volume 2 [2], and rather than attempting to define "IoT," employs a functional description to establish a common understanding of IoT components, systems and applications for which the standards could be relevant. This analysis starts with a functional description of IoT components, which are the basic building blocks of IoT systems.

To gain insight on the present state of IoT cybersecurity standardization, five IoT technology application areas are described. These application areas are not exhaustive but are sufficiently representative to use in an analysis of the present state of IoT cybersecurity standardization. Connected vehicle (CV) IoT enables vehicles, roads, and other infrastructure to communicate and share vital transportation information. Consumer IoT consists of IoT applications in the residence as well as wearable and mobile devices. Health IoT processes data derived from sources such as electronic health records and patient generated health data. Smart building IoT includes energy usage monitoring systems, physical access control security systems and lighting control systems. Smart manufacturing IoT enables enterprise-wide integration of data, technology, advanced manufacturing capabilities, and cloud and other services.

Building upon NISTIR 8074 Volume 2, this Report describes eleven cybersecurity core areas and provides examples of relevant standards. IoT cybersecurity objectives, risks, and threats are then analyzed for IoT applications in general and for each of the five IoT technology application areas. Cybersecurity objectives for traditional IT systems generally prioritize Confidentiality, then Integrity, and lastly Availability. IoT systems cross multiple sectors as well as use cases within those sectors. As such, the priority of the individual's cybersecurity objectives may be prioritized very differently, depending on the application. The proliferation and increased ubiquity of IoT components and systems are likely to heighten the risks they present. Standards-based cybersecurity risk management will continue to be a major factor in the trustworthiness of IoT applications. Through analysis of the application areas, cybersecurity for IoT is unique and will require tailoring of existing standards, as well as, creation of new standards to address pop-up network connections, shared system components, the ability to change physical aspects of the environment, and related connections to safety.

With this foundational basis, this Report provides an analysis of the standards landscape for IoT cybersecurity. The basis for this analysis is the information in Annex D, which maps IoT relevant cybersecurity standards to the eleven cybersecurity core areas. The annotated listings in Annex D are not exhaustive but do represent an extensive effort to identify presently relevant IoT cybersecurity standards. The market impacts of existing standards are noted and possible gaps in standards identified. While the Annex D listing is a onetime snapshot, Annex D should prove useful as a point of departure for maintaining awareness of the evolving standards landscape. A summary on the status of cybersecurity standardization for the five specific examples of IoT applications is provided in Table 4: *Status of Cybersecurity Standardization for Several IoT Applications*.

The Report's conclusions focus upon the issue of standards gaps and the effective use of existing standards. For identified priorities, agencies should work with industry to initiate new standards projects in Standards Developing Organizations (SDOs) to close such gaps. In accordance with USG policy [3], agencies should participate in the development of IoT cybersecurity standards and, based upon each agency's mission, agencies should cite appropriate standards in their procurements. Also, in accordance with USG policy, agencies should work with industry to support the development of appropriate conformity assessment schemes to the requirements in such standards.

172 **Table of Contents**

List of Annexes

List of Figures

List of Tables

1 Introduction

The Internet of Things (IoT) has already changed the world for individual consumers and citizens, as well as for governments and industry. It is expected to be even more revolutionary and ubiquitous in the future. Yet, the adoption of IoT brings cybersecurity risks that pose a significant threat to the Nation.

The President's National Security Telecommunications Advisory Committee (NSTAC) has examined the cybersecurity implications of IoT within the context of national security and emergency preparedness (NS/EP). This examination "found that IoT adoption will increase in both speed and scope, and that it will impact virtually all sectors of our society. Additionally, the NSTAC determined that there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations [4]."

The President's Commission on Enhancing National Cybersecurity reached a similar conclusion: "The IoT facilitates linking an incredible range of devices and products to each other and the world. Although this connectivity has the potential to revolutionize most industries and many facets of everyday life, the possible harm that malicious actors could cause by exploiting these technologies to gain access to parts of our critical infrastructure, given the current state of cybersecurity, is immense [5]."

Our economy is increasingly global, complex, and interconnected. It is characterized by rapid advances in information technology (IT). IT products and services need to provide sufficient levels of cybersecurity and resilience. The timely availability of international cybersecurity standards is a dynamic and critical component for the cybersecurity and resilience of all information and communications systems and supporting infrastructures [6].

The growth of network-connected devices, systems, and services comprising the Internet of Things creates immense opportunities and benefits for our society [7]. However, to reap the great benefits of IoT and to minimize the potentially significant risks, these networked connected devices need to be secure and resilient. This depends in large part upon the timely availability and widespread adoption of clear and effective international cybersecurity standards.

2 Scope

This Report examines the current state of international cybersecurity standards development by voluntary consensus standards bodies for IoT [8].

This Report distills IoT down to the simplest concepts and describes the nuances associated with these concepts. It acknowledges but does not focus on specific technologies or concerns associated with IoT such as societal impact, safety, or privacy.

This Report recognizes that cybersecurity—and cybersecurity standards— can support individuals' safety and privacy. For example, cybersecurity standards when applied to the confidentiality, integrity, or availability of personally identifiable information (PII) are an important component of protecting individuals' privacy. However, privacy cannot be achieved solely by securing individuals' PII (see Figure 1). As noted in NIST Internal Report 8062, privacy concerns can arise from intentional or authorized processing of information about individuals, and in certain contexts, even measures used to secure PII can result in privacy issues [9].

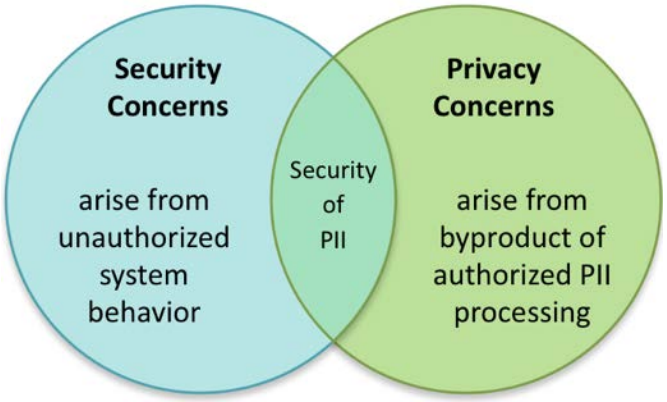


Figure 1 – Relationship Between Information Security and Privacy[1]

[1] Id. at 8.

3 Methodology

This Report uses terms and definitions as they are defined in Annex A – Terms and Definitions of NISTIR 8074 Volume 2, Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity, December 2015.

This Report:

- provides a functional description for IoT;
- describes several IoT applications that are representative examples of IoT;
- summarizes the cybersecurity core areas and provides examples of relevant standards;
- describes IoT cybersecurity objectives, risks, and threats;
- provides an analysis of the standards landscape for IoT cybersecurity; and
- maps IoT relevant cybersecurity standards to cybersecurity core areas (Annex D).

4 The Internet of Things (IoT)

IoT is a concept based on creating systems that interact with the physical world using networked entities (e.g., sensors, actuators, information resources, people).

There can be confusion around the meaning of the term "Internet of Things" for a variety of reasons. They include: the cross-cutting aspect of IoT (specifically with respect to application domains); the multitude of stakeholders involved in IoT and their specific use cases; the complexity of IoT; and the rapidly changing technology supporting IoT.

While there is no universal definition of IoT, common elements exist among the many high-level definitions and descriptions for IoT. A few IoT definitions and descriptions from other sources are listed in Annex A.

The Internet of Things consists of two foundational concepts:

- IoT components are connected by a network providing the potential for a many-to-many relationship between components (this network capability may or may not be TCP/IP based); and
- some of the IoT components have sensors and actuators that allow the components to interact with the physical world.

For the purposes of this Report, the following definitions apply:

Component: an entity that can interact with other entities to form systems that can achieve goals(s).

IoT component: a type of component that provides a network interface and therefore may be composed into IoT systems.

NOTE 1: IoT components are the basic building blocks of IoT systems.

NOTE 2: An IoT component has some combination of the following capabilities: [2] actuating, data storing, human user interface (UI), networking, network interface, processing, sensing, and supporting.

NOTE 3: Other publications use "IoT device" as a synonym for "IoT component" or define "device" as an actuator or sensor.

NOTE 4: An entire IT system can be an IoT component.

System: a set of components that interact together to achieve some goal.

IoT system: a system composed of IoT components or other, integrated IoT systems that

[2] A basic definition of a capability is the quality of being able to perform a given activity.

interacts with a physical entity of interest through sensors and actuators.

NOTE: IoT systems may also be IoT components if the IoT system provides a network interface.

IoT environment: a set of IoT components and supporting technologies that are networked together and can be built into IoT systems, which are also part of the IoT environment.

NOTE: An IoT environment is not a type of cyber-physical system.

As shown in Figure 2 below, the basic element of an IoT system is the IoT component. IoT components exhibit some combination of the five primary capabilities and three secondary capabilities shown. The five primary capabilities focus on the functionality the IoT component provides to the IoT system. The three secondary capabilities focus on how the IoT components work together. Some examples of capability functions are:

- Aggregation is part of a primary capability (i.e., processing) that provides the ability to combine and process some data of interest within a given IoT system.
- An Ethernet card is a part of a secondary capability (i.e., network interface) that provides the ability to connect different IoT components together within a given IoT system.
- Orchestration is part of a secondary capability (i.e., supporting) that allows the individual IoT components to interact together forming a system.

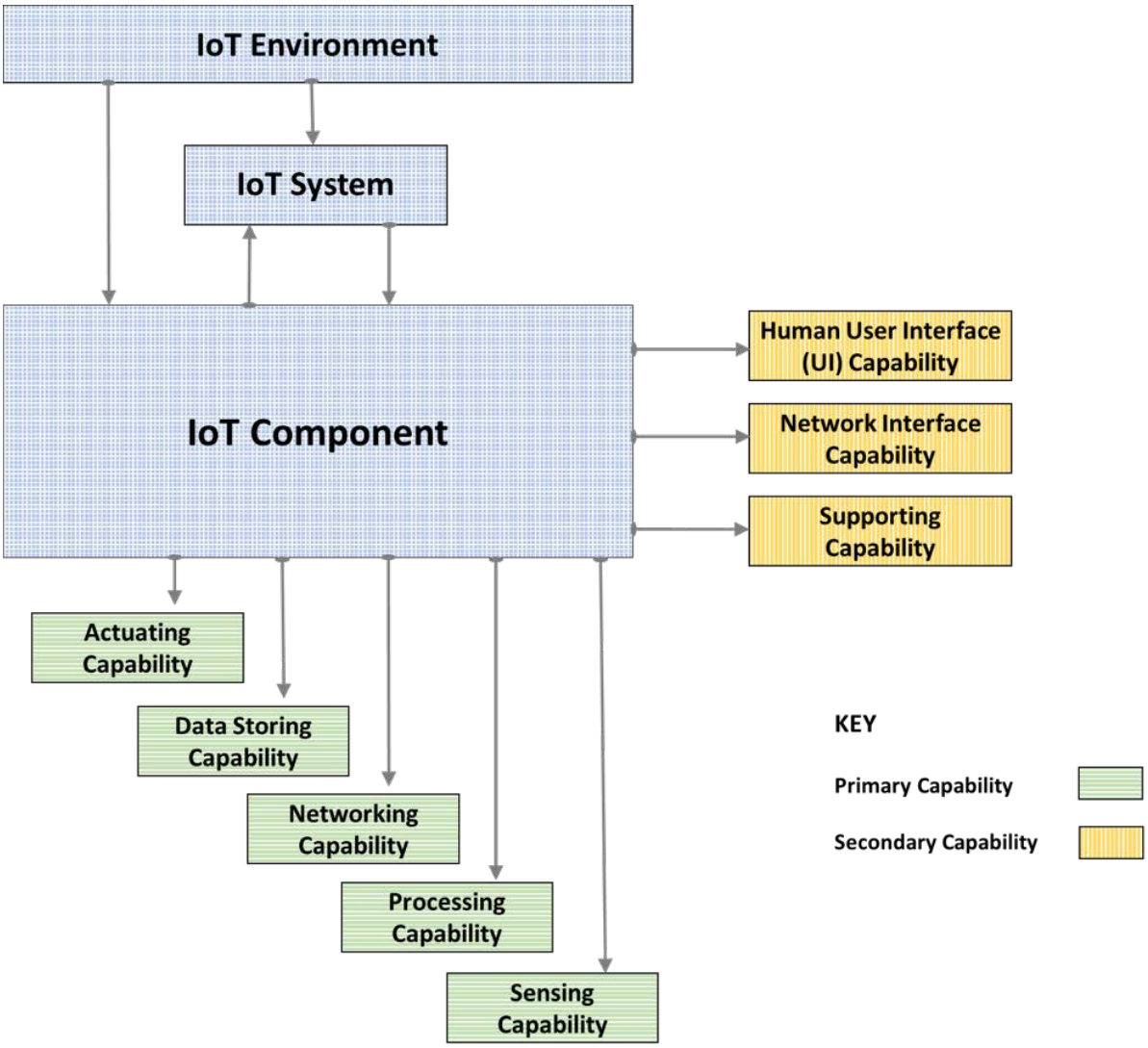


Figure 2 – Capabilities of an IoT Component.

An IoT system builder combines IoT components to create an IoT system that can meet a set of requirements. By understanding each IoT component as a set of capabilities, an IoT system builder can match those capabilities to the IoT system requirements. Using this capabilities viewpoint, an IoT component can be understood by the set of capabilities it provides. These capabilities are described below.

Primary Capabilities[3] of an IoT Component (which may also be an IoT system)

Actuating

The actuation capability provides the ability to make a change in the physical world. A black box control system that accepts a desired outcome as an input and uses internal sensors, actuators, and processors to make the physical changes to achieve the desired outcome would be

[3] See Appendix B Table 5: IoT Primary Capabilities Table.

considered an actuator in this model (since the model focuses on black box IoT components and their data inputs and outputs). Some other examples of actuation capability include: heating coil (heating capability), electric shock delivery (cardiac pacing), electronic door lock (lock/unlock capability), UAV operation (remote control), servo motors (motion/movement capability), and robotic arm (complex motion/movement capability).

Data Storing

The data storing capability provides the ability to store data and information over time. Some examples of data storing capability include storage of component input as well as the storage of component generated data. Electronic patient records are an example of this.

Networking

The networking capability provides the ability to move data from one physical or logical location to another. A component's network capability impacts the latency of information flow as well as the rate at which that information can flow. Some examples of networking capability include: Ethernet, Institute of Electrical and Electronics Engineers (IEEE) 802.11, and RS-422. Complex human operated surgical robots which incorporate haptic feedback and optical guidance are an example of sophisticated multi-mode networking.

Processing

The processing capability provides the ability to transform data based on an algorithm. The transformation may be very simple, with a single input variable and a single output, or it may be complex with multiple inputs and outputs. Control algorithms are an important type of processing that take the output of sensor(s) and actuator(s) or pre-processor(s) and provide an output that can be fed into an actuator or post-processor. These control algorithms often are used within negative feedback loops, but not always. A proportional-integral- derivative (PID) control algorithm is an example of such a control algorithm. Another example might be an algorithm which models the human insulin response in a real-time system that manages the function of an artificial pancreas.

Some additional examples of processing include: data aggregation capability and binary (Yes/No) analysis.

Sensing

The sensing capability provides the ability to sense an aspect of the physical or logical world. IoT components with sensing capability may acquire data in both analogue (e.g., a light sensor) or digital (e.g., a switch) form. Information about sensor observations may be provided to other IoT components through a networking capability for processing and storage or those capabilities may be native to the component. Examples include: temperature sensing (temperature measurement capability), CT scans[4](radiographic imaging), optical sensing, and audio sensing.

Secondary Capabilities of an IoT Component (which may also be an IoT system)

Human User Interface (UI)

[4] This illustrates the nature of complex sensing systems which can apply potentially harmful energy through actuators.

The human UI capability provides the ability for the component to interact directly with people. Not all IoT components will have a human UI capability (i.e., a dedicated processing component). These components will pass information to other system components in order to support the UI capability. Some examples of human UI capabilities include: optical and tactile display, and audio input and output.

Network Interface

The network interface capability provides the interface between communication network components necessary for communicating data between them. Every IoT component must have at least one network interface capability and may have more than one. While the network interface capability allows for a component to be connected to a communication network, it does not provide the communication (networking) capability. Some examples of network interface capability include: Ethernet adapter interface capability, long-term evolution (LTE) radio interface capability, and ZigBee radio interface capability.

Supporting

The supporting capability provides nonfunctional capabilities that support the main capabilities of IoT. Some examples of supporting capability include: encryption capability and authentication capability. IoT components performing sensing and/or actuating capabilities do not normally incorporate cryptographic controls (i.e. supporting capability) built-in so risk-adjacent-authentication is difficult unless additional engineering is implemented.

An IoT Component as a Black Box

From an IoT perspective, a "black box" viewpoint of each component is useful, because an IoT system builder may not have access to any details of the internal workings of an IoT component. In fact, the internal workings of a component may change over time. This is especially relevant for IoT systems of systems, in which components are comprised of other IoT components. When interfaces, capabilities, and limitations of a component are accurately and completely documented, including any details necessary for the system builder to map the component against capabilities to system requirements, the details of the inner workings may not be important. An IoT component that is documented in this manner provides the described capabilities within the described limitations, and can be easily integrated into systems, regardless of internal implementations. There are use cases where the internal workings of an IoT component may need to be completely documented and understood, including National Security Systems (NSS), and systems that carry a risk of injury or harm to an individual.

5 Examples of IoT Applications

For this Report, several significant IoT applications have been selected. They are considered to be sufficiently representative to use in the analysis of the present state of IoT cybersecurity standardization.

5.1 Connected Vehicles (CV)

Connected vehicle (CV) technology is expected to enable vehicles, roads, and other infrastructure to communicate and share vital transportation information. One proposed method for connecting vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) is dedicated short-range communications (DSRC), which is currently being studied by the Intelligent Transportations Systems Joint Program Office (ITS-JPO) at the U.S. Department of Transportation (DOT).

Figure 3 – Vehicle-to-Vehicle Communications [10]

DSRC is currently part of a CV pilot run by DOT. The expectation is that a vehicle will use DSRC to transmit its position, direction, and speed, as well as other information, to vehicles sharing the road. DSRC will also "talk" to equipment installed in the road itself and other infrastructure, such as traffic signals, stop signs, toll booths, work or school zones, and railroad crossings [11]. One concept implementation of DSRC has vehicles exchange Basic Safety Messages (BSM), which will be included with security credentials (see Figure 3, above). A possible alternative to DSRC is a technology concept called Visible Light Communication (VLC). LED lights are increasing being added to vehicles, and VLC can utilize these LED lights to communicate in the V2V and V2I scenarios.

The Security Credential Management System (SCMS) Proof-of-Concept (POC) is under development by the U.S. DOT. One of the objectives of this system is to support a subset of security needs for the CV Pilots Program. Therefore, each Pilot site must interface with and use the SCMS as part of its approach to address at least a subset of the Pilot's security requirements [12]. The goal of the SCMS POC design is to provide security services to support Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications at current passenger-vehicle production levels (up to 17 million annually) for the first year of deployment.

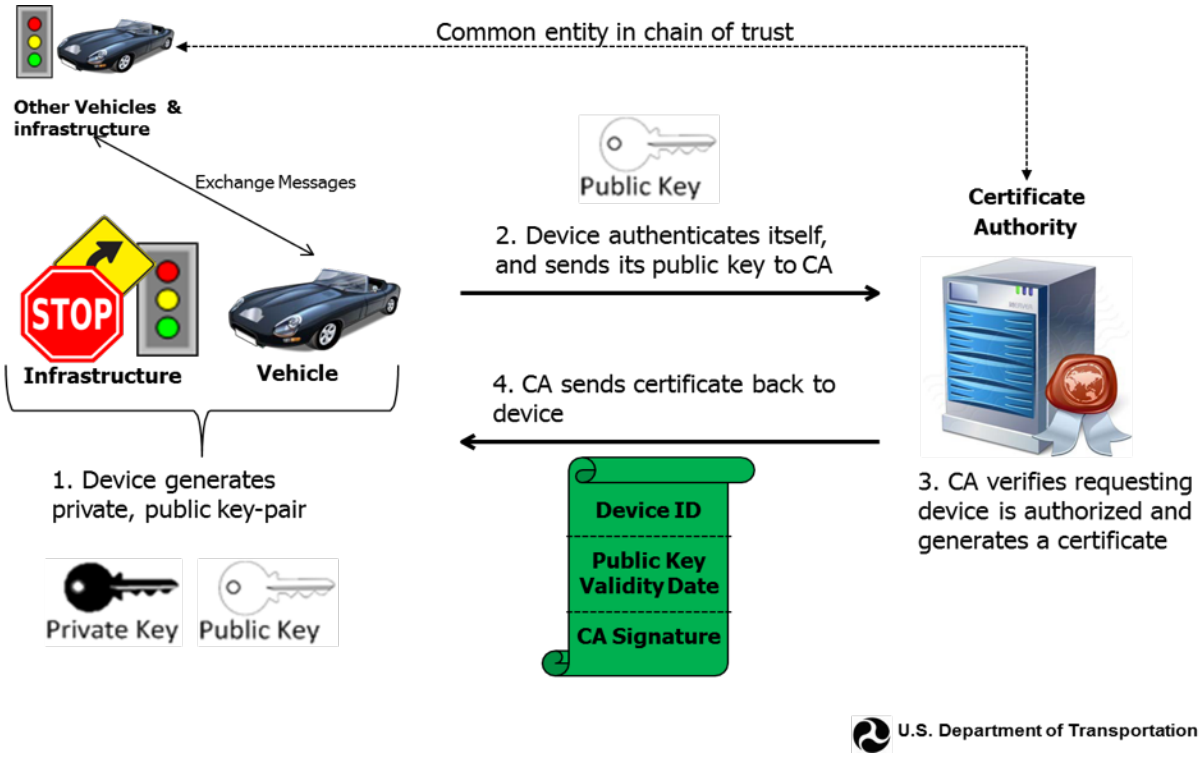


Figure 4 – V2X Public Key Infrastructure Overview [13]

An additional important goal of the SCMS POC system is to provide a flexible architecture that is capable of scaling to support larger numbers of V2V and V2I devices in the years following initial deployment [14]. The messages transmitted by vehicles are digitally signed to guarantee their integrity and authenticity. See Figure 4, above, for a vehicle-to-vehicle (V2V) and vehicle-to-infrastructure communication (V2I) (consolidated as V2X) Public Key Infrastructure overview.

Significant privacy and security challenges associated with both of these projects, including policies and laws governing the use of the information within BSM, as well as the implementation and governance of a central Certificate Authority, remain.

5.2 Consumer IoT

The consumer IoT includes all IoT applications for consumer products. In the residence, connected objects might include: thermostats, alarm systems, smoke detectors, doorbells, smart appliances (e.g., washers, dryers, refrigerators, ovens, televisions), door locks, door openers, and

smart lightbulbs. Wearables for consumer use, such as smart wristwear and smart fabrics, as well as implants, for applications such as consumer health or identification, are also part of the consumer IoT. Smart phones are often serving as the human user interface for these components, as are smart home assistants.

Home assistants are increasingly common. They can provide information, perform tasks, and control other IoT components. Home assistants often use conversational interfaces, but can also use text and images as input. These voice enabled user interface devices can be placed throughout a house. The ability to control these home assistants is included with every major smartphone operating system available today. The smart home assistant may connect and control some or all of the IoT components in the home.

Smart appliances can provide sensing and actuating capabilities, as well as a network interface. Examples include sous vide machines that can be remotely programmed and monitored, and refrigerators that alert the occupants when the milk is running low or the steak is going bad. A smart home security system may alert the home occupant to a burglary, high carbon dioxide levels, or a fire event, even if the occupant is not within the sounding alarm's range (likely done through text, email, or dedicated app). Smart homes may include systems for fire detection, monitoring and communication for fire suppression, and alerting first responders. Chore automation is a growing trend for IoT devices in the home. This is where autonomous home appliances and devices learn about users' behaviors and identify the best time to perform tasks autonomously. For example, a thermostat could be linked to the owner opening the garage door, adjusting the temperature to the person's liking. A refrigerator or kitchen cabinet may communicate with the smart phone to inform the owner of items that need to be purchased at the grocery store.

While the idea of converting a home's control over to smart devices could be attractive, consumers may be hesitant to embrace IoT-based systems if they feel that their privacy and data are at risk. The proper implementation of security within consumer IoT software, firmware, and hardware is often a neglected and overlooked priority. Securing IoT devices is a major challenge, and manufacturers tend to focus on functionality, compatibility requirements, and time-to-market rather than security. The adoption of consumer IoT devices is expected to explode in the near future. However, the increased popularity and acceptance by the consumer must be weighed against the security risks inherent to every device attached to a network.

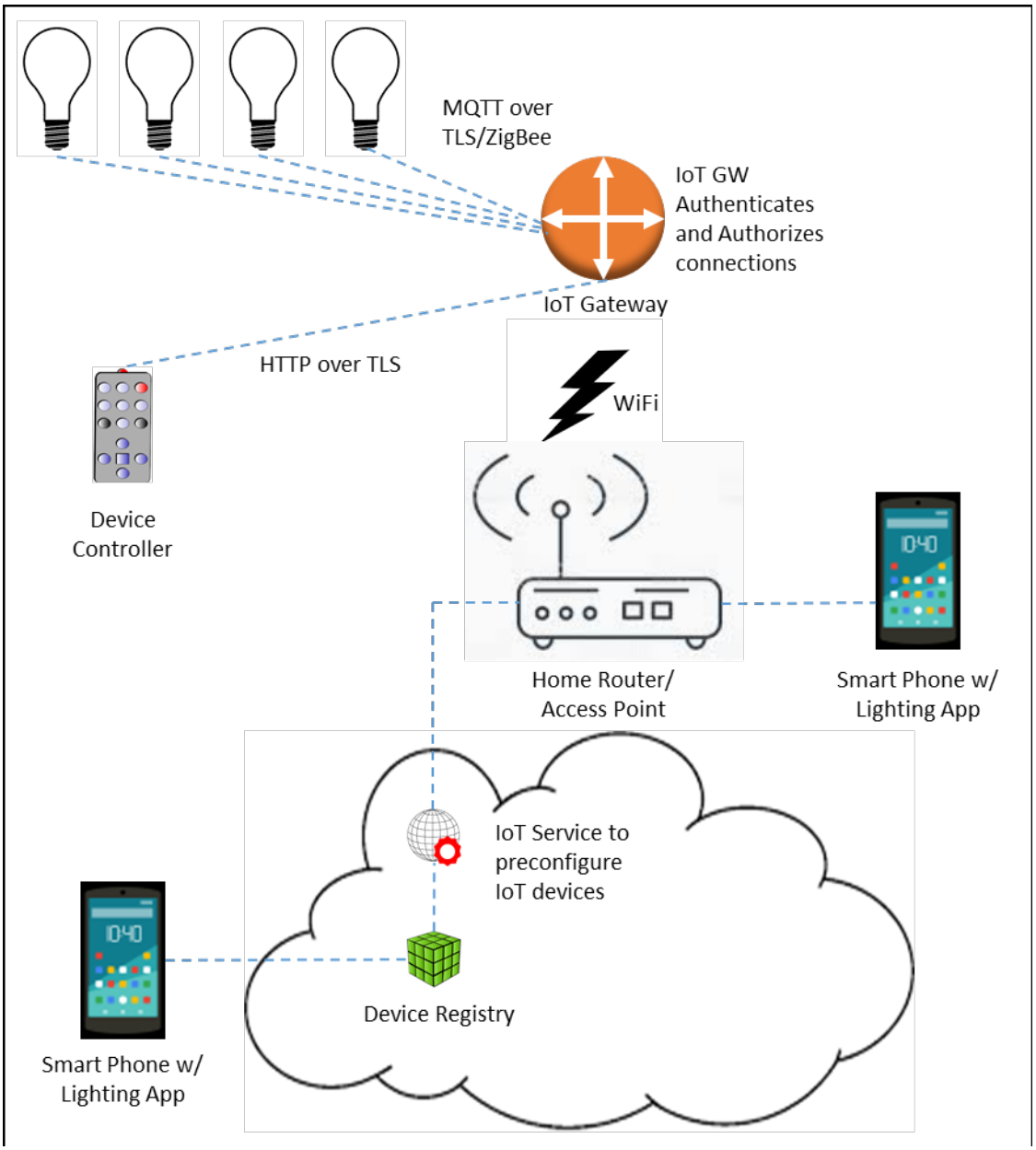


Figure 5 – Home Lighting Application

Consumers may not be aware of the far-reaching security vulnerabilities introduced by something as innocuous as connecting a smart LED bulb to the home network. A representative diagram for connecting a smart LED bulb to a home network is shown in Figure 5, above. Connecting a smart LED bulb illustrates typical network connectivity for a consumer IoT device. The smart LED bulb allows the homeowner, via either a smartphone or remote control device, to turn the bulb on or off as well as schedule its activation and deactivation. The homeowner can access web services to store configurations of color, illumination intensity, and activation/deactivation schedules. These web-stored configurations can be used to seamlessly restore operation after a power outage.

If a consumer IoT device becomes compromised, it can be a gateway into the broader network.

IoT threats could spread through networks and the Internet. By infecting a device and infiltrating one network, the threat can spread to an entirely separate network just by being in wireless range of another IoT device. In the particular case of a smart LED bulb, hackers in Wi-Fi™ range can learn Wi-Fi™ credentials sent in plain text and gain access to other systems and devices on the network and Internet. Possible attacks can range from spoofing connections to enabling malicious command and control of an IoT device by planting backdoors to create and launch an IoT distributed denial-of-service (DDoS) attack.

Consumers can gain many benefits from IoT devices, but it is misguided to implicitly trust these devices because they are connected to the home network. Securing IoT devices so that consumer privacy and data remains protected is a continuing challenge.

5.3 Health IoT and Medical Devices

IoT has recently gained traction by its spread from manufacturing to the electrical grid and other new sectors such as healthcare [15]. In the healthcare sector, health IoT gathers, transmits and analyzes data derived from sources such as electronic health records (EHR) containing personally identifiable information (PII), personal health records (PHR), patient generated health data, and other machine-generated healthcare data. Health IoT will support services like such as real-time monitoring, medication compliance, and imaging.

Characteristics of the Health IoT Environment

Health IoT is characterized by its objects, information resources, people, systems, and intelligent services. Table 1 illustrates some of the principal characteristics of the healthcare domain.

584 **Table 1 – Characteristics of the Health IoT Environment**

Objects	Information Resources	Systems	Intelligent Computing Services
• Home telehealth • Medical devices • Health and wellness products	• HL7 Fast Healthcare Interoperability Resource (FHIR) • Structural and semantic standards (vocabularies, code and value sets) • Actuators that receive commands • Personally worn physiological sensors	• Operations • Payment • Research (system of systems) • Personal health records • Treatment o Electronic health records o Monitoring o Treatment	• Learning Health System o Big data o High performance computing o Knowledge access o Natural language processing o Transformation o Longitudinal monitoring of patients progress o Adverse event monitoring o Translation
People			
• Patients o Patient representatives o Relatives o Health conscious individuals	• Licensed Healthcare Providers: o Audiologists, o Dentists o Dietitians o Optometrists o Physicians o Nurses o Technicians/ Technologists o Therapists	▪ Non-Licensed Healthcare Providers: o Administrative personnel o Aides o Emergency services o Interpreters ▪ Transport personnel ▪ Insurance payers	

585
586 **Use Cases**
587 Wireless telecommunications companies have developed smart sensors that support wearable
588 and implantable, injectable, and ingestible medical devices used in the healthcare industry, and
589 vendors have incorporated them into products such as insulin pumps, cochlear implants, and
590 pacemakers. Health IoT components talk to the Internet via a smart interactive interface
591 connected to the device's firmware [16]. The following use cases are representative of services
592 that can be provided by the emerging health Internet of Things.
593

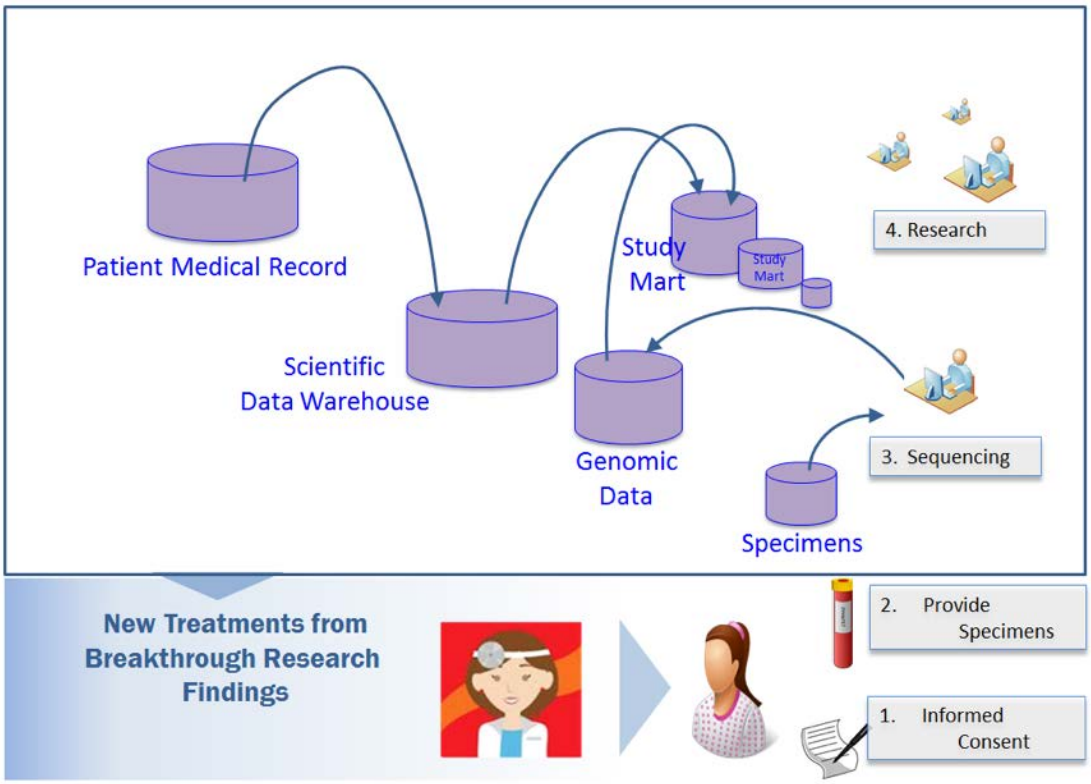


Figure 6 – Precision Medicine Research Case

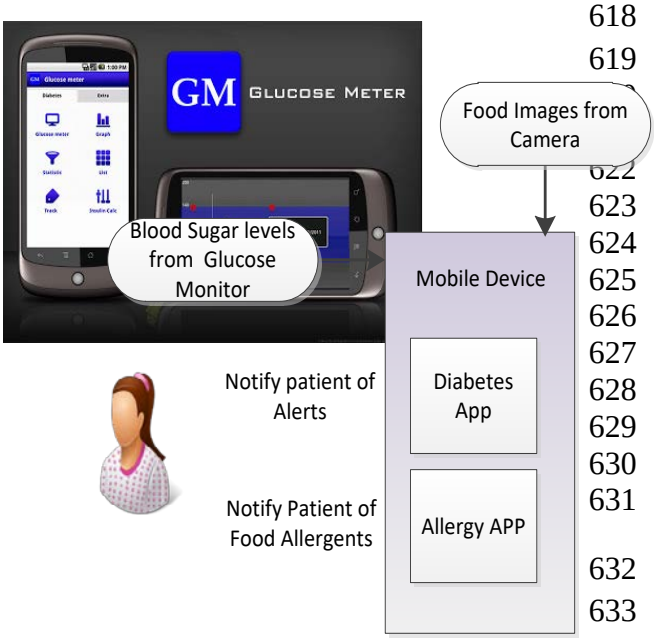
Precision Medicine (See Figure 6)

Precision Medicine and the Internet of things is driving market growth in healthcare [17]. According to the National Institutes of Health (NIH), **precision medicine** is "an emerging approach for disease treatment and prevention that takes into account individual variability in genes, environment, and lifestyle for each person [18]."

Alice is a disabled veteran who has been determined to have Hepatitis C [HCV] brought on by drug use related to combat induced stress. As normal treatments have failed, the VA wants her to participate in a large-scale hepatitis research program involving clinical trials of DNA matched treatments in an environment containing data from hundreds of thousands of other patients. Emerging standards for information sharing, such as Health Level 7's (HL7) Fast Healthcare Interoperability Resource (FHIR), provide Internet addressable information flow. Sequenced DNA from participant blood samples will be analyzed for efficacy of alternative Hepatitis treatments. Alice consents to participate in the clinical trial. She receives medicine reminders via cellphone or via an IoT enabled pillbox offering a wireless link to the patient, doctor, family members, and monitoring center. The pillbox helps to ensure Alice complies with the strict medication regimen times and sequences that are essential for the trial.

Diabetes Treatment (See Figure 7)

Alice has decided to travel outside of the United States but is diabetic and wants to monitor her blood glucose levels and receive updates on her condition from her primary care provider.



Alice has a wireless-enabled wearable glucose monitor and injection device. Advanced diabetes treatments being evaluated will be able to publish her blood sugar data for receipt by subscribing clinicians and intelligent computing technologies. Her clinicians, with assistance from intelligent computing technologies, will proactively evaluate and personalize her treatment, sending predictive alerts for hypoglycemia and insulin dosage updates.

Figure 7 – Diabetes Treatment/Allergen Identification

Nutrition control

While still on travel Alice needs assistance on the nutrition aspects of the local food. She downloads an App which can recognize the typical ingredients of many menu choices available to her and when presented at table can estimate the calorific and nutritional values from the photo image of her plate. This allows her to make more appropriate choices later in the day when she has her next meal. The App annotates what she consumes into her diabetes management app for the physician to monitor and study later.

The physician can see in near real-time how the consumed food selected affects the existing insulin response model algorithm stability and can suggest any necessary behavior changes by email.

5.4 Smart Buildings

The following GSA Smart Building Use Case is illustrative of the requirements for smart buildings in general.

The GSA Headquarters Building located at 1800 F Street NW, Washington, D.C., includes over 750,000 square feet of space, two-thirds of which has been modernized, and incorporates a variety of smart building technologies to help its occupants work comfortably, while improving energy efficiency and achieving various sustainability goals as mandated by the government. The various technology components, as implemented, form an integrated automated environment (see Table 2), that help building and facilities managers achieve their goals of occupant satisfaction, energy use intensity, maintenance costs, water usage, and CO_2 emissions.

656 **Table 2 – IoT Components for Intelligent Buildings**

IoT Components for Intelligent Buildings		
Infrastructure	**People**	**Combined Systems**
• Plumbing • Windows • Building wrap • Solar panels • Back-up power • HVAC • Waste control • Parking facilities • Elevators • Communication facilities • Rooms	• Tenants provide feedback on lighting and temp conditions via mobile app • Property managers share practices/know-how • Managers • Security guards • Maintenance/custodial crews	▪ Energy usage monitoring system ▪ Hoteling book-it system ▪ Card access and security system ▪ Weather station ▪ Occupant interface dashboard ▪ Lighting control system ▪ Universal control and monitoring system
Sensing	**Actuating**	**Computing**
• CCTV • IP video • Air quality • Water flow • Air temp • Humidity • Light • Door • Smoke/fire	• Door access • Elevator • Heater/AC • Fire alarms • Irrigation system • Window blinds	Processors/data stores • Databases • Servers • Cloud services • Edge devices Network • Ethernet • Fiber optics • Wi-Fi™ • Low power networks • Cellular

657

658 Scenario (illustrated in Figure 8): Before GSA staff begin arriving Tuesday morning, a Universal
659 Control system reviews its business rules and informs the HVAC system controller that a 20%
660 higher occupancy rate is expected. The system also checks the Hoteling Book-It system to
661 estimate power and ventilation demands of all pre-scheduled meetings. The HVAC system
662 initiates its cooling routines to compensate for the increased demand. As GSA staff and guests
663 arrive, the Card Access & Security System sends data wirelessly to the Universal Control system
664 that verifies that the rate of occupancy is within the projected arrival rate and no additional BTUs
665 are needed.

666

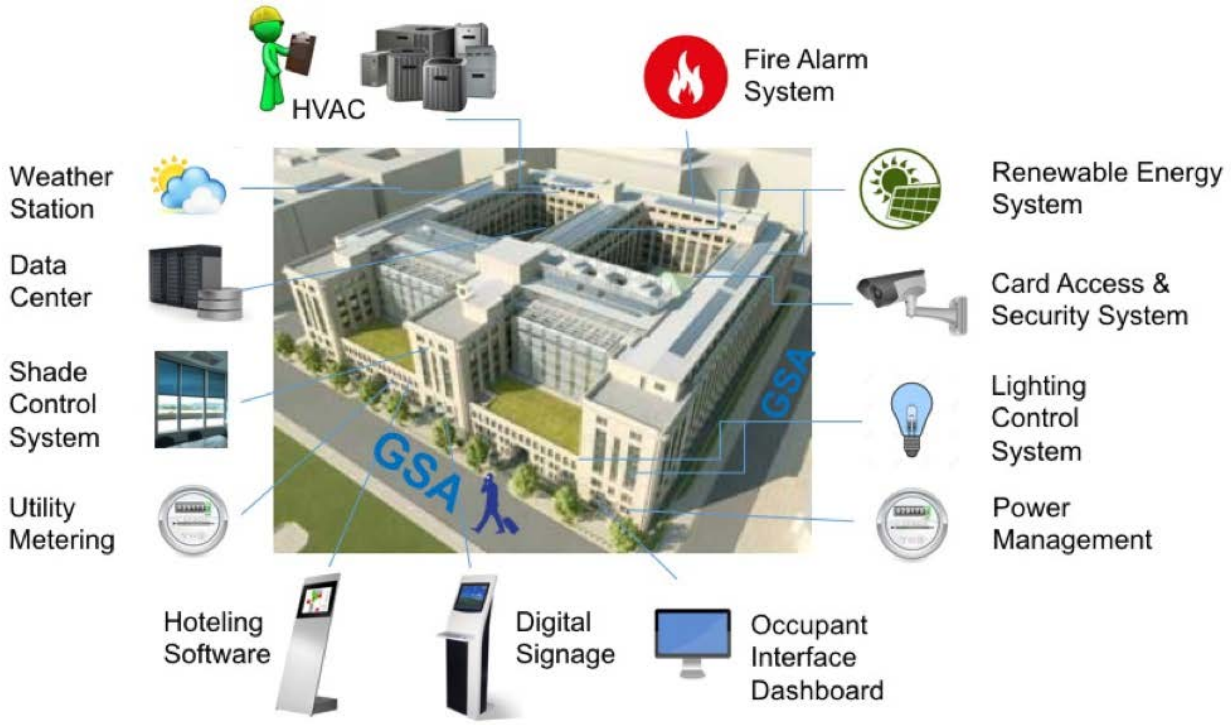


Figure 8 – IoT for the GSA Smart Building

At around 2pm, a significant cold front moves into the area. The building's Weather Station system, which is tied to the NOAA Internet Weather Service, detects the drop in the outside temperature and feeds that data to the Occupant Interface Dashboard, which controls the Window Switch Report and Shade Control system within each zone floor plan. As the outside cloud cover increases, the window shades are raised automatically and the interior lights are increased by the Lutron Lighting Control System. After a while, several users begin to complain that it is too cold. Individually, they open the building control app and submits their request to lower the temp in their area and increase the lighting. The system receives this feedback and averages the input from other users to make current adjustments, as well as record it for future adjustments.

By now, the meeting in GSA's largest conference room, reserved until 3pm, has ended. The Hoteling Book-It system notifies the Universal Control system, which verifies that lack of occupants. To conserve energy, the air conditioning is placed into standby state and lights are turned off until the space is occupied again. At the end of the day, the facility manager reviews the energy consumption for the day and checks tomorrow's meeting calendar. The dashboard alerts the manager of a large conference, with over 200 attendees, planned for tomorrow, starting with a 7am breakfast. The manager verifies that AC and ventilation will begin one hour earlier and adjusts the power metering to ensure plug loads are adequate for the A/V equipment and number of devices.

5.5 Smart Manufacturing[5]

Smart manufacturing environments will leverage enterprise-wide integration of data, technology, advanced manufacturing capabilities, and cloud and other services with new business models as shown in Figure 9. These technological developments are enabling product innovation, process efficiencies, customization, collaborative and/or distributed production, and other new modes and business models. However, strategies are still needed to comprehensively address security challenges brought about by this new industrial revolution, as these opportunities are revolutionizing attack capabilities as well.

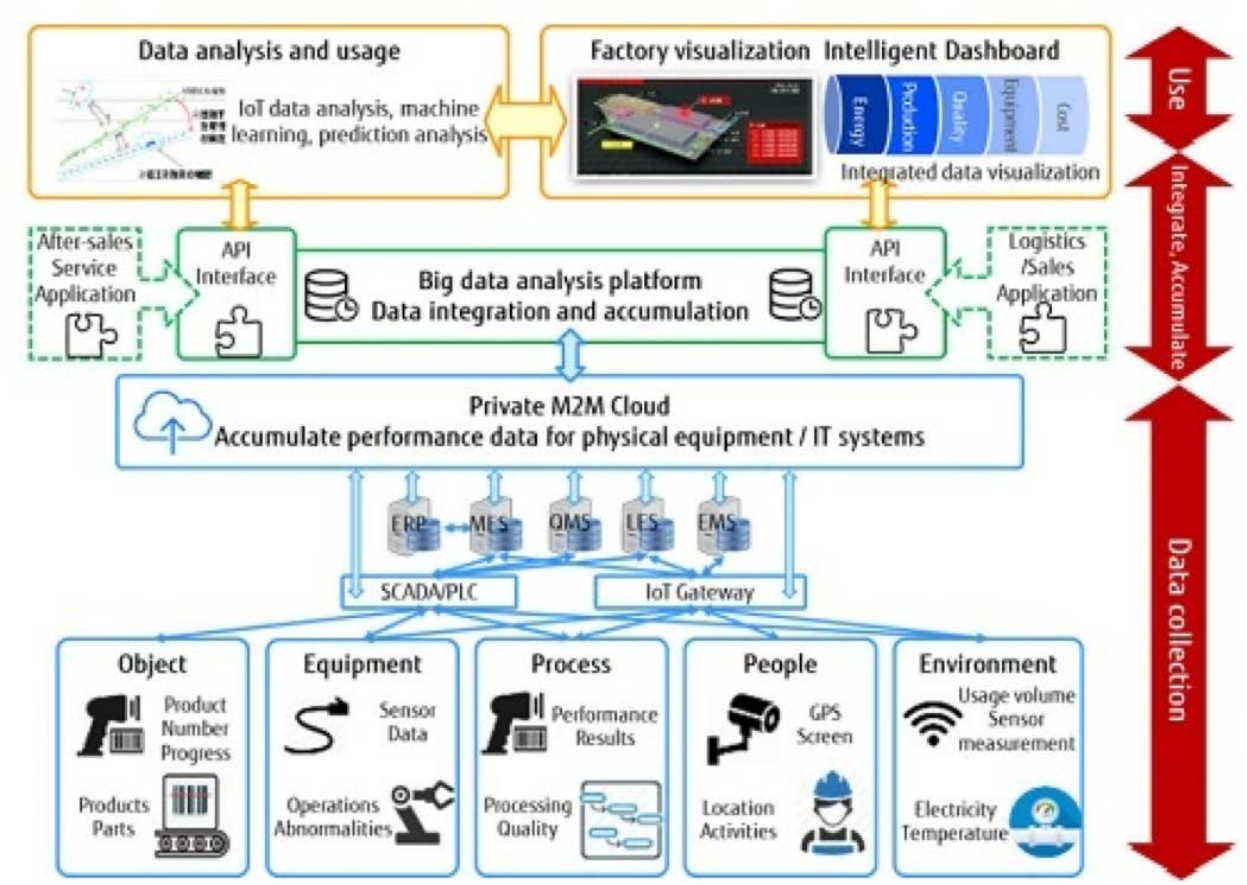


Figure 9 – Smart Manufacturing Environment

Securing smart manufacturing assets requires a comprehensive security model based on a well-defined set of security policies. Given the human-to-machine and machine-to-machine interfaces, a robust Security Management Plan must address technology, processes, and people (Figure 10). As security of organizations could be compromised at many layers, it is important to create a single point of contact (individual or office) to coordinate security matters and report incidents. Solutions are emerging that allow unified reporting to detect any threat to the application, process, or network, providing granular visibility of traffic and alerts to deviations from baseline

[5] content courtesy of NDIA CFAM effort – final paper under development

operations and facilitating attack forensics.

Figure 10 – Security Management Plan

Currently, smart manufacturing environments are custom solutions that are complicated, expensive, and built on proprietary communications. To achieve affordable plug-and-play capabilities, next generation hardware and software technologies need to work together through common security and communication standards. Standardization would lower the cost of entry to smart manufacturing for small and medium-sized businesses. In addition, as more cloud technology and Internet connectivity is leveraged toward the Industrial Internet of Things, it becomes imperative to assure the identity of the "things" in order to have secure exchanges of information. The IT to OT (Information Technology to Operations Technology) integration issue is solvable but needs standards of secure communication to leverage the Internet as the main gateway.

A distributed global manufacturing ecosystem increases the challenge of intellectual property protection. Engineers and operators are no longer under one roof but in different physical locations or countries. The process of black-boxing intellectual property could be the norm, so that no single entity has total exposure to the full process intellectual property. As some vendors start to shift from providing physical parts to providing digital code that the end-user purchases to make parts themselves, new business models and rules for protecting intellectual property will also emerge out of necessity. For example, a 3D printer file may need not only to be encrypted for security, but also may require provisions to restrict the number of allowable uses.

Smart manufacturing includes software and sensors that allow for precise predictions of maintenance needs, material demand, overtime, and other factors, based on data captured through all points of production. However, the volume of unstructured data that could be consumed in big-data projects creates new kinds of security challenges and requires a new

mindset toward data-centric security measures. Big data is too new for security personnel to understand what constitutes normal behavior. Security professionals need to comprehend the analytics and automation being applied to determine how best to protect a big-data enterprise, because there is currently no practical way to fully maintain situational awareness of the data at the accelerated rates of acquisition and change. With that level of understanding, organizations and vendors working in big data will continue to evolve their tools, techniques, and best practices, which will benefit smart manufacturing security.

Combining the advantages of big data and mobile devices, augmented reality (AR) is being used with increasing frequency on the shop floor in a number of ways, including as a training aid, maintenance aid, and operational dashboard. While the virtual overlay of information provides many benefits, it also opens up another vulnerable interface. For example, a hacker could compromise the output of an AR system, tricking users into thinking computer-generated objects are real. AR applications require access to a variety of sensor data such as video and audio feeds and geolocation; a malicious application could leak a user's field of view or location. AR solution vendors must address head-on the potential privacy and security risks that this technology can introduce. Some existing security controls and practices—such as encrypting wireless data transmissions—can serve to protect AR system inputs and outputs. Organizations need to have clear visions about how to overlay their existing security regimes onto the AR field.

A Cybersecurity Framework Manufacturing Profile, NISTIR 8183 [19], may help address some of the cybersecurity challenges associated with implementing IoT technologies in manufacturing environments. The CSF Manufacturing Profile has been developed for reducing cybersecurity risk for manufacturers in a way that is aligned with manufacturing sector goals and industry best practices. This Manufacturing "Target" Profile focuses on desired cybersecurity outcomes and can be used to identify opportunities for improving the current cybersecurity posture of a manufacturing system. This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

6 Cybersecurity Areas and IoT

6.1 Cryptographic Techniques

Cryptographic techniques are indispensable in securing IoT data and transactions. Cryptographic techniques and mechanisms and their associated standards provide: confidentiality, entity authentication, non-repudiation, key management, data integrity, trust-worthy data platforms, message authentication, and digital signatures.

Implementation of cryptographic techniques provide information assurance, which is built upon the following five pillars of data security:

- *Authentication*: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system;
- *Availability*: Ensuring timely and reliable access to and use of information;
- *Confidentiality*: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;
- *Integrity*: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and
- *Non-repudiation*: Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Of these five pillars of information assurance, four (authentication, confidentiality, integrity, and non-repudiation) are provided by cryptographic techniques that include encryption, digital signatures, and message authentication codes (MACs), which are a digital signatures that use the same key to generate the MAC as to verify it. Encryption provides confidentiality to data at rest and in transmission. A digital signature provides authentication, integrity, and non-repudiation, while MACs are used for integrity and data-origin authentication.

Cryptographic techniques do not directly provide availability; on the other hand, poor implementations of cryptographic techniques can significantly decrease availability of communication networks.

Encryption

Cryptographic algorithm standards have been widely available for some time. For example, the Advanced Encryption Standard (AES) block cipher, included in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3:2010, is the preferred block cipher for Institute of Electrical and Electronics Engineers (IEEE) 802.11 to secure wireless networks, and is required to implement in version 1.2 of the Internet Engineering Task Force's (IETF) Transport Layer Security (TLS) protocol.

Public key cryptography standards have also been widely available. The Internet Engineering Task Force has been developing public key cryptography standards for Internet applications. The IEEE 1363 working group has been publishing standards for public key cryptography including: IEEE 1363-2000, IEEE 1363a-2004, IEEE 1363.1-2008, IEEE 1362.2-2008, IEEE 1363.3-2013, and IEEE 1363-2013 Cor.

Lightweight cryptography standards are needed for emerging areas in which highly constrained devices are interconnected, typically communicating wirelessly with one another, working in concert to accomplish some task. Examples of these areas include: sensor networks, healthcare, distributed control systems, IoT, cyber-physical systems, and the smart grid. Security and privacy can be very important in these areas. Because most modern cryptographic algorithms were designed for desktop/server environments, many of these algorithms cannot be implemented in the devices used by these applications [20] .

Approved lightweight cryptography standards include:

- ISO/IEC 29192-1: 2012, *Information technology – Security techniques – Lightweight cryptography – Part 1: General*;
- ISO/IEC 29192-2: 2012, *Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers*;
- ISO/IEC 29192-3: 2012, *Information technology – Security techniques – Lightweight cryptography – Part 3: Stream ciphers*;
- ISO/IEC 29192-4: 2013, *Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques*;
- ISO/IEC 29192-4:2013/Amd.1: (2016), *Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques*; and
- ISO/IEC 29192-5:2016, *Information technology – Security techniques – Lightweight cryptography – Part 5: Hash-functions*

Digital Signatures

A digital signature is an electronic analogue of a written signature and provides assurance that the claimed signatory signed the information and that the information was not modified after signature generation. Digital signatures are used in in technologies including Connected Vehicle Systems and in cryptographic-enabled protocols such as IPSEC, S/MIME, and TLS. Example implementations include using digital signatures to authenticate from one machine to another, sign software/firmware to verify source and integrity, and sign PKI public key certificates. Common digital signature algorithms include:

- RSA with Public-Key Cryptography Standards (PKCS) 1 or probabilistic signature scheme (PSS) padding schemes;
- DSA (digital signature algorithm) (FIPS 180-4); and
- Elliptic curve DSA (ESDSA) (FIPS 186-4).

6.2 Cyber Incident Management

Cyber incident management standards support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident, and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.

While higher-level standards for cyber incident management are available, emerging low-level standards and implementations are under development that will facilitate the automated exchange of incident-related data such as indicators of compromise; tactics, techniques, and procedures (TTPs); threat actors; and courses of action. Existing standards include:

- ISO/IEC 27035:2016, *Information technology – Security techniques – Information security incident management – Part 1;*
- ISO/IEC 27035-2:2016, *Information technology – Security techniques – Information security incident management – Part 2*;
- ITU-T X.1056, *Security incident management guidelines for telecommunications organizations*;
- Payment Card Industry (PCI) Data Security Standard (DSS) v3;
- ISO/IEC 29147: 2014, *Information technology – Security techniques – Vulnerability disclosure*;
- ISO/IEC 30111: 2013, *Information technology – Security techniques – Vulnerability handling process*;
- IETF Request for Comments (RFC) 4765, *Intrusion Detection Message Exchange Format (IDMEF)*;
- IETF RFC 5070, *Incident Object Description Exchange Format (IODEF)*;
- IETF RFC 5901, *Extensions to the IODEF for Reporting Phishing*;
- IETF RFC 6545, *Real-time Inter-network Defense (RID)*;
- *OASIS Structured Threat Information Expression (STIX) Version 2.0*; and
- *OASIS Trusted Automated Exchange of Indicator Information (TAXII) Version 2.0*.

IT cyber incident management procedures are relatively well understood. For industrial control systems (ICS), the procedures are not so well understood, specifically related to what critical infrastructure organizations should do in the event of a cyber incident. Shutting down a continuously operating plant has its own risks—commercial and safety—and careful consideration and consensus are required to identify scenarios and recommended courses of action.

6.3 Hardware Assurance

Hardware assurance is an activity to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.

Existing standards include:

- ISO/IEC 15408 *Information technology – Security techniques – Evaluation criteria for IT security* (three parts);
- ISO/IEC 20243:2015 *Information technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains*;

- ISO/IEC 27036 *Information technology – Security techniques – Information security for supplier relationships* (three parts);
- SAE International AS5553B-2016 *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria*; and
- SAE International AS6081-2012 *Counterfeit Electronic Parts; Avoidance Protocol, Distributors*.

6.4 Identity and Access Management

Identity and access management and related standards enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.

Significant identity and access management standards are included in risk management techniques and specifications to assert identity and authentication, as well as enforce access policy on a range of platforms. Mature enterprise standards such as Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML) and the family of Public Key Infrastructure (PKI) cryptographic techniques to authenticate users and devices are widely deployed and in use in the cloud-computing key IT application. Emerging standards are being developed to abstract authentication form factors away from applications, allowing a rich set of strong credentials to be interoperable online.

Risk-based approaches to determine assurance levels required to protect online transactions, and the associated technical and procedural controls, have been adopted at the federal level and similar standards ratified within international standards organizations. However, international government identity programs are developing their own standards and guidelines rather than adopting a smaller set of existing standards. In the private sector, industry has developed profiles to meet the needs of their business model and partners, as well as their risk tolerance, but there is not agreement among organizations as to which identity assurance standard is the most holistic and therefore capable of being adopted cross-industry.

Standards to enforce access policies, share attributes, preserve anonymity, minimize data release, and consent are still immature, difficult to deploy, and not available by a large majority of software-as-a-service providers and traditional enterprise product vendors, additionally hampering adoption.

Health information technology (health IT) [21] is standardizing authentication, consent, and authorization to medical records across patients, providers, insurers, and research entities to secure use and sharing of health information.

With the increase of commercial and enterprise Internet-connected devices (such as IoT

components), standards for device identity, outside of traditional PKI, are just being researched, but the market has yet to determine what, if any that exist, will be leveraged.

PKI architecture for privacy: PKI is traditionally implemented to provide a trusted identity to either an individual or device. However, the ability to remain anonymous and to not be tracked while operating in network and RF environments is becoming more and more important.

6.5 Information Security Management Systems (ISMS)

Information security management system (ISMS) standards provide a set of processes and corresponding security controls to establish a governance, risk, and compliance structure for information security for an organization, an organizational unit, or a set of processes controlled by a single organizational entity. An ISMS requires a risk-based approach to security that involves selecting specific security controls based on the desired risk posture of the organization and requires measuring effectiveness of security processes and controls. An ISMS requires a cycle of continual improvement for an organization to continue assessing security risks, assessing controls, and improving security to remain within risk tolerance levels by balancing security and risk tolerances.

The ISO/IEC 27000 series provides best practice recommendations on information security management, risks, and controls within the context of an overall information security management system. The fundamental parts of this series are broadly applicable to IT systems and applications.

Because of some distinctive attributes of cloud computing, several standards have been approved or are under development for cloud computing applications. These include:

- ISO/IEC 27017:2105, *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*;
- ISO/IEC 27036-4;2016, *Information technology – Information security for supplier relationships – Part 4: Guidelines for security of Cloud services*;
- ISO/IEC 27018:2014, *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*;
- ISO/IEC DIS 19941 *Information technology – Cloud computing – Interoperability and portability*; and
- ISO/IEC FDIS 19944 *Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use*.

There is a sector-specific technical report (TR) for smart grid:

- ISO/IEC TR 27019:2013 (1st edition), *Information security management guidelines based on ISO/IEC27002 for process control systems specific to the energy industry*.

There is one standard for business continuity that is relevant to emergency management:

- ISO/IEC 27031:2011 (1st edition), *Guidelines for information and communications technology (ICT) readiness for business continuity*.

The ISA/IEC 62443 series of Industrial Automation and Control Systems (IACS) standards and technical reports includes security management requirements.

- ISO/IEC 20243:2015 *Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products* identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains.

More specific standards have been and are being developed to augment existing portfolios, such as the 27000-series.

6.6 IT System Security Evaluation

IT system security evaluation and assurance standards are used to provide: security assessment of systems, security requirements for cryptographic modules, security tests for cryptographic modules, automated security checklists, and security metrics.

There is a growing portfolio of standards for testing and validation of cryptographic modules that are being widely applied. Approved standards include:

- ISO/IEC 19790:2015, *Security requirements for cryptographic modules*;
- ISO/IEC 24759:2014, *Test requirements for cryptographic modules;*
- ISO/IEC 17825:2016, *Information technology – Security techniques – Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*; and
- ISO/IEC 18367:2016, *Information technology – Security techniques – Cryptographic algorithms and security mechanisms conformance testing*.

A technical report is also published: ISO/IEC TR 30104:2015, *Physical security attacks, mitigation techniques and security requirements*.

Standards under development include:

- ISO/IEC CD 20085-1, *Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules – Part 1: Test tools and techniques*;
- ISO/IEC CD 20085-2, *Test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules – Part 2: Test calibration methods and apparatus*;
- ISO/IEC DIS 19896-1, *Information technology – IT Security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements*; and
- ISO/IEC CD 19896-2, *Information technology – Security techniques – Competence requirements for information security testers and evaluators – Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers*.

Standards for the security assessment of systems have been revised several times. These include the three-part standard ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security*.

In addition, certain process evaluation programs should be considered. One program for mitigating the risk of maliciously tainted and counterfeit parts in IT products, to help assure security and integrity in these products, is *ISO/IEC 20243-2:2018 Information technology -- Open Trusted Technology Provider™ Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products -- Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018*. As noted under the ISMS core area above, this standard identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains. While it does not cover product evaluations, it does provide for process evaluation. Such evaluations determine if a technology provider, component supplier, or distributor meets all the process requirements in the standard throughout a product's life-cycle (design through disposal). This would include the product development and secure engineering methods they use and the supply chain security they provide.

These above standards are broadly applicable to the evaluation of security properties of IT products.

6.7 Network Security

Network security standards provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.

IoT networks are deployed over a multitude of protocols and physical links. Selecting the appropriate messaging and communication protocols depends on the use case and security requirements for each system.

One characteristic of IoT is the potential for spontaneous connections (due to the networking) without a system view. Viewed in this way the IoT could not be 'planned' nor secured well using traditional approaches to security since system compositional or emergent properties would never be seen by a risk manager. The network interfaces in these loosely coupled systems represent attack surfaces. Therefore, without a system asset definition and subsequent threat analysis the security design is very unlikely to be useful.

Annex D lists the standards of the common protocols that support IoT communications and establish the security of the underlying network connections. These protocols extend over the Open Systems Interconnection (OSI) layers, i.e., physical, link, network, transport, and application layers.

Many standards developers have developed and are developing network security standards. The IETF developed RFC 2196 provides a general and broad overview of information security including network security, incident response, or security policies. IETF Security Area Working Groups include: IP Security Maintenance and Extensions, Kitten (GSS-API Next Generation), Managed Incident Lightweight Exchange, Network Endpoint Assessment, Open Authentication, and Transport Layer Security.

ISA/IEC-62443 standards series define procedures for implementing electronically secure industrial automation and control systems.

The IEEE standard, 802.11i-2004, implemented as Wi-Fi™ Protected Access II (WPA2). This amendment to IEEE 802.11 defined TKIP and CCMP, which provided more robust data protection mechanisms than WEP affords. The current version of IEEE 802.11 is IEEE 802.11™-2016 : *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.

6.8 Security Automation and Continuous Monitoring (SACM)

Security Automation and Continuous Monitoring (SACM) standards describe protocols and data formats that enable the ongoing, automated collection, monitoring, verification, and maintenance of software, system, and network security configurations, and provide greater awareness of vulnerabilities and threats to support organizational risk management decisions. Automation protocols also include standards for machine-readable vulnerability identification and metrics, platform and asset identification, actionable threat information and policy triggers for actions to respond to threats and policy violations. Automated activities would include a security operation center (SOC) to ensure autonomous and continuing monitoring and evolution of the security state of assets based upon prescribed events.

While higher level standards for security automation and continuous monitoring are available and low-level specifications and implementations are in use, they require maturation and shepherding through international standards developing organizations.

Existing standards include a large body of work under ISO/IEC, IETF, and industry-led efforts (e.g., Cloud Security Alliance, Health Information Trust Alliance [HITRUST], North American Electric Reliability Corporation [NERC] Critical Infrastructure Protection [CIP]) related to asset, configuration, and vulnerability management—the underpinning of a continuous monitoring capability. Other standards include those being developed by the IETF Security Automation and Continuous Monitoring (SACM) Working Group.

As with incident management, IT security automation and monitoring is relatively well developed. Security automation and continuous monitoring is much more difficult to implement in ICS. Disruption of finely balanced network communications timing and the lack of in-depth understanding of industrial communications protocols are two major limiting factors that will need to be addressed before this security barrier is more widely used.

6.9 Software Assurance

Software assurance standards describe requirements and guidance for significantly decreasing the likelihood of software having vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web,

software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.

It is important to have in place software assurance standards that provide assurance over the full lifecycle of software. Software assurance across the life cycle includes threat modeling, use/misuse cases, secure design, defensive design, and secure coding expectations that can be validated using source code and binary analysis techniques. The integrity of the code is also considered an aspect of software assurance. ISO/IEC 19770-2:2015, *Information technology – Software asset management – Part 2: Software identification tag*, can be used to identify software, measure the integrity of software distributions and installations, and to detect and manage missing software patches for deployed software. Further work is needed to either apply this existing standard to cloud deployments or to identify additional approaches that address software and service deployments in cloud scenarios. Other relevant standards include:

- ISO/IEC 27034-1:2011 *Information technology -- Security techniques – Application security*
- ISO/ IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships (Part 1: Overview and concepts)*;
- ISO/ IEC 27036-2:2014, *Information technology – Security techniques – Information security for supplier relationships (Part 2: Common requirements)*;
- ISO/ IEC 27036-3: 2013, *Information technology – Security techniques – Information security for supplier relationships (Part 3: Guidelines for ICT supply chain security)*;
- ISO/IEC 20243:2015 *Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*;
- SAE International AS5553, *Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*;
- SAE International AS6462A - AS5553A, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria*;
- ISO/ IEC 27035, *Information technology – Security techniques – Information security incident management*;
- ISO 3011, *Information technology – Security techniques – Vulnerability handling processes*; and
- ISO/IEC 29147:2014, *Information technology – Security techniques – Vulnerability disclosure*.

6.10 Supply Chain Risk Management (SCRM)

Supply chain risk management (SCRM) standards provide the confidence that organizations will produce and deliver information technology products or services that perform as required and mitigate supply chain-related risks, such as the insertion of counterfeits and malicious software, unauthorized production, tampering, theft, and poor quality products and services. IT SCRM standardization requirements include methodologies and processes that enable an organization's increased visibility into, and understanding of, how technology that they acquire and manage is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. IT SCRM standardization lies at the intersection of cybersecurity and supply chain management and provides a mix of mitigation strategies from both disciplines for a targeted approach to managing IT supply chain risks.

There are two high-level SCRM standards available: The Open Group standard is focused on IT providers (not the acquirer), and the multipart standard, ISO/IEC 27036, covers information security for supplier relationships.

The Open Group standard has been approved as ISO/IEC 20243:2015 *Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*). The requirements cover best practices for product development, secure methodologies, and supply chain security—from design through disposal. The Open Group O-TTPS conformance assessment program is for providers, component suppliers, integrators, and distributors of IT. It is not applicable to acquirers.

ISO/IEC 27036 has four parts:

- ISO/IEC 27036-1:2014 *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts;*
- ISO/IEC 27036-2:2014 *Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements;*
- ISO/IEC 27036-3:2013 *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security; and*
- ISO/IEC 27036-4:2016 *Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services.*

In a couple of cases, standards developers are focused on SCRM for specific applications, such as ISO/IEC JTC1 for cloud computing and IEC TC 65 for industrial-process measurement, control and automation for industrial control systems (ICS). While any organization and any application would benefit from implementing those broad-based standards immediately, there is still a need for defining additional application specific requirements, which could be achieved either by evolving these standards, or by developing more specific standards to supplement or overlay these.

6.11 System Security Engineering

System security engineering standards describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort:

- Includes a combination of technical and nontechnical activities;
- Ensures all relevant stakeholders are included in security requirements definition activities;
- Ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle;
- Assesses and understands susceptibility to threats in the projected or actual environment of operation;
- Identifies and assesses vulnerabilities in the system and its environment of operation;

- Identifies, specifies, designs, and develops protective measures to address system vulnerabilities;
- Evaluates/assesses protective measures to ascertain their suitability, effectiveness, and degree to which they can be expected to reduce mission/business risk;
- Provides assurance evidence to substantiate the trustworthiness of protective measures;
- Identifies, quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and
- Leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.

Relevant international standards include:

- The ISA/IEC-62443 standards series define procedures for implementing electronically secure industrial automation and control systems (IACS);
- ISO/IEC 15026-2:2011, *Systems and software engineering – Systems and software assurance – Part 2: Assurance case*
  ISO/IEC 15026-4:2012, *Systems and software engineering – Systems and software assurance – Part 4: Assurance in the life cycle*;
- NDIA SA Guide Book/NATO AEP-67, Engineering for System Assurance in NATO Programs; and
- ISO/IEC 20243:2015 *Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

7 IoT Cybersecurity Objectives, Risks, and Threats

7.1 Overview

Trustworthiness is the degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks [22]." Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems [23]. Trustworthiness of IoT systems will require active management of risks for privacy, safety, security, etc. Cybersecurity risk management for IoT systems will continue to be a major factor in the trustworthiness of IoT applications.

Cybersecurity Objectives

***Confidentiality*:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;
***Integrity*:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and
***Availability*:** Ensuring timely and reliable access to and use of information.

Given how the pace of IT innovation is magnitudes faster than the pace of development of supporting standards, it is critical to be forward thinking about cybersecurity needs in the future operational environment. Physical implications are already a reality of cyber-attacks on one or more IoT components. Traditional IT security focuses on confidentiality, integrity, and availably. Due to the nature of many IoT components, which interact with the physical world through sensors and actuators, IoT security also addresses threats to people, their objects, and their environment.

IoT components have the capability to connect to the Internet, being Internet Protocol (IP) based, but may also be deployed in stand-alone IP networks that are not connected to the Internet. In addition, IoT includes the facilities that allow users and organizations to analyze and understand the data gathered and actions taken by the things.

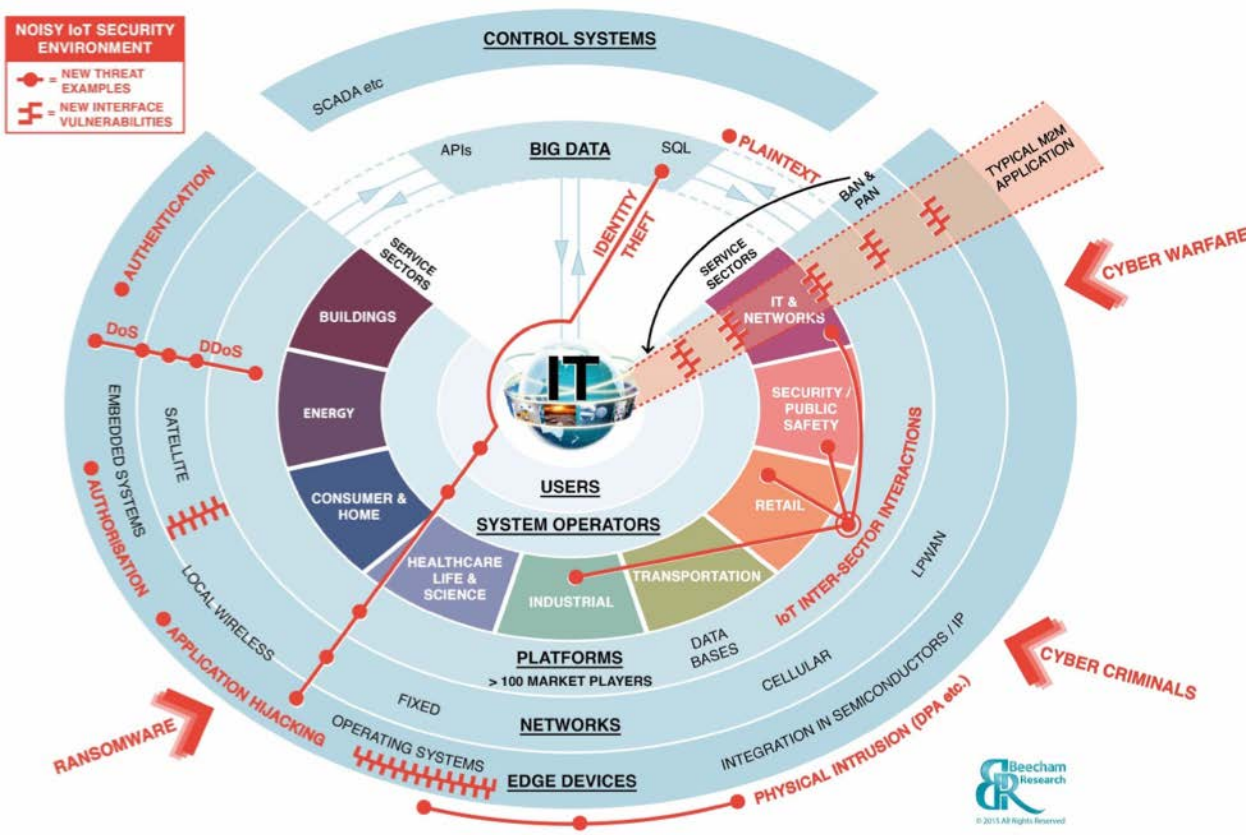


Figure 11 – Beecham Research IoT Security Threat Map [24]

Inexpensive, pervasive, highly capable edge devices create a new attack surface

According to the DoD CIO: "IoT brings together primary characteristics of traditional Internet and mobile capabilities and those of industrial control systems. The major difference between IoT and previous Internet and mobile capabilities is the control and sensing capabilities of Things. The major differences between IoT and previous industrial control system capabilities are the connectivity of Things to the Internet and their wider scope of application. Still, IoT and industrial control systems do share three quality dimensions of systems: Integrity, Availability, and Confidentiality. While traditional information systems generally prioritize Confidentiality, then Integrity, and lastly Availability, control systems and IoT usually prioritize Availability first, then Integrity and lastly Confidentiality. This does not mean that focus should be exclusively on Availability. We need to ensure that we maintain sufficient focus on Integrity and Confidentiality to address safety, privacy, and mission requirements [25]." Medical devices prioritize integrity over the others since it relates most strongly to patient safety.

With the changing threat environment, the cybersecurity needs of the future—including the data that informs, reports, and controls functionality of the IoT—should be considered. Although not specific to IT security, privacy, safety, authentication, and resilience provide contributions to IT and cybersecurity. Evolutions in system security engineering approaches can aid in the reduction of susceptibility of systems to a variety of simple, complex, and hybrid threats including physical

and cyber-attacks, structural failures, natural disasters, and errors of omission and commission. One ongoing challenge is to reduce the susceptibility of systems to a variety of simple, complex, and hybrid threats including physical and cyber-attacks, structural failures, natural disasters, and errors of omission and commission. This reduction is accomplished by fundamentally understanding stakeholder protection needs and subsequently employing sound security design principles and concepts throughout the system life cycle processes.

The specific security objectives for industrial control systems in NIST SP 800-82 [26] can be adapted for IoT systems in general as follows:

- **Restricting logical access to the network and network activity.** This may include using unidirectional gateways, a demilitarized zone network architecture with firewalls to prevent network traffic from passing directly between the corporate and IoT networks, and having separate authentication mechanisms and credentials for users of the corporate and IoT networks. An IoT system should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restricting physical access to IoT network and components.** Unauthorized physical access to components could cause serious disruption of IoT system's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
- **Protecting individual IoT components from exploitation.** This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services and assuring that they remain disabled; restricting IoT user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
- **Preventing unauthorized modification of data.** This includes data that is in transit (at least across the network boundaries) and at rest.
- **Detecting security events and incidents.** Detecting security events, which have not yet escalated into incidents, can help defenders break the attack chain before attackers attain their objectives. This includes the capability to detect failed IoT components, unavailable services, and exhausted resources that are important to provide proper and safe functioning of an IoT system.
- **Maintaining functionality during adverse conditions.** This involves designing IoT system so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on IoT or other networks, or does not cause another problem elsewhere, such as a cascading event. IoT system should also allow for graceful degradation such as moving from "normal operation" with full automation to "emergency operation" with operators more involved and less automation to "manual operation" with no automation.

- **Restoring the system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly IoT system can be recovered after an incident has occurred.

Risks

For the purposes of this Report, *risk* is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts (both inherent and residual) that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. For example, information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Risk assessment is the process of identifying, estimating, and prioritizing risks. Assessing risk requires the careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur [27].

The proliferation and increased ubiquity of IoT components are likely to heighten the risks they present; particularly as cyber criminals work to develop new generations of malware dedicated to exploiting them. For instance, Dyn, a company that monitors and routes Internet traffic, was a victim of a DDoS attack in October 2016 that was launched from thousands of IoT components infected with the “Mirai” malware. The torrent of traffic unleashed by the Mirai-infected IoT components overwhelmed Dyn’s systems and, in turn, rendered unavailable many high-traffic websites (e.g., PayPal, Twitter, Netflix, and CNN) that used Dyn’s Internet services for substantial periods of the day. The disruption of Dyn and associated Internet services underscores the significant, systemic harm that may be caused by malware dedicated to exploiting the security vulnerabilities of IoT components.

As the market for IoT components expands, it is critical that manufacturers design components with security in mind and system designers pay attention to new attack surfaces revealed with unforeseen emergent properties of these systems.

Overall, there is a multiplicity of risks associated with IoT. To minimize impact, these risks should not be assessed and monitored in a vacuum, but take into consideration the broader perspective of risk to ensure all aspects of threat and vulnerability are addressed.

Threats

A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service [28].

Threats exist both to and from the Internet of Things. Data storage and communication must be protected as the increasing quantity of components will bring an increasing amount of data requiring protection. Threats to people, their property, and their interactions with society are

becoming more abundant as a result of the growing attack surface.

NIST SP 800-30 Revision 1 provides an extensive list of threats [29]. Categories of adversarial threats include:

- Perform reconnaissance and gather information**;**
- Craft or create attack tools;
- Deliver/insert/install malicious capabilities;
- Exploit and compromise;
- Conduct an attack (i.e., direct/coordinate attack tools or activities);
- Achieve results (i.e., cause adverse impacts, obtain information); and
- Maintain a presence or set of capabilities.

Other types of non-adversarial threats include mistakes by authorized privileged users and severe natural events such as earthquakes, floods, hurricanes, and tornados.

7.2 Connected Vehicles

Cybersecurity Objectives

Confidentiality	V2V, V2I, and V2X communications require secure cryptographic authentication.
Integrity	The contents of messages (e.g., BSM) require protection from modification of the authentic information.
Availability	The real-time nature of V2V, V2I, and V2X communications require resilient and secure networks.

Vehicle manufacturers have already been focused on driver and passenger safety. Greater emphasis may be required due to the increased attack surface from V2V, V2I, and V2X communications. Beyond physical safety, there are privacy concerns. Users may connect and have access to their vehicles through their smartphones, thus personal information on these components need to be protected from unauthorized access through the vehicle. Similarly, the vehicle must be protected from threats that may come through the mobile device.

Risks

Connected vehicles face many of the same risks as other IoT systems and cyber systems in general. Severe safety consequences to vehicles and people require risk assessments to be developed. Potential safety-critical risks include [30]:

- Driver distractions (volume, wipers, etc.) ;
- Engine shutoff or degradation; and
- Steering changes (in drive-by-wire vehicles).

There are other, less safety-critical risks, some of which are fairly unique to vehicles:

- Theft of the car or its contents;
- Enabling physical crimes against the occupants;
- Insurance or lease fraud;
- Eavesdropping on the occupants;
- Theft of information (e.g., phone list);
- Vector for attacking mobile devices in the car;
- Theft of personally identifiable information (PII); and
- Tracking the vehicle's location.

Threats

The addition of Internet connectivity to infotainment consoles has already introduced threats to driver and passenger safety as a result of intercommunications between vehicle controls and entertainment. Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications introduce new attack vectors. The addition of these communication channels brings an increased threat of spoofed, manipulated, damaged, and missing sensors and actuators, which could cause vehicles to behave unpredictably.

Appropriate security measures must be taken within each subsystem as well as any communications or interactions between them. Protections must be made against user error, device malfunction, and device damage in addition to deliberate attacks by malicious actors (e.g., disgruntled employees, agents of industrial espionage, and terrorists).

Additional threats:

- Increased complexity of these dynamic networks may introduce vulnerabilities and increase exposure to potential attackers and unintentional errors.
- Set-and-forget sensors will provide ample opportunities for capture and compromise attacks to cause unexpected and unsafe behavior of vehicles.
- Threats to sensors and actuators risk harm to passengers and passersby in addition to damage to vehicles and objects on and along the road.
- Location of the vehicle could be exposed through vulnerabilities in the vehicles information system as well as those in mobile devices that may be used to interface.
- The heavy push towards automated, or "self-driving," vehicles must also be a heavy push towards fault-tolerances and fail-safes to adapt to the dynamic networks.

The Tampa Hillsborough Expressway Authority (THEA) CV Pilot Team [31] has assembled the following lists of V2X threats:

- An attacker learns restricted information on the device/system, such as private keys, certificates, etc., using a non- invasive attack such as a side channel attack and/or cryptanalysis of algorithms and signed messages.
- An attacker learns restricted information on the device/system, such as private keys, certificates, etc., using an invasive software attack such as malware (available on Internet for example) that exploits vulnerabilities in algorithms and software.
- An attacker learns physically protected restricted information on the device, such as private keys, using a physical attack.

- An attacker replays a BSM or other system message at a different (than original) time and/or location.
- An attacker modifies the sensor inputs on a single device before the device uses them to generate and send a BSM or other system message.
- An attacker modifies the sensor inputs to multiple devices before the device uses them to generate and send a BSM or other system message (for example, by GPS spoofing).
- An attacker is able to use restricted information on the device/system to create a false BSM or other system message without actually extracting the information from the device/system (e.g., use private key to sign a message without completing one of the T.Extract attacks).
- An attacker who knows about the misbehavior detection algorithms (and associated parameters) manipulates the content of the BSM to evade detection.
- An attacker who has been reported sending invalid messages denies that those messages came from the attacker's device, thwarting the misbehavior detection process.
- An attacker who knows about the misbehavior detection algorithms (and associated parameters) manipulates misbehavior reports to implicate innocent devices/systems and evade detection.
- An attacker uses the change pattern(s) of certificates and other BSM-relevant information to track a vehicle or other device.
- An attacker uses BSM data to track a vehicle/device.
- An attacker installs malware on a device/system that prevents receiving, or making use of, or providing user interaction based on BSMs or other system messages.
- An attacker uses the device as an attack vector on the rest of the vehicle/system.
- An attacker transmits noise and energy on the same frequency as the DSRC safety channel.
- An attacker transmits messages to jam or distract. These messages may contain incorrect info but are validly signed or may appear valid but have a bad cert or signature.

7.3 Consumer IoT

Cybersecurity Objectives

Confidentiality	Consumer IoT systems require preserving authorized restrictions on access and disclosure to consumer data and services.
Integrity	Consumer IoT systems require the protection of data integrity and the operation of other electronic components on the network.
Availability	Consumer IoT systems require continuity of operations for consumer IoT components that are connected to the physical world.

The main cybersecurity objectives for Internet-connected consumer electronic components are confidentiality, integrity, availability of consumer data and services. These objectives can intersect with consumer safety and privacy. The cybersecurity of an Internet-connected consumer device is also important to depriving hackers of a conduit through which they may compromise the data integrity and operation of other electronic components on the same network. In addition,

the burgeoning popularity of connected consumer components also makes them ripe targets for criminals who seek to execute coordinated, widespread cyber attacks that cause significant, systemic harm across the Internet. To achieve these security objectives, consumer components should use strong and readily updatable firmware and robust authentication practices, such as strong password requirements. In some instances, using encryption or a virtual private network (VPN) connection to your local network may protect against unauthorized eavesdropping and protect the login credentials of your IoT consumer components.

Risks

Consumer IoT components are challenged by many of the same cybersecurity risks as computers, smartphones, and other categories of IoT components. For instance, to attack IoT components, cyber criminals often probe the components for security vulnerabilities and then install malicious software ("malware") to surreptitiously control the device, damage the device, gain unauthorized access to the data on the device, and/or otherwise affect the device's operation without permission. The risks posed by malware-infected IoT components, however, may be more pronounced because their low costs and energy constraints often constrain the resources that are invested in their cybersecurity and, therefore, make them ripe targets for hackers intent on causing widespread harm. Indeed, given their growing volume, consumer IoT components are increasingly targeted as a means for penetrating other electronic components on the same network, or assembling an army of machines capable of transmitting Internet traffic without the device owners' knowledge as part of a DDoS attack.

Additional risks created by consumer IoT components include:

- Risks to physical safety by small consumer IoT components that are connected to the physical world and may be accessed or controlled remotely, such as smart ovens, stoves, toasters, etc.;
- Risks to property that may be caused by interrupting the operation of certain consumer IoT components that are connected to the physical world, such as refrigerators, thermostats, or washing machines;
- Risks to privacy that may be caused by accessing and remotely controlling components that are capable of collecting information about their surroundings, such as digital web cameras, autonomous robotic vacuum cleaners, connected toys, etc.;
- Risks to data security and privacy from consumer IoT components that collect a substantial amount of personal information. While consumers stand to reap the greatest benefits from the IoT, they will have to balance potential benefits with privacy concerns. Consumers will have to be discerning about how they engage with that information and with whom they share it;
- Risks to other components on the network by creating a variety of new interconnection between components and drastically expanding the attack surface of consumer/home networks;
- Risks to privacy by exposing login information for various consumer accounts that are stored on consumer IoT components; and
- Risks of side-channel attacks that could lead to physical intrusions of consumer premises and loss of property.

Threats

Without adequate cybersecurity safeguards, even inexpensive, consumer IoT components with limited functionalities may be exploited to threaten confidentiality, integrity, availability of consumer data and services, consumer privacy and safety, and other systems on the Internet. For instance, as detailed above, the disruption of Dyn and associated Internet services in October 2016 by a DDoS attack underscores the significant, systemic harm that insecure IoT components may cause. Further, as connected IoT technologies progressively extend their reach to consumer components critical to basic home functions (e.g., the connected thermostat), cyber criminals may increasingly target them in ransomware attacks or other traditional cyber attacks directed to collecting highly-sensitive personal information. Personal privacy and safety may also be compromised by the interruption of certain consumer IoT components (e.g., the connected oven) or certain side-channel attacks, such as a prospective burglar monitoring communications between and operations of components to determine the whereabouts of a homeowner.

7.4 Health IoT and Medical Devices

Cybersecurity Objectives

Confidentiality	Health IoT requires the protection of patient information from unauthorized disclosure and access.
Integrity	Health IoT requires the protection of patient safety from unauthorized modification of the intended use of the medical device.
Availability	Health IoT requires that patient information is available to authorized entities when it is needed and that the medical device's functionality continues to be available when needed.

The security objectives of health information technology (HIT) revolve around the implementation of security controls that provide for the confidentiality, integrity, and availability of patient information and for the systems supporting the use and exchange of that information. The security objectives of medical devices are concentrated around *patient safety aspects* and concentrate more on Integrity and Availability.

Major security objectives for this application area include the following:

- Protect patient safety from network originated inauthentic commands to actuators;
- Protect patient sensor data from tampering to allow correct algorithmic response;
- Protect medical device processing capability;
- Protect patient data where the data forms part of a treatment and monitoring regime;
- Protect patient information from unauthorized disclosure or modification;
- Ensure patient information is available to authorized entities when it is needed;
- Ensure prompt and secure patch delivery to medical devices;
- Ensure continuous security risk management throughout the device lifecycle;
- Explore and promote, where appropriate, existing and emerging technologies to enhance security and confidentiality of health information; and
- Educate HIT consumers on security and privacy issues related to the uses of HIT and protected health information.

Risks [32]

Cybersecurity threats and vulnerabilities can impact the safety of IT networks and the medical devices and other systems connected to these networks. However, medical devices and the IT networks they connect to are unique. In addition to data security and privacy impacts, patients may be physically affected (i.e., illness, injury, death) by cybersecurity threats and vulnerabilities of medical devices. This harm may stem from the performance of the device itself, impeded hospital operations, or the inability to deliver care. As a result, addressing the patient privacy and safety risks posed by cyber threats are of paramount importance.

Table 3 below provides examples of cybersecurity risks that may relate to networked medical devices. In Table 3: C = Confidentiality, I = Integrity, A = Availability, and PS = Patient Safety.

Table 3 – Examples of Cybersecurity Risks to Networked Medical Devices and Connected ID Networks

Risk Description	C	A	I	PS
Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices).	x	x	x	x
Failure to place authentication between a remote command and a risk.	x	x	x	x
Malware which alters data on a diagnostic device.			x	x
Device reprogramming which alters device function (by unauthorized users, malware, etc.).	x	x	x	x
Denial of service attacks which make a device unavailable.		x		x
Exfiltration of patient data or PHI from the network.	x			
Unauthorized access to the healthcare network, which allows access to other devices.	x	x	x	x
Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel).	x	x	x	x
Security vulnerabilities in off-the-shelf software due to poorly designed software security features.	x	x	x	x
Improper disposal of patient data or information, including test results or health records.	x			

Risk Description	C	A	I	PS
Misconfigured networks or poor network security practices.	x	x	x	x
Open, unused communication ports on a device which allow for unauthorized, remote firmware downloads.	x	x	x	x

Threats

Challenges include:

- The economic penalty incurred by manufacturers for ongoing cyberthreat management during the product's lifetime;
- The delivery of prompt secure and authenticated firmware and software updates to fielded systems;
- The incorrect deployment of a device system which does not optimally utilize the features available in device systems;
- Funding shortages which permit unsupported devices to remain in service; and
- The unauthorized access and modification of patient identifiable information including protected health information.

7.5 Smart Buildings

Cybersecurity Objectives

Authentication	Smart buildings require identity verification to prevent unauthorized access to any building control system.
Integrity	Smart buildings require the protection of building control system information from unauthorized modification.
Availability	Smart buildings require that building control system information is available to authorized entities when it is needed.

Preventing unauthorized access to any building control system is paramount to securing smart buildings. Thus, the main objective must be to protect the interfaces to and between each system, even when they may be overlaid on top of one another. A domino effect caused by the compromise of one system leading to the compromise of another, cannot be allowed happen. It is also important for fail-safes and backup systems to be in place in the event of a malfunction of any one of the systems. Since some of these systems may be dynamic and impossible to model in each-and-every scenario, robust modeling and testing must be done to handle foreseeable situations. Occupant safety is also a vital objective.

Risks

Smart buildings may contain several sets of IoT components that each have their own security objectives, risks, and threats. The sets include infrastructure, networked, people, digital transducers, computing resources, and combined systems. A challenge with securing smart buildings is this heterogeneity. Interoperability between systems and components from different vendors may introduce weaknesses for an attacker to exploit. The interfaces between these different components may present vulnerabilities, which, once one system becomes compromised, may be an avenue for an attacker to traverse laterally into another. The dynamic nature of these networks presents additional difficulties. As employees and visitors move around inside and around the building, the components they carry may be interacting with various networks. Vulnerabilities from edge-cases may be missed since every scenario cannot be tested.

Threats

In addition to threats arising from the many IoT systems in a smart building, additional threats include:

- Smart building controlled data centers and information systems are subject to traditional cybersecurity threats including corporate espionage;
- Threats to power management risk outages, surges, and inefficient operation;
- Threats to alarm systems could raise false alarms which may be used as distractions for other attacks;
- Compromise of security systems could allow unauthorized access/entry; and
- An attack on automated HVAC systems could result in uncomfortable work conditions that make it difficult to continue day-to-day operations.
- A physical attack could be combined with a cyber one—for instance, arson could be combined with the cyber compromise of a sprinkler system.

7.6 Smart Manufacturing

Cybersecurity Objectives

Confidentiality	Smart Manufacturing requires the protection of manufacturing information from unauthorized disclosure and access.
Integrity	Smart Manufacturing requires the protection of manufacturing information from unauthorized modification.
Availability	Smart Manufacturing requires that manufacturing information is available to authorized entities when it is needed. This includes processed within milliseconds so that it is available virtually immediately.

Today's manufacturing environment poses unique cybersecurity challenges beyond the considerable technical complexities of cyber-physical systems. These challenges stem from

fundamental differences between IT and OT. Too often, organizational stovepipes separate engineering, management and decision-making processes for enterprise business operations and the production environment, a problem exacerbated by the inherently change- and risk-averse culture on the shop floor. In the past thirty years, adaptation has meant integrating advanced technologies involving computer-based systems into the manufacturing processes. Today the line from design to production to distribution to employment of American-manufactured goods may begin in one part of the country (or the globe) and extend across the nation (or across continents).

Risks

The emerging digital manufacturing environment, often referred to as Industry 4.0, is a system built on automation, cyber-physical systems, cloud computing, and the Industrial Internet of Things (IIoT). New technologies allow manufacturers to produce reliable products efficiently and adapt to changing requirements from both civilian and military customers. But with this integration and flexibility comes the potential for malicious actors to infiltrate key systems by gaining access to manufacturing networks. When successful, these actors may extort ransom from a company to release the system from their control, copy sensitive proprietary information that can be sold to other companies or other governments, or install software that can affect a product's performance. The potential consequences for national security are compelling.

Evidence already exists that state-sponsored efforts to infiltrate and steal information from companies involved in defense manufacturing have led to the development of military equipment remarkably like U.S. systems; it is no coincidence that several of the planes, drones, and vehicles deployed by China and Russia bear striking resemblances to ones in the U.S. inventory.

Equally troubling is the fact that adversaries who penetrate the security systems in processes used to produce arms and equipment for the U.S. military may have the capability to alter or halt production processes to affect these items' reliability, safety, or security, putting the lives of service personnel at risk and materially degrading the ability of the nation's fighting forces to succeed on the battlefield.

Threats

Managing a modern manufacturing enterprise exposes the data exchanged by designers, the production team, and those involved in the supply chain to attacks by individuals or state actors, intent on stealing intellectual property, damaging the United States' competitive advantage, or sabotaging mission-critical components. Similar to emerging cybersecurity concerns related to the rapid expansion of the commercial IoT, as the number of factory floor device connections grows, the cyber-attack surface expands and requires new cybersecurity protections for confidentiality, integrity, and availability, as well as, prevention distributed denial of service (DDoS) and other attacks that require the use of distributed devices.

8 Standards Landscape for IoT Cybersecurity

IoT systems include a diverse set of new applications across consumer and industrial sectors. IoT cybersecurity considerations include but are not limited to:

- Some IoT systems have direct connections to owner networks, while others directly connect to non-owner networks. Some IoT systems have direct connections to both owner and non-owner networks.
- IoT systems may comprise highly distributed IoT components that have a variety of owners or may effectively have no defined owner.
- Some IoT systems are intended for use by or association with a particular person or group of people, while others are autonomous.
- Some IoT components are low cost, often because they use low-capability computing hardware (minimal processing, storage, etc.) and have low power consumption.
- Some IoT components are largely static (e.g., software cannot be updated, configuration cannot be changed as needed).
- Some IoT components process data locally, some IoT components have their data processed remotely, and some do both.
- A single IoT sensor may collect massive volumes of data.
- IoT components are highly heterogeneous (operating systems, network interfaces/protocols, functions, etc.)
- Many IoT systems rely on proprietary protocols for data communication.
- IoT systems are often deployed as part of highly dynamic systems and system environments.
- Many IoT systems do not provide centralized management capabilities for the owner.
- Many IoT systems can be remotely controlled by first parties (e.g., manufacturers).
- Some IoT components are deployed in physically unrestricted locations. This may mean the inability to provide physical security or a requirement for a very small form factor or low power consumption that limits computational capacity and capability.
- IoT components may encounter statistical errors when sensing and acting on physical objects.
- IoT systems may affect the safety, reliability, resiliency, performance, and other aspects of an owner's computing infrastructure and physical presence. . If a failure occurs, the IoT system should fail in a secure manner. That is, if a failure occurs, security should still be enforced. It is better to lose functionality than lose security.
- IoT systems may collect, store, and use data that the owner's personnel are not aware of or cannot manage.
- Some IoT systems have the ability to manage, update, and patch IoT components at scale.
- Some IoT systems support impromptu architectural changes.
- Some IoT systems are created through novel combinations of existing IoT systems and data streams that are re-purposed for an application not envisioned by the original designers. Further, such IoT systems may evolve as additional sensors or data streams become available or accessible.
- Some IoT systems include IoT components designed for decades-long use, such as smart meters in smart grid applications.

Annex C — An IT Standards Maturity Model, provides a classification system for characterizing

the present state of market impact of a standard or draft standard. The standards listed in Annex D – IoT Standards Mapping to Core Areas of Cybersecurity, have been collected by the IoT Task Group. They are the basis for the following observations on the present state of standards availability and standards use for IoT systems.

8.1 Cryptographic Techniques

There are many cryptographic standards. These standards are being used to protect data in transit and at rest and to provide for strong authentication.

Many of these standards can support IoT systems. For instance, many IoT components can support the Advanced Encryption Standard (AES) block cipher, included in ISO/IEC 18033-3:2010. The AES standard has widespread market acceptance.

Other standards have been developed to specifically support IoT systems. For example, the multipart ISO/IEC 29167 standard provides cryptographic options for the air interface of RFID components and the multipart ISO/IEC 29192 standard for lightweight cryptography provides cryptographic options for IoT components with constrained processing capabilities. Market acceptance for parts of these standards has not yet occurred.

Cryptographic techniques will need adjustments and innovations to accommodate the IoT. Scalability, performance, memory- and power-limited devices, and constrained communication channels all contribute to the cryptographic challenges associated with the IoT. Public-key cryptography, ubiquitous on the Web, may appear as a natural choice since the inconvenience and restrictions of shared secrets are eliminated. However, the computational demands of public-key cryptography, which may not be feasible for tiny IoT devices, must be weighed against the key management and protocol limitations that come with symmetric key cryptography. As an example, and given the immense scale envisioned for IoT applications, certificate revocation, which include resource-hungry activities such as the processing and storage associated with certificate revocation lists (CRLs) or the bandwidth associated with Online Certificate Status Protocol (OSCP), would have to be compared to the manual process and vulnerability of symmetric key distribution and update.

Fortunately, existing standards and standards in development address these concerns. Elliptic curve cryptography (ECC), defined in accepted standards such as ISO/IEC 29192-4:2013, is a public-key approach that provides well understood levels of security with smaller keys and signatures than, for example, RSA. ECC has also become entrenched as a "must implement" mechanism in many Internet protocols, such as TLS (RFC 5246), DTLS (RFC 6347), and the Internet Key Exchange for IPsec (RFC 7296). For symmetric key applications (either alone or in conjunction with PKC), light-weight algorithms are defined in ISO/IEC 29192-2. These symmetric ciphers are tuned for limited power devices. Key management guidance is available in publications such as NIST Special Publication 800-57.

Market Impact?

The AES standard has widespread market acceptance including testing and validation of thousands of implementations.

Some of the recently approved RFID and lightweight cryptographic standards have no

commercial implementations or only one commercial implementation.

Possible Standards Gaps?

Blockchain is an evolving technology that could revolutionize IoT security. The blockchain model favors peer-to-peer interactions between devices and thus de-centralizes security. Because blockchain is still under development and its applicability to security mechanisms is still not well understood, no standards exist for using blockchain in a regular interoperable fashion. However, the potential is significant enough that standards development organizations should be taking note.

8.2 Cyber Incident Management

There are many standards for cyber incident management that cover cyber incident identification, handling, and remediation. Many of these standards are applicable to IoT systems. Examples include: HITRUST CSF v9 for reporting information security incidents and weaknesses; IETF RFC 5070 – 2007 for sharing information about computer security incidents; ISO/IEC 29147: 2014 and ISO/IEC 30111: 2013 for vulnerability disclosure and handling process; OASIS OpenC2 (draft) for machine to machine exchange of commands to achieve investigative, remediation and/or mitigation effects; and OpenFog RA (February 2017) for tamper response. Some of these standards have widespread market acceptance.

Market Impact?

Market implementations are lagging for IoT systems.

Possible Standards Gaps?

Some IoT systems are not able to use software patches to fix cybersecurity flaws. In such cases, cyber incident management is important for identifying incidents but remediation may require replacing IoT components. Replacement could be time consuming and expensive. An area for new standards development could be remediation (compensating controls) when software patches are not feasible.

8.3 Hardware Assurance

ISO/IEC JTC 1 has developed several standards relevant to hardware assurance such as: ISO/IEC 27036, a multipart information security management system standard for supplier relationships; and ISO/IEC 20243:2015, for secure engineering best practices, including secure management of the IT products, components, and their supply chains. SAE International has over ten approved or draft standards dealing with counterfeit electronic parts, such as AS5553B (2016), Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria.

Market Impact?

Unknown

Possible Standards Gaps?

Detecting malware in software is technically challenging. This challenge would apply to firmware. Developing best practices for avoiding malware in firmware could be an area for new

standards development.

8.4 Identity and Access Management

There are many identity and access management standards with guidance available. Many of these standards have been developed to specifically support IoT systems or specific IoT applications. As in the case of the other core areas of cybersecurity, standards are being developed by many SDOs. Examples include: the FIDO Universal Authentication Framework (UAF) v1.1 Specifications; HITRUST CSF v9; IEEE 802.1X-2004 for port based network access control; OCF SPEC 1.0 for access control; the IETF RFC 7925 to authenticate and to negotiate cryptographic algorithms and keys; and the Thread Specifications for home and building IoT applications.

Market Impact?

Unknown

Possible Standards Gaps?

Existing standards should be reviewed to determine if they are sufficient or require revision for IoT systems.

8.5 Information Security Management Systems (ISMS)

There are several ISMS standards with market acceptance that are generally applicable to IoT systems or specific IoT applications. The ISA/IEC 62443 series includes security management requirements for Industrial Automation and Control Systems (IACS). ISO 13485:2016

Provides management requirements for medical devices and related services. ISO 27799:2016 covers information security management in health using ISO/IEC 27002. ISO/IEC 20243:2015 identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains. And, ISO/IEC 27002:2013 is being widely used as a reference for selecting security controls when implementing an Information Security Management System (ISMS).

Market Impact?

Existing standards are being implemented.

Possible Standards Gaps?

While there are specific management system standards for some IoT applications, there are other IoT applications that could possibly benefit from a management system standard based upon ISO/IEC 27002.

A new area of work could be to develop IoT security controls overlay where they would not only specify the security controls, but also could stipulate specific implementation requirements for the controls. For example, NIST SP 800-82 includes a security controls overlay for industrial control systems; and NIST SP 800-161 includes a security controls overlay for supply chain.

8.6 IT System Security Evaluation

There are many IT system security evaluation standards with market acceptance that should be relevant to IoT systems. Standards for security requirements for cryptographic modules (e.g., ISO/IEC 19790:2015) and security test requirements for cryptographic modules (e.g., ISO/IEC 24759:2014) are relevant for many types of IoT components. Other examples include: the three-part ISO/IEC 15408 for IT security evaluation; ISO/IEC TR 30104:2015 for guidance on physical security attacks, mitigation techniques and security requirements; and UL 2900 for testable cybersecurity criteria for network-connectable products and systems.

Market Impact?

Although standards exist, practical application to IoT systems has not been consistently demonstrated.

Possible Standards Gaps?

Existing standards are not specific to IoT and should be reviewed to determine if they are sufficient or require revision for IoT systems.

8.7 Network Security

There are many network security standards for various types of networks that are relevant to IoT systems. Examples include: the 3GPP Long-Term Evolution (LTE) for high-speed wireless communication for mobile phones; the Bluetooth wireless standard for exchanging data over short distances from fixed and mobile devices, and building personal area networks; the IETF RFC 7252 for a generic web protocol for the special requirements of the constrained environment of machine-to-machine (M2M) applications; IEC 62591:2016 for industrial wireless sensor networks; the IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE); IEEE 802.11-2016 for Wi-Fi™; the OMA Lightweight Machine to Machine Technical Specification, a device management protocol designed for sensor networks and the demands of a machine-to-machine (M2M) environment; and the ZigBee 3.0 specification that enables IoT components from separate IoT systems/applications to communicate.

Market Impact?

Many of these existing standards have widespread market acceptance with numerous commercial implementations. However, updates and/or new standards may be needed to deal with the IoT cybersecurity considerations listed at the beginning of Section 8.

Possible Standards Gaps?

Many existing standards may require updates and/or new standards will be needed to address IoT networks that have the potential for spontaneous connections (due to the networking) without a system view. Such IoT systems cannot be planned or secured well using traditional approaches to security since system compositional or emergent properties would never be seen by a risk manager.

IEEE 802.15.7 is a physical layer specification for visible light communication. Standards from the viewpoint of application service function development have yet to be developed.

8.8 Security Automation and Continuous Monitoring (SACM)

There are several approved and draft SACM standards. Most are specifically relevant to IoT systems. Approved standards include: IEC TR 62443-2-3:2015 for requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program; and the IETF RFC 7632 with use cases for securely aggregating configuration and operational data and evaluating that data to determine an organization's security posture. IETF Active Internet Drafts include: the Resource-Oriented Lightweight Information Exchange (ROLIE) Definition of the ROLIE Software Descriptor Extension; Concise Software Identifiers; Endpoint Compliance Profile; Software Inventory Message and Attributes (SWIMA) for PA-TNC; and Security Automation and Continuous Monitoring (SACM) Terminology.

Market Impact?

The resource limitations of IoT devices (memory, processor, power) can make it difficult to implement agent-based approaches to continuous monitoring. Device manufacturers will need to consider price and performance as more advanced capabilities are developed. The IoT ecosystem is heterogeneous and until standards are in place and broadly adopted, device manufacturers and security vendors will need to make investments in developing device-specific agents and interfaces for monitoring.

Possible Standards Gaps?

Adoption of standard protocols, interfaces, and data models will help achieve the interoperability needed to automate security operations.

8.9 Software Assurance

There are many approved software assurance standards. Many are specifically relevant to IoT systems. Examples include: IEC 82304-1:2016 for the safety and security of health software products; ISO/IEC 20243:2015 for secure engineering best practices, including secure management of the products, components, and their supply chains; the multi-part ISO/IEC 27036 for the information security for supplier relationships; and the UL 2900 criteria to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness.

Market Impact?

Despite known impacts of insecure software, the pace of adoption is slow.

Possible Standards Gaps?

The integration of best practices for software development into standards for IoT contributing disciplines is slow.

Detecting malware in software is technically challenging. Developing best practices for avoiding malware in software could be an area for new standards development.

8.10 Supply Chain Risk Management (SCRM)

There are three approved SCRM standards. They are relevant to IoT systems or specific IoT systems (i.e., medical IoT components). They are the multi-part ISO/IEC 27036; ISO/IEC 20243:2015; and UL 2900, which are also included above for software assurance.

Market Impact?

The market has been slow to implement.

Possible Standards Gaps?

The generic standards (e.g., ISO/IEC 27036) are not specific to IoT and they need to be reviewed to determine if they are sufficient or require revision for IoT systems.

8.11 System Security Engineering

There are many approved or draft system security engineering standards. Some are relevant to IoT systems or specific IoT systems (e.g., healthcare). Examples include: ISO/IEC/IEEE 15288:2015 for a set of systems engineering processes and associated terminology; the ISA/IEC 62443 series for Industrial Automation and Control Systems (IACS) that includes security management requirements.

The generic, multipart ISO/IEC 15026 for systems and software engineering assurance may be relevant to IoT systems.

Market Impact?

It is unclear if system security engineers apply systems engineering practices to IoT systems.

Possible Standards Gaps?

It is unclear if the generic system engineering standards (e.g., ISO/IEC 15026) consider IoT systems as part of the IT system.

9 Status of International Cybersecurity Standards for Selected IoT Applications

Based upon the preceding information and analysis, Table 4 provides a snapshot of the present status of cybersecurity standards development and their implementation by the marketplace.

- "Standards Available" indicates that SDO approved cybersecurity standards are for the most part available. "Some Standards" indicates that some SDO approved cybersecurity standards exist but there may be a need for additional standards and/or revisions to existing standards in this area. "Being Developed" indicates that needed SDO approved cybersecurity standards are still under development. "Standards Needed" indicates that new cybersecurity standards development projects are starting to be considered by various SDOs.
- "Implemented" indicates that two or more standards-based implementations are available for most of these SDO approved cybersecurity standards. "Slow Uptake" indicates market implementations are lagging for many SDO approved cybersecurity standards. "Not Implemented" indicates that SDO cybersecurity standards are still under development or new standards project will be needed before the market can implement.

Where there are existing standards that are being implemented, it should be noted that these standards require continuous maintenance and updating. This is based upon feedback from testing and deployments of standards-based products, processes, and services, as well as improvements in technology.

Table 4 – Status of Cybersecurity Standardization for Several IoT Applications

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Cryptographic Techniques	ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C	**Standards Available** **Slow Uptake**	**Standards Available** **Slow Uptake**	**Some Standards** **Slow Uptake**	**Standards Available** **Slow Uptake**	**Some Standards** **Slow Uptake**
Cyber Incident Management	ETSI ; ISO/IEC JTC 1; ITU-T; PCI	**Some Standards** **Slow Uptake**	**Some Standards** **Slow Uptake**	**Some Standards** **Slow Uptake**	**Some Standards** **Slow Uptake**	**Some Standards** **Slow Uptake**
Identity and Access Management	ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C	**Standards Available** **Slow Uptake**	**Standards Available** **Slow Uptake**	**Some Standards** **Slow Uptake**	**Standards Available** **Slow Uptake**	**Standards Available** **Slow Uptake**

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Information Security Management Systems	ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group; UL	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Hardware Assurance	ISO/IEC JTC 1; SAE International	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Not Implemented
Network Security	3GPP; 3GPP2; IEC; IETF; IEEE; ISO/IEC JTC 1; ITU-T; The Open Group; WiMAX Forum	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Security Automation & Continuous Monitoring	IEEE; IETF; ISO/IEC JTC 1; TCG; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Software Assurance	IEEE; ISO/IEC JTC 1; OMG; TCG; The Open Group; UL	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Supply Chain Risk Management	IEEE; ISO/IEC JTC 1; IEC TC 65; The Open Group; UL	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
System Security Engineering	IEC; IEEE; ISA; ISO/IEC JTC 1; SAE International; The Open Group	Some Standards Slow Uptake	Standards Needed Slow Uptake	Some Standards Slow Uptake	Standards Needed Slow Uptake	Standards Needed Slow Uptake

1990

10 Conclusions

This Report includes a functional description of IoT (Section 4). This provides a starting point for the assessment of the current state of international cybersecurity standards development for IoT. It may also serve as a basis for future understanding and communications among agencies about IoT.

Several IoT applications have been reviewed to better understand IoT cybersecurity objectives, risks, and threats. From this review, it appears that many IoT systems, which have been developed for diverse agency missions, share many common cybersecurity threats. Additionally, specific IoT applications may face additional classes of threats. Risk assessments need to be based upon an IoT application's priorities for confidentiality, integrity, and availability of information.

With the continuing, rapid innovation of IT, the inventory of IoT relevant cybersecurity standards will remain dynamic. Annex D of this Report contains a listing of international cybersecurity standards that the IoT Task Group has identified to be IoT relevant. The listing is substantial but it is not being represented as complete. It is also a one-time, static listing. The standards have been organized by the eleven core areas of cybersecurity described in this report (Section 6). The substantial number of standards for some of the core cybersecurity areas are the result of IT innovation as well as competitive solutions for various technologies. Based upon the information in Annex D, a high-level summary has been developed of IoT relevant cybersecurity standards including market impact and possible standards gaps (Section 8).

The identified possible standards gaps are:

- **Cryptographic Techniques:** applying blockchain technology for IoT security mechanisms;
- **Cyber Incident Management**: best practices for remediation when software patches are not feasible;
- **Hardware Assurance**: best practices for avoiding malware in firmware;
- **Information Security Management Systems (ISMS):** management system standards based upon ISO/IEC 27002 for IoT applications not already covered by the 27000 series; IoT security controls overlay where they would not only specify the security controls, but also could stipulate specific implementation requirements for the controls;
- **Network Security**: existing standards may require updates and/or new standards will be needed to address IoT networks that have the potential for spontaneous connections (due to the networking) without a system view; standards for application service function development in support of IEEE 802.15.7 (a physical layer specification for visible light communication);
- **Software Assurance:** best practices for avoiding malware in software;
- **Software Assurance:** integration of best practices for software development into standards for IoT contributing disciplines;
- **Security Automation & Continuous Monitoring:** since the IoT ecosystem is heterogeneous, IoT device manufacturers and security vendors may need to develop device-specific agents and interfaces for monitoring until the standards are tailored for the various IoT use cases and implemented in products;

- **Supply Chain Risk Management (SCRM):** generic standards (e.g., ISO/IEC 27036) are not specific to IoT and need to be reviewed to determine if they are sufficient or require revision for IoT systems;
- **System Security Engineering:** need to determine if generic system security engineering standards (e.g., ISO/IEC 15026) consider IoT systems.

Agencies should further review these possible standards gaps with respect to their respective missions. For identified priorities, agencies should work with industry to initiate new standards projects in SDOs to close such gaps.

Based upon all of this information, Table 4 provides a summary of the Task Group's views on the status of cybersecurity standardization for the five IoT applications described in Sections 5 and 7.

The availability and use of international cybersecurity standards are major factors for ensuring the secure and resilient operation of the expanding number of agency mission critical IoT systems. In accordance with USG policy, agencies should participate in the development of these standards in many SDOs and, based upon each agency's mission, cite appropriate standards in agency procurements.

Also, in accordance with USG policy, agencies should support the development of appropriate conformity assessment schemes to the requirements in such standards. US industry has a rich history of developing conformity assessment (CA) programs to meet our society's needs. In the IT sector for example, the Wi-Fi™ logo appearing on wireless network devices show that the product has been tested and certified by the Wi-Fi™ Alliance, a non-profit member association, whose goal is to ensure that any device carrying the logo connect seamlessly to any Wi-Fi™ network. Many consumers may not understand the technical details of Wi-Fi™, but they have confidence that the logo ensures that the device will connect to their home networks.

The decision on the type, independence and technical rigor of conformity assessment should be risk-based. The need for confidence in conformity must be balanced with the cost to the public and private sectors, including their international operations and legal obligations. Successful conformity assessment provides the needed level of confidence, is efficient, and has a sustainable and scalable business model.

Annex A—Some IoT Definitions and Descriptions

Internet of Things (IoT) [33]
Systems underpin every facet of American society—from transportation to utilities to communications—and are accessible and often controllable from around the world. More devices are connected to networks, and those networks are connected to each other, a concept known as IoT; however, there is no universal definition of IoT, just as there is no agreement in the use of that name to describe this trend. Whether it is called IoT, the Industrial Internet, or cyber-physical systems (CPS), the term describes a decentralized network of objects (or devices), applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical environment. These devices range from small sensors on consumer devices to sophisticated computers in industrial control systems (ICS). Ultimately, the devices have some type of kinetic impact on the physical world, whether directly or through a mechanical device to which they are connected.

Internet of Things (IoT) [34]
an infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react

Internet of Things (IoT) [35]
It is important to understand what the Internet of Things is and what the difference is between IoT ecosystem and an IoT system. A simple definition of an Internet of Things system is “a system of entities (including cyber-physical devices, information resources, and people) that exchange information and interact with the physical world by sensing, processing information, and actuating.” An IoT ecosystem may be defined as “an infrastructure of networked objects (cyber-physical devices, information resources, and people) that can be combined to create systems that interact with the physical world.

Internet of Things (IoT) [36]
In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g., sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

Internet of Things (IoT) [37]
This green paper will continue to use the term Internet of Things as an umbrella term to reference the technological development in which a greatly increasing number of devices are connected to one another and/or to the Internet. This acknowledges the widespread use and general popular acceptance of the term. The term itself is, as pointed out by some commenters, a misnomer, as many of the devices included in the Internet of Things do not use Internet Protocol or in any event may not connect directly to the Internet. At times, IoT term is more descriptive of the system or network than an actual thing. IoT has become the commonly used term for the technologies and related issues discussed here, and for the sake of simplicity it will be used throughout this paper.

Internet of Things (IoT) [38]
There is no formal, analytic, or even descriptive set of the building blocks that govern the operation, trustworthiness, and lifecycle of IoT. A composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: "what is the science, if any, underlying IoT?" This document offers an underlying and foundational science to IoT based on a belief that IoT involves *sensing*, *computing*, *communication*, and *actuation*.

Internet of Things (IoT) [39]
A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

Annex B—An IoT Capabilities Table

This table provides some details about the types of functions that each capability type can perform and the type of inputs and outputs for the function. These functions are the primary capabilities provided by the component. The three capability types not included in the table (supporting, network interface, and human UI) provide secondary capabilities that are used to connect the components to other components and support the primary functions.

Table 5 – IoT Primary Capabilities Table

Atomic Capability Type	Input Type	Transform	Output Type	Assumptions
Actuating	Digital data	Desired change in representation of aspect of physical state	Physical energy	Intent is to effect change of state in the physical world. Errors may be introduced in the digital logic, the D/A converter, the analog electrical circuit and the actuator transducer. There is a time delay between the input data arriving at the component and the change being made to the environment.
Data Storing	Digital data	Set of Information →set or subset of information available over time	Digital data	Intent is to store data for later use. Data is persistent. Data may be pushed out by the component or provided based on an external request. There is a time delay between the input and output and between a response to a data request and the initial request.
Networking	Digital data	Set of information → same set of information available over distance	Digital data	Intent is to move data from one location to another. Location is understood in a logical sense rather than purely physical. There is a time delay between the input and output.

Atomic Capability Type	Input Type	Transform	Output Type	Assumptions
Processing	Digital data	Set of information → new set of information	Digital data	Intent is to transform digital data. There is no fundamental "lossiness" in digital processing. There is a time delay between the input and output.
Sensing	Physical energy	Aspect of physical system state → Representation of aspect of physical state	Digital data	Intent is to observe a property of the physical world. Is "read only" – any change to the physical state is an undesired side effect. Measurement errors are introduced by the physical environment between the physical system and the sensor transducer, in the sensor transducer itself, in the analog electrical circuit, in the A/D converter, and in the digital logic of the sensor. There is also a time delay between the sensing and the data becoming available at the component output.

2134

Annex C—An IT Standards Maturity Model

Table 6 provides a proposed classification system for characterizing the present state of market impact of a standard. The present state may consist of several maturity levels. For instance, it's possible for Under Development, Reference Implementation, Testing, Commercial Availability and Market Acceptance levels to occur concurrently.

Table 6 – IT Standards Maturity Model

Maturity Level	Definition
No Standard	SDOs have not initiated any standard development projects.
Under Development	SDOs have initiated standard development projects. Open source projects have been initiated.
Guidance Available	A company, government agency, or industry group document is available, indicating there may be sufficient understanding and content to use the document as a basis for a standard.
Approved Standard	SDO-approved standard is available to public. Some SDOs require multiple implementations before final designation as a "standard."
Under Revision	Revisions or amendments are in progress that may affect backward compatibility with the original standard.
Technically Stable	The standard is stable and its technical content is mature. No major revisions or amendments are in progress that will affect backward compatibility with the original standard.
Reference Implementation	Reference implementation is available.
Testing	Test tools are available. Testing and test reports are available.
Conformity Assessment	First, second, or third party (e.g., certification) assessment programs are available.
Commercial Availability	Several products/services from different vendors exist on the market to implement this standard.
Market Acceptance	Widespread use of technology within an industry. De facto or de jure market acceptance of standards-based products/services.
Sunset	Newer standards (revisions or replacements) are under development.

Some SDOs require two or more implementations before final approval of a standard. Such implementations may or may not be commercial products or services. In other cases, an SDO may be developing a standard while conforming commercial products or services are already being sold. Innovation in IT means that IT standards are constantly being developed, approved, and maintained. Revisions to previous editions of standards may or may not be backward-

compatible. An SDO approved standard does not necessarily equate with success. Widespread market acceptance of an approved standard is the goal.

Annex D—IoT Standards Mapping to Core Areas of Cybersecurity

This annex represents a snapshot in time. It has been developed by the IoT Task Group to help understand the present state of international cybersecurity standards development for IoT.

The following annotated listing of standards is not exhaustive but does represent an extensive effort to identify relevant IoT cybersecurity standards. Some standards may be listed for more than one core area of cybersecurity.

The state of market acceptance for standards (i.e., Maturity Level) can be relatively easy or difficult to ascertain. The Maturity Levels are described in Table 6. The Maturity Level and other information below is subject to change based upon further review and comments on this draft Report.

The listing is sorted by Core Area of Cybersecurity, then by SDO, and last by Documents.

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
Bluetooth LE	**Bluetooth SIG**	Bluetooth Low Energy (BLE) Key Generation: When using Bluetooth LE Secure Connections, the following keys are exchanged between master and slave: • Connection Signature Resolving Key (CSRK) for Authentication of unencrypted data • Identity Resolving Key (IRK) for Device Identity and Privacy Encryption: BLE uses AES-CCM cryptography. Like BR/EDR, the LE controller will perform the encryption function. This function generates 128-bit encrypted data from a 128-bit key and 128-bit plaintext data using the AES-128-bit cypher defined in FIPS-1971.	Guidance Available Commercial Availability Market Acceptance Reference Implemen-tation	**What is BLE?** A BLE beacon is a small device – usually powered by battery or USB – that emits a Bluetooth Low Energy signal.

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Signed Data: BLE supports the ability to send authenticated data over an unencrypted transport between two devices with a trusted relationship. This is accomplished by signing the data with a CSRK.		
ETSI GR QSC 004 V1.1.1 (2017-03):	**ETSI**	Quantum-Safe Cryptography; Quantum-Safe threat assessment The present document presents the results of a simplified threat assessment following the guidelines of ETSI TS 102 165-1 [i.3] for a number of use cases. The method and key results of the analysis is described in clause 4. The present document makes a number of assumptions regarding the timescale for the deployment of viable quantum computers, however the overriding assertion is that quantum computing will become viable in due course. This is examined in more detail in clause 5. The impact of quantum computing attacks on the cryptographic deployments used in a number of existing industrial deployment scenarios are considered in clause 7.	Approved Standard	
ETSI GR QSC 001 V1.1.1 (2016-07)	**ETSI**	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework The present document gives an overview of the current understanding and best practice in academia and industry about quantum-safe cryptography (QSC). It focuses on identifying and assessing cryptographic primitives that have been proposed for efficient key establishment and authentication applications, and which may be suitable for standardization by ETSI and subsequent use by industry to develop quantum-safe solutions for real-world applications. QSC is a rapidly growing area of research. There are already academic conference series such as PQC and workshops have been established by	Approved Standard	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		ETSI/IQC [i.1] and NIST. The European Commission has recently granted funding to two QSC projects under the Horizon 2020 framework: SAFEcrypto [i.2] and PQCrypto [i.3] and [i.4]. The present document draws on all these research efforts. The present document will cover three main areas. Clauses 4 and 5 discuss the types of primitives being considered and describe an assessment framework; clauses 6 to 10 discuss some representative cryptographic primitives; and clause 11 gives a preliminary discussion of key sizes.		
ETSI GR QSC 003 V1.1.1 (2017-02)	**ETSI**	Quantum Safe Cryptography; Case Studies and Deployment Scenarios The present document examines a number of real-world uses cases for the deployment of quantum-safe cryptography (QSC). Specifically, it examines some typical applications where cryptographic primitives are deployed today and discusses some points for consideration by developers, highlighting features that may need change to accommodate quantum-safe cryptography. The main focus of the document is on options for upgrading public-key primitives for key establishment and authentication, although several alternative, non-public-key options are also discussed. The present document gives an overview of different technology areas; identify where the security and cryptography currently resides; and indicate how things may have to evolve to support quantum-safe cryptographic primitives. Clauses five and six discuss network security protocols, using TLS and S/MIME as typical examples. These are contrasted in clauses seven and eight by an examination of security options for IoT and Satellite use cases, which have very different requirements and constraints than traditional Internet-type services.	Approved Standard	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Some alternatives to public key protocols are reviewed in clause nine. Authentication requirements are discussed in clause ten and some forward-looking examples providing advanced functionality are examined in clause eleven.		
ETSI GS QKD 002 V1.1.1 (2010-06)	**ETSI**	Quantum Key Distribution; Use Cases The Use Cases Document shall provide an overview of possible application scenarios in which Quantum Key Distribution (QKD) systems ([i.1]) can be used as building blocks for high security Information and communication technology (ICT) systems. QKD	Approved Standard	
Trusted Execution Environment (TEE)	**GlobalPlatform**	The TEE's ability to offer isolated safe execution of authorized security software, known as 'trusted applications', enables it to provide end-to-end security by enforcing protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights. *Under Section "What is a TEE?"*	Approved Standards Guidance Available	**What is a TEE?** The TEE is a secure area of the main processor in any connected device that ensures that sensitive area is stored, process and protected.
HITRUST CSF v9 10 September 2017	**HITRUST Alliance**	Message Integrity: Specification: Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and controls implemented. Implementation: The information system provides mechanisms to protect the authenticity of communications sessions. The system shall implement one (1) of the following integrity protection algorithms	Approved Standard Under Revision Guidance Available	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• HMAC-SHA-1 • HMAC-MD5 <u>Output Data Validation:</u> Specification: Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Implementation: Output validation shall include: • Plausibility checks to test whether the output data is reasonable • Reconciliation control counts to ensure processing of all data • Providing sufficient information for a reader • Procedures for responding to output validation tests • Defining the responsibilities of all personnel involved in the data output process • Creating an automated log of activities in the data output validation process <u>Cryptographic Controls:</u> Objective: to protect the confidentiality, authenticity and integrity of information by cryptographic means. A policy shall be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques. <u>Key Management:</u> Specification: key management shall be in place to support the organization's use of cryptographic techniques. Implementation: all cryptographic keys shall be protected against modification, loss, and destruction. Keys shall not be stored in the		

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Cloud, but maintained by the cloud consumer or trusted key management provider. Key management and key usage are separated duties. *Page 462, Sections under category 10*		
IEEE 1363-2000 and IEEE 1363a-2004	**IEEE**	traditional public-key cryptography	Approved Standard	
IEEE 1619-2007	**IEEE**	cryptographic protection of data on block-oriented storage devices	Approved Standard Some activity regarding revisions	
IEEE 802.1X-2010	**IEEE**	An IEEE Standard for port-based Network Access Control (PNAC). It provides authentication mechanisms to devices wishing to attach to an LAN or WLAN. 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. Supplicant: a client device that wishes to attach to the LAN/WLAN. Authenticator: a network device, such as an Ethernet switch or wireless access point. It acts like a security guard to a protected network. Authentication server: typically, a host running software supporting the RADIUS and EAP protocols.	Approved Standard Under Revision?	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Typical authentication progression: 1. Initialization: on detection of a new supplicant, the port on the switch is enabled and set to the unauthorized state. 2. Initiation: to initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address on the local network segment. 3. Negotiation: The authentication server sends a reply to the authenticator, containing an EAP Request specifying the EAP Method. The authenticator encapsulates the EAP Request in an EAPOL frame and transmits it to the supplicant. At this point the supplicant can start using the requested EAP Method, or do an NAK ("Negative Acknowledgement") and respond with the EAP Methods it is willing to perform. 4. Authentication: If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server (translated by the authenticator) until the authentication server responds with either an EAP-Success message (encapsulated in a RADIUS Access-Accept packet), or an EAP-Failure message (encapsulated in a RADIUS Access-Reject packet). If authentication is successful, the authenticator sets the port to the "authorized" state and normal traffic is allowed, if it is unsuccessful the port remains in the "unauthorized" state. When the supplicant logs off, it sends an EAPOL-logoff message to the authenticator, the authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.		

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
IEEE P1363.3	**IEEE**	identity-based public-key cryptography using pairings	Under Development	
IEEE 1619.1-2007	**IEEE**	authenticated encryption with length expansion for storage devices Cryptographic unit: a cryptographic unit is any combination of software, firmware, or hardware that is capable of handling plaintext and ciphertext using at least one of the cryptographic modes. The cryptographic unit shall contain the following subcomponents: • Plaintext record formatter and/or plaintext record de-formatter • Encryption routine and/or decryption routine • Cryptographic parameters The cryptographic unit may contain the following subcomponents: • Random bit generator • Key wrapping routine • Key unwrapping routine *Page 10, Section 4.2.4* Cryptographic modes: • Counter with cipher block chaining-message authentication code (CCM) • Galois/Counter Mode (GCM) • Cipher block chaining with keyed-hash message authentication code (CBC-HMAC) • Xor-encrypt-xor with tweakable clock-cipher with keyed-hash message authentication code (XTS-HMAC)	Approved Standard	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Page 13, Section 5		
IEEE 1363.2-2008	**IEEE**	Variations of the network password problem: This standard describes three classes of password-based methods that solve three variations of the password-only network login problem. These methods can provide mutual zero knowledge password proof and remote password-authenticated establishment of cryptographic keys. 1. Balanced password-authenticated key agreement – two parties share a common password and they want to prove to each other that they know the password, and only then engage in secure communications, without revealing the password to others. 2. Augmented password-authenticated key agreement methods – similar to the first except that one of the parties, the Server, has password verification data derived using a one-way function of the password. 3. Password- authenticated key retrieval – addresses the scenario where one desires to further decrease the sensitivity of stored password-derived data. All these methods require one or more parties to use specific password-related data to make the method succeed. Primitives: The following types of primitives are defined in this standard: • Random element derivation primitives (REDP), components of password-authenticated key agreement schemes (PKAS) and password-authenticated key retrieval schemes (PKRS).	Approved Standard	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• Password-entangled public-key generation primitives (PEPKGP); components of PKASs and PKRSs • Secret value derivation primitives (SVDP), components of augmented password-authenticated key agreement and PKRSs • Password verification data generation primitives (PVDGP), components of augmented password-authenticated key agreement schemes (APKAS) • Key retrieval blinding primitives (KRBP), key retrieval unblinding primitives (KRUP), and key retrieval permutation primitives (KRPP), components of key retrieval schemes.		
IEEE 1619.2-2010	**IEEE**	wide-block encryption for shared storage media This document specifies two different EAD algorithms: EME2-AES and XCB-AES. Both implement a tweakable pseudorandom permutation with substantially similar security properties and have similar bounds with respect to the amount of data that is able to be safely be encrypted with a single key. Nevertheless, upon choosing an algorithm, implementers might need to consider other factors than security level such as software performance or hardware implementation size	Approved Standard	
IEEE 802.11-2016	**IEEE**	Classes of security algorithm: This standard defines two classes of security algorithms for IEEE802.11 networks: Algorithms for creating and using an RSNA, called *RSNA algorithms*, and Pre-RSNA algorithms. Security methods:	Approved Standard Market Acceptance	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Pre-RSNA security comprises the following algorithms and procedures: • WEP • IEEE 802.11 entity authentication RSNA security comprises the following algorithms and procedures: • TKIP • CCMP • GCMP • BIP • RSNA establishment and termination procedures, including use of IEEE 802.1X authentication and SAE authentication • Key management procedures *Page 1923, Section 12*		
IEEE 802.15.4-2015	**IEEE**	Security: The MAC sublayer is responsible for providing security services on specified incoming and outgoing frames when requested to do so by the higher layers. This standard supports the following security services: • Data confidentiality • Data authenticity • Replay protection (when not using TSCH mode) Outgoing frame security procedure: The inputs to this procedure are the frame to be secured and the SecurityLevel, KeyIdMode, KeySource, and KeyIndex parameters.	Approved Standard Market Acceptance	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Page 360, Section 9		
Internet Draft	**IETF**	End-to-end Security: Regarding end-to-end security in the context of the confidentiality and integrity protection, the packets are processed applying message authentication codes or encryption. The five approaches to handle such end-to end confidentiality and integrity protection while letting middleboxes access/modify data for different purposes: • Sharing credentials with middleboxes enables middleboxes to transform packets and re-apply the security measures after transformation • Reusing the Internet wire format in the IoT makes conversion between IoT and Internet protocols unnecessary. However, it can lead to poor performance in some use cases because IoT specific optimizations are not possible. • Selectively protecting vital and immutable packet parts with a MAC or with encryption requires a careful balance between performance and security. Otherwise, this approach will either result in poor performance or poor security. • Message authentication codes that sustain transformation can be realized by considering the order of transformation and protection. • Object security based mechanisms can bridge the protocol worlds, but still requires that the two worlds use the same object security formats. *Page 35 section 7.1.3*	Under Development	IETF "State of the Art and Challenges for the Internet of Things" draft-irtf-t2trg-iot-seccons-02
RFC 5280 -	**IETF**	Internet X.509 Public Key Infrastructure Certificate and Certificate	Approved	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
2015		Revocation List (CRL) Profile (Updated)	Standard	
RFC 7925	**IETF**	TLS and DTLS: The TLS protocol provides authenticated, confidentiality and integrity protected communication between two endpoints. The protocol is composed of two layers: The Record Protocol and the handshaking protocols. At the lowest level, layered on top of a reliable transport protocol (e.g., TSP), is the Record Protocol. It provides connection security by using symmetric cryptography for confidentiality, data origin authentication, and integrity protection. *Page 5, Section 3.1*	Approved Standard Commercial Availability Conformity Assessment Market Acceptance	
RFC 8105	**IETF**	Security Considerations: The secure transmission of circuit more services in DECT (Digital Enhanced Cordless Telecommunications) is based on the DSAA2 (DECT Standard Authentication Algorithm #2) and DSC/DSC2 (DECT Standard Cipher/DECT Standard Cipher #2) specifications developed by ETSI Technical Committee (TC) DECT and the ETSI Security Algorithms Group of Experts (SAGE). DECT ULE communications are secured at the link layer (DLC) by encryption and per-message authentication through CCM (Counter with Cipher Block Chaining Message Authentication Code (CBC-MAC)) mode. The underlying algorithm for providing encryption and authentication is AES128. The DECT ULE (Digital Enhances Cordless Telecommunications Ultra Low Energy) pairing procedure generates a master User Authentication Key (UAK). During the location registration procedure, or when the permanent virtual circuits are established, the session security keys are generated. Both the master authentication key and session security keys	Under Development	Guidance Available Currently in the IETF Standard Track

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		are generated by use of the DSAA2 algorithm, which uses AES127 as the underlying algorithm. *Page 17, Section 5*		
ISO/IEC 29167-1:2014	**ISO/IEC**	security services for RFID air interfaces Defines the architecture for security services for the ISO/IEC 18000 air interfaces standards for radio frequency identification (RFID) devices.	Approved Standard	
ISO/IEC 29167-10:2017	**ISO/IEC**	Part 10: Crypto Suite AES-128 Security Services for Air Interface Communications	Approved Standard Commercial Availability	
ISO/IEC 29167-11:2014	**ISO/IEC**	Part 11: Crypto Suite PRESENT-80 Security Services for Air Interface Communications	Approved Standard	
ISO/IEC 29167-12:2015	**ISO/IEC**	Part 12: Crypto Suite ECC-DH Security Services for Air Interface Communications	Approved Standard	
ISO/IEC 29167-13:2015	**ISO/IEC**	Part 13: Crypto Suite Grain-128A Security Services for Air Interface Communications	Approved Standard Commercial Availability	
ISO/IEC 29167-14:2015	**ISO/IEC**	Part 14: Crypto Suite AES OFB Security Services for Air Interface Communications	Approved Standard	
ISO/IEC 29167-16:2015	**ISO/IEC**	Part 16: Crypto Suite ECDSA-ECDH Security Services for Air Interface Communications	Approved Standard	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
ISO/IEC 29167-17:2015	**ISO/IEC**	Part 17: Crypto Suite CryptoGPS Security Services for Air Interface Communications	Approved Standard	
ISO/IEC 29167-19:2016	**ISO/IEC**	Part 19: Crypto suite RAMON security services for air interface communications	Approved Standard	
ISO/IEC TR 29181-9:2017	**ISO/IEC**	Data Encryption: IPv4 can only utilize data encryption (IPV6-IPSec), but its addresses cannot be encrypted. It cannot provide address confidentiality. This technical report is Part 2 of the Technical report on Future Network – Problem Statement and Requirements developed by ISO/IEC JTC1 SC6. Part 2 focuses on the issue of naming and addressing. New Communications Rules to Supplement New NAS: In order to protect the addressing security, Future Network may consider adopting a new communication rule requiring verification of source address and destination address before sending message to the networks. The new rules should design and utilize better and newer authentication and verification systems to achieve system wide security. • To construct a true identity authentication, verification and certification system. • To change from passive and defensive network security into proactively managed cybersecurity. • To prove communicator true identity, verify network (Internet) address and routing path authenticity, and prevent unauthorized access, and realize trusted connection.	Approved Standard	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• To certify the authenticity of software and the consistency of software identity and software data, achieving trusted computing. • Trusted connection which is the key for trusted systems. Trusted routing is the key for realizing trusted connection. *Page 23, Section 6.2.4.3* This technical report is Part 2 of the Technical report on Future Network – Problem Statement and Requirements developed by ISO/IEC JTC1 SC6. Part 2 focuses on the issue of naming and addressing.		
ISO/IEC 29192-1:2012	**ISO/IEC**	Lightweight Cryptography – includes general information such as security, classification and implementation requirements	Approved Standard Market Acceptance Under revision	
ISO/IEC 29192-2:2012	**ISO/IEC**	specifies two block ciphers suitable for lightweight cryptography: a) PRESENT: a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits; b) CLEFIA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits.	Approved Standard Market Acceptance	
ISO/IEC 29192-2:2012 PDAM 1	**ISO/IEC**	The SIMON and SPECK families of lightweight block ciphers were developed as an aid for securing applications in very constrained environments where AES may not be suitable.	Under Development	
ISO/IEC 29192-2:2012 NP Amd 2	**ISO/IEC**	LEA is a lightweight block cipher that is being developed within ISO/IEC JTC 1 SC 27 WG 2 as an aid for securing application in very constrained environments.	Under Development	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
ISO/IEC 29192-3:2012	**ISO/IEC**	specifies two dedicated keystream generators for lightweight stream ciphers: •Enocoro: a lightweight keystream generator with a key size of 80 or 128 bits; •Trivium: a lightweight keystream generator with a key size of 80 bits.	Approved Standard Market Acceptance	
ISO/IEC 29192-4:2013 Amd.1: (2016)	**ISO/IEC**	specifies three lightweight mechanisms using asymmetric techniques: a) a unilateral authentication mechanism based on discrete logarithms on elliptic curves; b) an authenticated lightweight key exchange (ALIKE) mechanism for unilateral authentication and establishment of a session key; c) an identity-based signature mechanism.	Approved Standard Market Acceptance	
ISO/IEC 29192-5:2016	**ISO/IEC**	specifies three hash-functions suitable for applications requiring lightweight cryptographic implementations. - PHOTON: a lightweight hash-function with permutation sizes of 100, 144, 196, 256 and 288 bits computing hash-codes of length 80, 128, 160, 224, and 256 bits, respectively. - SPONGENT: a lightweight hash-function with permutation sizes of 88, 136, 176, 240 and 272 bits computing hash-codes of length 88, 128, 160, 224, and 256 bits, respectively. - Lesamnta-LW: a lightweight hash-function with permutation size 384 bits computing a hash-code of length 256 bits.	Approved Standard Market Acceptance	
ISO/IEC 9594-8:2017	**ISO/IEC**	X.509 Certificate definition	Approved Standard	
ISO/IEC CD 29192-6	**ISO/IEC**	message authentication codes (MACs)	Under Development	
ISO/IEC WD 29192-7	**ISO/IEC**	broadcast authentication protocols	Under Development	

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
KMIP 1.1 and KMIP Profiles 1.1 - 2013	**OASIS**	key management interoperability protocol	Approved Standard	
OCF SPEC 1.0 June 28, 2017	**OCF**	Message Integrity and Confidentiality: Secured communications between OCF Clients and OCF Servers are protected against eavesdropping, tampering, or message replay, using security mechanisms that provide message confidentiality and integrity. *Page 75, Section 11* The goal for the OCF security architecture is to protect OCF resources and all aspects of Hardware and Software that are used to support the protection of OCF resource.	Guidance Available Reference Implemen-tation	The Open Interconnect Consortium (OIC) has been re-launched in early 2016 as the Open Connectivity Foundation (OCF)
OMA-TS-LightweightM2M-V1_0-20170208-A	**OMA**	The LwM2M protocol utilizes DTLS with these channel bindings to implement authentication, confidentiality, and data integrity features of the protocol between communicating LwM2M entities. LwM2M supports three different types of credentials, namely: • Certificates • Raw public keys o TLS_PSK_WITH_128_CCM_8 o TLS_PSK_WITH_AES_128_CBC_SHA256 • Pre-shared secrets o TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 o TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 *Page 58 Section 7*	Guidance Available	**Open Mobile Alliance (OMA) What is OMA M2M?** OMA's LightweightM2M is a device management protocol designed for sensor networks and the demands of a machine-to-machine (M2M) environment.

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
OpenFog RA	**OpenFog Consortium**	There are three cornerstones of the fog security perspective: Confidentiality, Integrity and availability Threat model is also displayed. *Page 49, Section 5.4.2.3* Cryptographic Functions: Initial base list of required standard cryptographic algorithms that must be available on all OpenFog nodes: • Symmetric (or Secret-key) Ciphers for confidentiality protection • Cryptographic Hash Functions for integrity protection and authentication of communicating parties • Asymmetric (or Public-Key) Ciphers for generating secret keys, establishing long-term security credentials and providing non-repudiation services. The OpenFog cryptographic module must support the following FIPS approved cryptographic functions at a minimum: • Symmetric Key Ciphers o AES (with at least 128-bit keys) o Triple-DES • Asymmetric Key Ciphers *Page 122, Section 10.1.1*	Guidance Available (has a few use cases)	**What is Fog?** A system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.
TPM 1 March 2011	**TCG**	Trusted Platform Module (TPM) Cryptographic Co-Processor: The TPM employs conventional cryptographic operations in conventional ways: • Asymmetric key generation (RSA)	Guidance Available Commercial Availability Market	**What is TPM?** An industry specification that enables trust in computing

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• Asymmetric encryption/decryption (RSA) • Hashing (SHA-1) • Random number generation (RNG) The TPM uses these capabilities to perform generation of random data, generation of asymmetric keys, signing and confidentiality of stored data. *Page 30, Section 4.2.2* Remote Attestation: allows changes to the user's computer to be detected by authorized parties. Remote attestation is usually combined with public-key encryption do that the information sent can only be read by the programs that presented and requested the attestation, and not by an eavesdropper. *Link*	Acceptance Reference Implement	platforms in general.
Thread Spec 1.1 Feb 13 2017	**Thread Group**	J-PAKE/EC J-PAKE: The fundamental security used during the joining of authentication and key agreement is an elliptic curve variant of J-PAKE (Password Authenticated Key Exchange with juggling), using the NIST P-256 elliptic curve. Key agreement: Diffie-Hellmann Authentication: Schnorr signatures *Doc 2, Page 28, Section 1.3.3.1* Key Generation: Each Thread node receives the Master Key when joining and assigns it to the *thrMasterKey* attribute, which is used in conjunction with a sequence counter. The use of Hashed Message Authentication Mode with the SHA-256 algorithm (HMAC-SHA256) as the keyed hash function produces an	Approved Standard Guidance Available Commercial Availability Conformity Assessment Market Acceptance Reference Implemen-tation	**What is Thread?** Securely and reliably connects products around the home using a robust mesh network and an open IPv6 based protocol. **What is IEEE 802.15.4?** Thread leverages IEEE 802.15.4 The IEEE 802.15.4

Cryptographic Techniques: **Techniques and mechanisms and their associated standards are used to provide: confidentiality; entity authentication; non-repudiation; key management; data integrity; trust worthy data platforms; message authentication; and digital signatures.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		output of 32 bytes. Therefore, this is sufficient for the two separate keys required for the MAC sublayer and MLE. *Doc 2, Page 162, Section 7.1.4*		standard targets low-power personal area networks.

2166

2167

Cyber Incident Management: **Standards that support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
ETSI GS NGP 005 V1.1.1 (2017-04)	**ETSI**	Next Generation Protocols (NGP); Next Generation Protocol Requirements The scope of the present document is to specify the minimum set of key requirements for the Next Generation Protocols (NGP), Industry Specific Group (ISG). The present document addresses requirements in the following areas: • Business Case and Techno-Economics • Migration • General Technical Requirements • Addressing • Security • Mobility • Multi-Access Support (including FMC) • Context Awareness • Performance (including Content Enablement) • Network Virtualisation • IoT Support • Energy Efficiency • e-Commerce • MEC • Mission Critical Services • Drones and Autonomous Vehicles and Connected Vehicles • Ultra Reliable Low Latency Communications	Approved Standard	
ETSI TR 103 118 V1.1.1 (2015-08)	**ETSI**	Machine-to-Machine communications (M2M); Smart Energy Infrastructures security; Review of existing security measures and convergence investigations The present document reviews security methods provided by deployed standards used in the Smart Energy industry (e.g., IEC 62351 [i.7], IEC 62443 [i.8]) or mandated by regulation (e.g., Requirements from the German BSI for Smart Meter Gateways and Secure Element) as well as gaps identified by the Smart Grid Information Security group for the M/490 mandate, in order to identify areas where ETSI may bring additional value, e.g., by	Approved Standard	

Cyber Incident Management: **Standards that support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		extending or harmonising security solutions where possible		
ETSI TR 103 375 V1.1.1 (2016-10)	**ETSI**	SmartM2M; IoT Standards landscape and future evolutions: The scope of the present document is to provide an overview of the IoT standards landscape: requirements, architecture, protocols, tests, etc. to provide the roadmaps of the IoT standards, when they are available. The essential objectives are: • To analyse the status of current IoT standardisation. • To assess the degree of industry and vertical market fragmentation. • To point towards actions that can increase the effectiveness of IoT standardisation, to improve interoperability, and to allow for the building of IoT ecosystems	Approved Standard	
ETSI TR 118 518 V2.0.0 (2016-09)	**ETSI**	oneM2M; Industrial Domain Enablement (oneM2M TR-0018 version 2.0.0 Release 2) The present document collects the use cases of the industrial domain and the requirements needed to support the use cases collectively. In addition, it identifies the necessary technical work needed to be addressed while enhancing future oneM2M specifications.	Approved Standard	

Cyber Incident Management: **Standards that support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
HITRUST CSF v9 10 September 2017	**HITRUST Alliance**	Access Control: Control objective: to control access to information, information assets, and business processes based on business and security requirements. Authorized Access to Information Systems: Control Objective: to ensure authorized user accounts are registered, tracked and periodically validated to prevent unauthorized access to information systems. Network Access Control: Control Objective: to prevent unauthorized access to networking services that they have been specifically authorized to use. Authentication and authorization mechanisms shall be applied for users and equipment. Operating System Access Control: Objective: to prevent unauthorized access to operating systems. User identification and Authentication: Specification: All users shall have a unique identifier for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user.	Approved Standard Under Revision Guidance Available	
Internet Draft SACM Information Model	**IETF**	Secure Automation and Continuous Monitoring (SACM) Information Model	Under Development	
RFC 5070 – 2007	**IETF**	Incident Object Description Exchange Format (IODEF) for sharing information commonly exchanged by Computer Security	Approved Standard	

Cyber Incident Management: **Standards that support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Incident Response Teams (CSIRTs) about computer security incidents		
RFC 5901 -2010	**IETF**	extensions to the IODEF for reporting phishing	Approved Standard	
RFC 6545 - 2012	**IETF**	real-time inter-network defense	Approved Standard	
ISO/IEC 27035-1:2016	**ISO/IEC**	guidance on information security incident management for large and medium-sized organizations	Approved Standard	
ISO/IEC 29147: 2014	**ISO/IEC**	vulnerability disclosure	Approved Standard	
ISO/IEC 30111: 2013	**ISO/IEC**	vulnerability handling process	Approved Standard	
X.1056 - 2009	**ITU-T**	security incident management guidelines for telecommunications organizations	Approved Standard	
OpenC2	**OASIS**	Enables the machine to machine exchange of commands to achieve investigative, remediation and/or mitigation effects. Enables real-time automated and active cyber defense through	Under Development	

Cyber Incident Management: **Standards that support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		the use of standardized commands. Provides the action to be taken.		
Trusted Automated Exchange of Indicator Information (TAXII) Version 2.0 October – 2017	**OASIS**	*OASIS Trusted Automated Exchange of Indicator Information (TAXII) Version 2.0* application layer protocol for the communication of cyber threat information	Approved Specification	
Structured Threat Information Expression (STIX) Version 2.0 – October 2017	**OASIS**	*OASIS Structured Threat Information Expression (STIX) Version 2.0* defines a framework that enables cyber threat information sharing and cyber threat analysis	Approved Specification	
OpenFog RA February 2017	**OpenFog Consortium**	Tamper Response: Soft Fail: Sensitive data is cleared and a second interrupt signal is sent to the security monitor to confirm this has been done so that it can restart the processor and continue execution. Hard Fail: The actions for a Soft Fail are performed, plus the	Guidance Available (has a few use cases)	**What is Fog?** A system-level horizontal architecture that distributes resources and

Cyber Incident Management: **Standards that support information sharing processes, products, and technology implementations for cyber incident identification, handling, and remediation. Such standards enable organizations to identify when a cyber incident has occurred, to properly respond to that incident and recover from any losses as a result of the incident. Such standards are one method to enable jurisdictions to exchange information about incidents, vulnerabilities, threats and attacks, the system(s) that were exploited, security configurations and weaknesses that could be exploited, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		caches and memory are zeroed and the system is reset. Both lower and higher consequences may be available. The lowest consequence would be to do nothing, or the event can be logged for later analysis. *Page 71, Section 5.5.6.5*		services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.
DSS 3.2 – 2016	**PCI**	security controls around cardholder data to reduce credit card fraud	Approved Standard	

2168

2169

2170

Hardware Assurance: **Hardware assurance describe requirements and guidance to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
15408-1 :2009	**ISO/IEC**	Information technology – Security techniques – Evaluation criteria for IT security (Part 1: Introduction and general model)	Approved Standard Technically Stable Conformity Assessment Commercial Availability Market Acceptance	
15408-2 :2008	**ISO/IEC**	Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components	Approved Standard Technically Stable Conformity Assessment Commercial	

Hardware Assurance: **Hardware assurance describe requirements and guidance to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
			Availability Market Acceptance	
15408-3 :2008	**ISO/IEC**	Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components	Approved Standard Technically Stable Conformity Assessment Commercial Availability Market Acceptance	
20243:2015	**ISO/IEC**	Open Trusted Technology Provider Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products	Approved Standard Under Revision	Will be replaced by ISO/IEC FDIS 20243-1 and ISO/IEC CD 20243-2
27036-1 2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships (Part 1: Overview and concepts)	Approved Standard	This standard can be freely

Hardware Assurance: **Hardware assurance describe requirements and guidance to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
				downloaded.
27036-2 2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships (Part 2: Common requirements)	Approved Standard	
27036-3 2013	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for ICT supply chain security	Approved Standard	
ARP6178 2011	**SAE International**	Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors	Approved Standard	
AS5553B 2016	**SAE International**	Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria	Approved Standard	
AS6081 2012	**SAE International**	Counterfeit Electronic Parts; Avoidance Protocol, Distributors	Approved Standard	
AS6171 2015	**SAE International**	Test Method Standard; Counterfeit Electronic Parts	Approved Standard	
AS6171/11 2016	**SAE International**	Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods.	Approved Standard	
AS6171/5	**SAE International**	Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods.	Under Development	
AS6171/7	**SAE International**	Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods	Under Development	
AS6171/8 2016	**SAE International**	Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods.	Approved Standard	
AS6174A 2014	**SAE International**	Compliance Verification Matrix (VM) Slash Sheet for SAE AS6174A, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel.	Approved Standard	
AS6462A	**SAE**	Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation,	Approved	

Hardware Assurance: **Hardware assurance describe requirements and guidance to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or intellectual property) function as intended and are free of known vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, throughout the life cycle.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
2014	**International**	and Disposition Verification Criteria (2014)	Standard	

2171

2172

2173

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
ETSI TR 118 512 V2.0.0 (2016-09)	**ETSI**	The present document provides options and analyses for the security features and mechanisms providing end-to-end security and group authentication for oneM2M. The scope of this technical report includes use cases, threat analyses, high level architecture, generic requirements, available options, evaluation of options, and detailed procedures for executing end-to-end security and group authentication.	Approved Standard	
Universal Authentication Framework (UAF) v1.1 Specifications	**FIDO**	The UAF is designed around passwordless and multifactor authentication flows. This architecture lends itself to authentication of users connecting to devices and M2M authentication.	Approved Standard	https://fidoalliance.org
CLP.14 v1.1	**GSMA**	Secure Identification: When appropriate for the IoT Service, Network Operators recommend the use of UICC based mechanisms to securely identify Endpoint devices. “Single sign-on” services could also be provided by Network Operators to allow Endpoint devices to establish and prove their identity once, and then connect to several IoT Service Platforms without further	Guidance Available	The GSMA IoT Security Guidelines are backed by an IoT Security Assessment scheme that enables companies to build secure IoT devices and solutions.

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		inconvenience. *Page 11. Section 3.1*		
DS4P Release 1, May 2014	**HL7**	Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1, May 2014	Approved Standard	
FHIR Release 3	**HL7**	Fast Healthcare Interoperability Resources Specification (FHIR), Release 3	Under Development (Trial Use)	
HCS Release 1, August 2014	**HL7**	HL7 Healthcare Privacy and Security Classification System (HCS), Release 1, August 2014	Approved Standard	
PASS;SLS Release 1 June 2014	**HL7**	Privacy, Access and Security Services (PASS); Security Labeling Service (SLS) describes the conceptual-level viewpoints associated with the business requirements that relate to the content, structure, and functional behavior of information important to the Access Control area of the Privacy, Access, and Security domains within the healthcare environment.	Approved Standard	
802.1AE-2006 802.1AEbw-2013	**IEEE**	connectionless data confidentiality and integrity for media access independent protocols	Approved Standard	

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Security Services: The guarantees provided by MACsec support the following security services for stations participating in MACsec: • Connectionless data integrity • Data origin authenticity • Confidentiality • Replay protection • Bounded receive delay • And can be used to limit the nature and extent of denial of service attacks *Page 19, Section 6.9*		
802.1X-2004	**IEEE**	port based network access control	Approved Standard Under Revision?	
Open Trust Protocol	**IETF**	protocol to install, update, and delete applications and to manage security configuration in a Trusted Execution Environment	Under Development	
RFC 7925 July 2016	**IETF**	The handshaking protocol consist of three subprotocols, namely the handshake protocol, the change cipher spec protocol. And the alert	Approved Standard	

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		protocol. The handshake protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic key before the application protocol transmits or received data. *Page 5, Section 3.1*		
ISO 19731: 2017	**ISO**	Digital analytics and web analyses for purposes of market, opinion and social research Confidentiality of information: All information supplied to the service provider by the client to conduct a research project shall be treated in the strictest confidence. It shall only be used in this context and shall not be made available to third parties without the client's authorization. Confidential information shall be stored securely. *Page 16, Section 4.2* Data Security: Service providers shall provide personnel with adequate access technology controls and protocols for data centers, processing and reporting servers, and general system access, as well as encryption and password policies.	Approved Standard	

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Service providers shall ensure that security arrangements are sufficient to ensure that only those authorized can access systems and data. *Page 24, Section 6.7*		
OCF SPEC 1.0 June 28, 2017	**OCF**	Access Control: The OIC framework assumes that resources are hosted by an OIC server and are made available to OIC clients subject to access control and authorization mechanisms. The resources at the end point are protected through implementation of access control, authentication and confidentiality protection. *Page 15, Section 5.1* ACL Evaluation and Enforcement: The OIC server enforces access control over application resources before exposing them to the requestor. The security manager in the OIC sever authenticates the requestor if access is received via the secure port. If the request arrives over the unsecured port, the only ACL policies allowed are for anonymous requestors. If the anonymous ACL policy doesn't name the requested resource access is denied.	Guidance Available Reference Implementation	The Open Interconnect Consortium (OIC) has been re-launched in early 2016 as the Open Connectivity Foundation (OCF) The goal for the OCF security architecture is to protect OCF resources and all aspects of Hardware and Software that are used to support the protection of O resource.

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Page 77, Section 12.2 <u>Device Authentication:</u> Asymmetric Keys Credentials: When using symmetric keys to authenticate, the server shall include the ServerKeyExchange message and set psk_identity_hint to the server's device ID. The client shall validate that it has a credential with the Subject ID set to the server's device ID, and a credential type of PSK. If it does not, the client shall respond with an unknown_psk_identity error or other suitable error. Raw Asymmetric Key Credentials: When using raw asymmetric keys to authenticate, the client and the server shall include a suitable public key from a credential that is bound to their device. Certifications: When using certificates to authenticate, the client and server shall each include their certificate chain, as stored in the appropriate credential, as part of the selected authentication cipher suite. *Page 74, Section 10*		

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
M2M Link 08 Feb 2017	**OMA**	Access Control: In the particular case where a single LwM2M Server Account exists in the LwM2M Client, the Server must have full access right on all the Objects and Object Instances in the LwM2M Client. Access Control Object: In the presence of several LwM2M Servers, there is a need to determine if a certain LwM2M Server is authorized to instantiate a supported Object in the LwM2M Client. This kind of authorization can only be managed during a Bootstrap Phase. Furthermore, the LwM2M Client needs to determine – per Object Instance – who the "Access Control Owner" of the Object Instance is DTLS-based Security: For authentication of communicating LwM2M entities, the LwM2M protocol required that all communication between LwM2M Clients and LwM2M Servers as well as LwM2M Clients and LwM2M Bootstrap-Servers are authenticated using mutual authentication.	Approved Standard Guidance Available	Open Mobile Alliance (OMA) **What is OMA M2M?** OMA's LightweightM2M is a device management protocol designed for sensor networks and the demands of a machine-to-machine (M2M) environment.

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Page 68, Section 7.3.1		
DDS-Security specification – 2016	**OMG**	Data Distribution Service (DDS)	Approved Standard	
OpenFog RA Link	**OpenFog RA**	Identity and Identity Protection: Public-key ciphers can be used to establishing a longer-term cyber identity, e.g., for authentication. In public-key cryptography, keys come in matched pairs (public key and private key) for each user, entity, computer, or subject. The private key must be accessible only to the subject and represents the subject's digital identity in cyberspace. Hashes can be used to verify the integrity of code modules by taking the hash of the good known code module and using that to identify the module (like a unique global name). The private key of someone's key pair is like their digital identity. Private keys must be kept confidential in order to protect someone's digital	Guidance Available (has a few use cases)	**What is Fog?** A system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		identity. *Page 50, Section 5.4.2.6*		
Trust Framework v2.5 - Updated June 22, 2017	**OTA**	strategic principles to help secure IOT devices and their data when shipped and throughout their entire life-cycle	Approved Standard	Online Trust Alliance (OTA) is now an initiative within the Internet Society (ISOC)
TPM Main Part 1 Version 1.2 1 March 2011	**TCG**	Authentication and Authorized Data: Each TPM object that does not allow "public" access contains a 160-bit shared secret. This shared secret is enveloped within the object itself. The TPM grants use of TPM objects based on the presentation of the matching 160-bits using protocols designed to provide protection of the shared secret. This shared secret is called the AuthData. From the perspective of the TPM looking out, this AuthData is its sole mechanism for authenticating the owner of its objects, thus from its perspective it is authentication data. AuthData is a 160-bit shared-secret plus high-entropy random number. The assumption is the shared-secret and random number are mixed	Approved Standard Guidance Available	**What is TPM?** An industry specification by the Trusted Computing Group (TCG) that enables trust in computing platforms in general.

Identity and Access Management: **Standards that enable the use of secure, interoperable digital identities and attributes of entities to be used across security domains and organizational boundaries. Examples of entities include people, places, organizations, hardware devices, software applications, information artifacts, and physical items. Standards for identity and access management support identification, authentication, authorization, privilege assignment, and audit to ensure that entities have appropriate access to information, services, and assets. In addition, many identity and access management standards include privacy features to maintain anonymity, unlinkability, untraceability, ensure data minimization, and require explicit user consent when attribute information may be shared among entities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		using SHA-1 digesting. *Page 47, Section 8* Authorization Session Setup: The TPM provides two protocols for authorizing the use of entities without revealing the AuthData on the network on the connection to the TPM. First protocol is the Object-Independent Authorization Protocol (OIAP), the second is the Object Specific Authorization Protocol (OSAP). *Page 78, Section 13.1*		
Thread Specs Feb 13 2017	**Thread Group**	Network-wide Key: To verify the joining device and limit the effect of rogue devices attempting to join the Thread Network, the network requires the joining device to identify a trusted device and communicate solely in a point-to-point fashion with this trusted device. The trusted device policies any traffic from the joining device and forwards it to the commissioning device to allow the authentication protocol (DTLS handshake) to execute. *Page 29, Section 1.3.3.2*	Guidance Available Commercial Availability Conformity Assessment Market Acceptance	**What is Thread?** Securely and reliably connects products around the home using a robust mesh network and an open IPv6 based protocol.

2176

Information Security Management Systems: Standards provide a set of processes and corresponding security controls to establish a governance, risk, and compliance structure for information security for an organization, an organizational unit, or a set of processes controlled by a single organizational entity. An ISMS requires a risk-based approach to security that involves selecting specific security controls based on the desired risk posture of the organization and requires measuring effectiveness of security processes and controls. An ISMS requires a cycle of continual improvement for an organization to continue assessing security risks, assessing controls, and improving security to remain within risk tolerance levels by balancing security and risk tolerances.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
TR 80001-2-2 2012	**AAMI IEC**	Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls Provides a framework for the disclosure of security-related capabilities and risks necessary for managing the risk in connecting medical devices to IT-networks and for the security dialog that surrounds the IEC 80001-1 risk management of IT-network connection.		
AUTO11-A2 October 31, 2014	**CLSI**	Provides a framework for communication of information technology security issues between the in vitro diagnostic system vendor and the health care organization.	Approved Standard	
COSO Enterprise Risk Management (ERM) Framework	**COSO**	Addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment.	Approved Standard	
62443 series	**ISA/IEC**	Industrial Automation and Control Systems (IACS) standards and technical reports includes security management requirements	Status for Each Part	
13485:2016	**ISO**	requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements	Approved Standard	

Information Security Management Systems: Standards provide a set of processes and corresponding security controls to establish a governance, risk, and compliance structure for information security for an organization, an organizational unit, or a set of processes controlled by a single organizational entity. An ISMS requires a risk-based approach to security that involves selecting specific security controls based on the desired risk posture of the organization and requires measuring effectiveness of security processes and controls. An ISMS requires a cycle of continual improvement for an organization to continue assessing security risks, assessing controls, and improving security to remain within risk tolerance levels by balancing security and risk tolerances.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
27799:2016	**ISO**	information security management in health using ISO/IEC 27002	Approved Standard	
ISO 31000:2009	**ISO**	A family of standards relating to risk management codified by the International Organization for Standardization. The purpose of ISO 31000 is to provide principles and generic guidelines on risk management.	Approved Standard	
20243:2015	**ISO/IEC**	identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains	Approved Standard Conformance Testing	
27001:2013	**ISO/IEC**	This International Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system. The information security management system preserves the confidentiality, integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed.	Approved Standard Market Acceptance	
27002:2013	**ISO/IEC**	This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on	Approved Standard Market	

Information Security Management Systems: Standards provide a set of processes and corresponding security controls to establish a governance, risk, and compliance structure for information security for an organization, an organizational unit, or a set of processes controlled by a single organizational entity. An ISMS requires a risk-based approach to security that involves selecting specific security controls based on the desired risk posture of the organization and requires measuring effectiveness of security processes and controls. An ISMS requires a cycle of continual improvement for an organization to continue assessing security risks, assessing controls, and improving security to remain within risk tolerance levels by balancing security and risk tolerances.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		ISO/IEC 27001 or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environments(s).	Acceptance	
27031:2011	**ISO/IEC**	guidelines for ICT readiness for business continuity	Approved Standard	
ISO/IEC TR 27019:2013	**ISO/IEC**	information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry	Approved Standard	
Y.4408 2015	**ITU**	This Recommendation specifies the capability framework for support of the requirements of e-health monitoring (EHM) services [ITU-T Y.2065]. The scope of this Recommendation includes: – EHM conceptual framework – EHM capability framework An overview of the EHM capabilities in the various EHM components is provided in Annex A. Two EHM service deployment technical scenarios are described in Appendix I.	Approved Standard	Former ITU-T Y.2075 renumbered as ITU-T Y.4408 on 2016-02-05 without further modification and without being republished.

2179

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
TR 80001-2-2 2012	**AAMI IEC**	Application of risk management for IT-networks incorporating medical devices -- Part 2-2: Guidance for the communication of medical device security needs, risks and controls	Approved Standard	
80001-1:2010	**AAMI IEC**	Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities	Approved Standard	
Common Criteria April 2017	**Common Criteria**	Class FIA: Identification and Authentication: Families in this class address the requirements for functions to establish and verify a claimed user identity. Authentication Failures: this family contains requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. User Attribute Definition: this family defines the requirements for associating user security attributes with users as needed to support the TSF in making security decisions. Specification of Secrets: this family defines requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric.	Guidance Available	**What is Common Criteria?** Provides a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. Definitions: **TOE:** a set of software, firmware and/or hardware possibly accompanied by user and administrator guidance documentation. **TSF:** consists of all hardware, software and firmware of a TOE that is either directly or indirectly relied upon for security enforcements.

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		User Authentication: this family defines the types of user authentication mechanisms supported by the TSF. User Identification: defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification. *Page 87, Section 12* <u>Class FCS: Cryptographic Support:</u> The TSF (TOE Security Functionality) may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel, and data separation. This class is composed of two families: FCS_CKM and FCS_COP. Cryptographic Key Management (FCS_CKM): intended to support the lifecycle of cryptographic keys and defines requirements for: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction.		

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Cryptographic Operation (FCS_COP): concerned with the operational use of those cryptographic keys. Typical cryptographic operations include data encryption and/or decryption, digital signature generation and/or verification, cryptographic checksum generation for integrity and/or verification of checksum, secure hash (message digest), cryptographic key encryption and/or decryption, and cryptographic key agreement. *Page 48, Section 10*		
DTSec Standard Version 1.0 May 23, 2016	**DTS**	Following the general framework of establishing security standards for information and electronic systems (ISO/IEC 15408), the DTSec program calls for the specification of security requirements for wireless diabetes devices. These requirements have the following objectives: • To establish the general requirements for connected devices that meet the balanced needs for security and clinical application. • To identify possible and potential threats related to the various components and interfaces of the connected devices, such as network, storage, software, connected peer devices, and cryptography.	Approved Standard	Diabetes Technology Society (DTS)

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• To define a set of generalized requirements that apply to families of similar devices • To define a set of specific mandatory requirements, derived from the generalized requirements, corresponding to specific connected-diabetes device products and components. • To outline additional optional functional requirements for manufacturers to consider adding to their toolbox for future development. <u>Identification of assets, threats and vulnerabilities:</u> DTSec leverages ISO 15408 to help developers identify and document, using the ISO 15408 standardized framework, the threats applicable to medical device products and components. The DTSec assurance-through-evaluation program helps developers identify vulnerabilities by augmenting the developer secure development lifecycle with independent vulnerability assessment by qualified cybersecurity test labs. <u>Assessment of the impact of threats and vulnerabilities on the device functionality and end user/patients:</u>		

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		DTSec helps to assess the impact of threats and vulnerabilities on device functionality and end users/patients by requiring developers to consider relevant threats and how they might impact safe clinical use. DTSec also helps assess the impact of vulnerabilities discovered during the security evaluation program DTSec also helps stakeholders balance the need for security with essential clinical performance. <u>Assessment of the likelihood of a threat and of a vulnerability being exploited:</u> DTSec helps to assess the likelihood of a vulnerability being exploited. As part of the vulnerability assessment requirement included in the Protection Profiles and Security Targets, the security evaluator will attempt to understand not only whether a vulnerability is exploitable but also what level of attack potential is required to exploit. <u>Determination of risk levels and suitable mitigation strategies:</u> DTSec helps to determine suitable mitigation strategies; as part of the protection profile and		

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Security Target authoring process, the DWG, evaluators, and developers work together to ensure that the security threats while balancing overall safe clinical use. Assessment of residual risk and risk acceptance criteria: The is a central focus of the DTSec assurance program. During a security evaluation, the evaluator must determine whether residual risk are acceptable relative to the assurance requirements specified in the Security Target. *Page 6, Sections 1 to 5*		
HITRUST CSF v9 10 September 2017	**HITRUST Alliance**	Information Security Policy Objective: To provide management direction in line with business objectives and relevant laws and regulations, demonstrate support for, and commitment to information security through the issue and maintenance of information security policies across the organization. Specification: The Information Security policy documents shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles. Security Requirements of Information Systems:	Approved Standard Under Revision Guidance Available	

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Objective: To ensure that security is an integral part of information systems Specification: Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls Implementation: The organization shall develop, disseminate and review/update annually: • A formal, documented system and information integrity policy that addresses purpose, score, roles, responsibilities, management commitment, coordination among organizational entities and compliance • Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls *Page 160, Category 4*		
RFC 7400 6LoWPAN-GHC November	**IETF**	Security Considerations: As usual in protocols with packet parsing/construction, care must be taken in implementations to avoid buffers overflows and out-of-area references during decompression.	Proposed Standard	

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
2014		In a 6LoWPAN stack, sensitive information will normally be protected by transport- or application-layer (or even IP-layer) security, which are all above the adaptation layer, leaving no sensitive information to compress at the GHC level. However, a 6LoWPAN deployment that entirely depends on Media Access Control (MAC) layer security may be vulnerable to attacks that exploit redundancy information disclosed by compression to recover information about secret values. This attack is fully mitigated by not exposing secret values to the adaptation layer or by not using GHC in deployments where this is done. *Page 10, Section 5*		
RFC 7959 August 2016	**IETF**	Block-Wise Transfer in CoAP Security Considerations: Where access to a resource is only granted to clients making use of specific security associations, all blocks of that resource must be subject to the same security checks; it must not be possible for unprotected exchanges to influence blocks of an otherwise protected resource. Mitigating Resource Exhaustion Attacks: Wherever possible, severs should minimize the opportunities to create state for untrusted sources	Approved Standard	

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		by using stateless approaches. Mitigating Amplification Attacks: A CoAP server can reduce the amount of amplification it provides to an attacker by offering large resource representations only in relatively small blocks. *Page 33, Section 7*		
15408-1:2009	**ISO/IEC**	general concepts and principles of IT security evaluation	Approved Standard Conformity Assessment	
15408-2:2008	**ISO/IEC**	defines the content and presentation of the security functional requirements to be assessed in a security evaluation	Approved Standard Conformity Assessment	
15408-3:2008	**ISO/IEC**	defines the assurance requirements of the evaluation criteria	Approved Standard Conformity Assessment	
17825:2016	**ISO/IEC**	specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4	Approved Standard	

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
18367:2016	**ISO/IEC**	guidelines for cryptographic algorithms and security mechanisms conformance testing methods	Approved Standard	
19790:2006	**ISO/IEC**	specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems	Approved Standard	
19790:2015	**ISO/IEC**	security requirements for cryptographic modules	Approved Standard Testing Conformity Assessment Market Acceptance	
20243:2015	**ISO/IEC**	identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains	Approved Standard Conformity Assessment	
24759:2014	**ISO/IEC**	test requirements for cryptographic modules	Approved Standard Testing Conformity	

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
			Assessment Market Acceptance	
CD 19896-2	**ISO/IEC**	competence requirements for information security testers and evaluators – Part 2 Knowledge, skills, and effectiveness requirements for ISO/IEC 19790 testers	Under Development	
CD 20085-1	**ISO/IEC**	test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules – Part 1: Test tools and techniques	Under Development	
CD 20085-2	**ISO/IEC**	test tool requirements and test tool calibration methods for use in testing noninvasive attack mitigation techniques in cryptographic modules – Part 2: Test calibration methods and apparatus	Under Development	
DIS 19896-1	**ISO/IEC**	competence requirements for information security testers and evaluators – Part 1 Introduction, concepts and general requirements	Under Development	
TR 30104:2015	**ISO/IEC**	guidance on physical security attacks, mitigation techniques and security requirements	Approved Standard	
F.748.1	**ITU**	Describes the requirements and common characteristics of the Internet of things (IoT) identifier for the IoT service.	Approved Standard	
2900-1 2900-2-2	**UL**	Access Control, User Authentication and User Authorization:	Guidance Available	UL 2900 outlines offer testable cybersecurity criteria for network-connectable products and systems to

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
Feb 2016		• Product operation or management services which may affect or alter the security of the product shall require user authentication prior to access • User authentication services to the product shall implement a session time-out or other appropriate mechanism to prevent perpetual authorization • Services that are accessible over a remote interface shall require user authentication prior to access • Services that are accessible over a remote interface shall require user authentication prior to access. • Once a user is authenticated and granted remote access to the product, the product shall reject and record any attempt to setup another remote connection using the same user identity. • The storage of the authentication credential on the product shall not be in plaintext and shall be protected from unauthorized disclosure or modification *Doc 1, Page 8, Section 8 & Doc 2, Page 6, Section 8*		assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness.

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Risk Management: When designing the product, the vendor shall establish and document a security risk analysis for the product, containing: • An identification of all product functionalities and all data stored, processed or used by the product • A list of all threats for the product, its functionalities and data • An assessment of the impact of each identified threat, should it become a reality • An assessment of the likelihood of each identified threat • A determination of the resulting risk level of each threat, considering its impact and likelihood • Risk acceptance criteria, i.e., clear criteria to determine whether or not a given risk level is acceptable. • A determination of suitable risk controls to mitigate each threat with an unacceptable risk level • An assessment of the residual risk level for each threat after application of these risk controls.		

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• The vendor shall document a risk evaluation method for the possible presence of known (types of) vulnerabilities in the product • If the vendor has allowed for the presence of any known vulnerabilities in the product, the vendor's security risk analysis for the product shall contain a description of each accepted known vulnerability. *Doc 1, Page 12, Section 12* <u>Cryptography:</u> Symmetric Algorithms: Block and Stream Ciphers Asymmetric Algorithms and Techniques: • Integer Factorization Based Mechanisms (ISO/IEC 9796-2) • Discrete Logarithm Based Mechanisms (ISO/IEC 9796-3) • Digital Signatures with Appendix (ISO/IEC 14888 all parts) • Cryptographic Techniques Based on Elliptic Curves (ISO/IED 15946 all parts) • Encryption Algorithms – Asymmetric Ciphers (ISO/IEC 18033-2) Message authentication codes:		

IT System Security Evaluation Standards that are used to provide: security assessment of operational systems; security requirements for cryptographic modules; security tests for cryptographic modules; automated security checklists; and security metrics.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• Message Authentication Codes (MACs) (ISO/IEC 9797-2) • Hash Functions (ISO/IEC 10118-2/10118-3/10118-4) Authentication Encryption: Authenticated Encryption (ISO/IEC 19772 all parts) *Page 8, Section 10*		

2180

2181

2182

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
3GPP 5G	**3GPP**	5th generation mobile networks/wireless systems	Under Development	
GPRS	**3GPP**	Link layer/Physical Layer General Packet Radio Service	Approved Standard	
Long-Term Evolution (LTE)	**3GPP**	standard for high-speed wireless communication for mobile phones and data terminals	Approved Standard Market Acceptance	
80001-2-3 2012	**AAMI IEC**	Application of risk management for IT-networks incorporating medical devices — Part 2-3: Guidance for wireless networks Offers practical techniques to address the unique risk management requirements of operating wirelessly enabled medical devices in a safe, secure and effective manner.	Approved Standard	
LIS09-A 2003	**CLSI**	Standard Guide for Coordination of Clinical Laboratory Services Within the Electronic Health Record Environment and Networked Architectures, LIS9AE	Approved Standard	
Security Guidance for Early Adopters of IoT - 2015	**CSA**	security guidance for the secure implementation of IoT-based systems	Approved Standard	
Protocol Specification v1.1	**DASH7 Alliance**	Wireless Sensor and Actuator Network Protocol	Approved Standard	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
24 January 2017			Market Acceptance	
Postmarket Management of Cybersecurity in Medical Devices	**FDA**	security guidance for medical devices that contain software	Approved Standard	
CLP.14 v1.1	**GSMA**	Network Security Principles: The most fundamental security mechanisms provided by a communication network are: • Identification and authentication of the entities involved in the IoT Service • Access control to the different entities that need to be connected to create the IoT Service • Data protection in order to guarantee the security (confidentiality, integrity, availability, authenticity) and privacy of the information carried by the network for the IoT Service. Processes and mechanisms to guarantee availability of network resources and protect them against attack *Page 11, Section 3*	Guidance Available	The GSMA IoT Security Guidelines are backed by an IoT Security Assessment scheme that enables companies to build secure IoT devices and solutions.
62591:2016	**IEC**	Wireless Highway Addressable Remote Transducer Protocol (HART); industrial wireless sensor networks)	Approved Standard	
1609	**IEEE**	Link layer/Physical Layer	Approved Standards	See Existing Standards Created

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		The IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications.		by this Working Group
2600.1-2009	**IEEE**	a protection profile in operational Environment A	Approved Standard Conformity Assessment	
2600.2-2009	**IEEE**	a protection profile for hardcopy devices operational Environment B	Approved Standard Conformity Assessment	
2600.3-2009	**IEEE**	a protection profile for hardcopy devices in operational Environment C	Approved Standard Conformity Assessment	
2600.4-2010	**IEEE**	a profile for hardcopy devices operational Environment D	Approved Standard Conformity Assessment	
2600-2008	**IEEE**	hardcopy device and system security	Approved	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
			Standard	
802.11-2016	**IEEE**	(Wi-Fi) Link Layer/Physical Layer <u>Overview of the services:</u> There are many services specified by IEEE Std 802.11. Six of the services are used to support medium access control (MAC) service data unit (MSDU) delivery between STAs. Three of the services are used to control IEEE 802.11 LAN access and confidentiality. Two of the services are used to provide spectrum management One of the services provides support for LAN applications with QoS requirements. Another of the services provides support for higher layer timer synchronization. One of the services is used for radio measurement. *Page 217 Section 4.5*	Approved Standard Market Acceptance	
802.11ah-2016	**IEEE**	Link Layer/Physical Layer uses sub-1 GHz license-exempt bands; provide extended range Wi-Fi networks, compared to conventional Wi-Fi networks operating in the 2.4 GHz and 5 GHz bands.	Approved Standard Market Acceptance	
802.11ai-2016	**IEEE**	Link Layer/Physical Layer This amendment defines mechanisms that provide IEEE 802.11 networks with fast initial link setup methods that do not degrade the security offered by Robust Security Network Association (RSNA) already	Approved Standard Market Acceptance	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		defined in IEEE 802.11.		
802.15.4-2015	**IEEE**	Link Layer/Physical Layer Low-Rate Wireless Personal Area Networks (LR-WPANs) <u>Security Overview:</u> The MAC sublayer is responsible for providing security services on specified incoming and outgoing frames when requested to do so by the higher layers. This standard supports the following security services: • Data confidentiality • Data authenticity • Replay protection (when not using TSCH mode)	Approved Standard Market Acceptance	
802.15.6-2012	**IEEE**	Link Layer/Physical Layer Wireless Body Area Network (WBAN) <u>Security Services:</u> the security association protocols shall be based on the Diffie-Hellman key exchange employing the elliptic curve public key cryptography. • Master key pre-shared association – a node and a hub shall each have a secret pre-shared MK prior to running the MK pre-shared association protocol to activate their pre-shared MK as their shared MK for their creation.	Approved Standard Market Acceptance	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• Unauthenticated association – a node and a hub shall each require no authentication credentials such as a shared secret or human intervention prior to running the unauthenticated association protocol to generate their shared MK for their PTK creation. • Public key hidden association – a node and a hub shall have a secured, secret transfer of the node's public key to the hub, typically through an out-of-band channel, prior to running the public key hidden association protocol to generate their shared MK for their PTK creation. • Password authenticated association – a node and a hub shall each have a secret shared password prior to running the password authenticated association protocol to generate their shared MK for their PTK creation. • Display authenticated association – a node and a hub shall each have a display of a 5-digit decimal number prior to running the display authenticated association protocol to generate their shared MK for their PTK creation.		
802.15.7-2011	**IEEE**	Link Layer/Physical Layer IEEE standard for local and metropolitan area networks – part 15.7: Short-range wireless optical communication visible light, 2011. The purpose of this standard is to provide a global standard for short-range optical wireless communication using visible light. The standard provides (i) access to several hundred THz of unlicensed spectrum; (ii) immunity to electromagnetic interference and noninterference with Radio Frequency (RF) systems;	Approved Standard	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		(iii) additional security by allowing the user to see the communication channel; and (iv) Communication augmenting and complementing existing services (such as illumination, display, indication, decoration, etc.) from visible-light infrastructures.		
6LoWPAN	**IETF**	(IPv6 over Low-power Wireless Personal Area Networks) A set of standards defined by the IETF and based on IEEE 802.15.4. The base standard is IETF RFC4944. 6LoWPan standards enable the efficient use of IPv6 over low-power, low-rate wireless networks on simple embedded devices through an adaptation layer and the optimization of related protocols.	Approved Standard	
draft-ietf-tls-tls13-22	**IETF**	Transport Layer Security (TLS) Protocol Version 1.3	Under Development	
RFC 2460-1998	**IETF**	Network Layer core specification that enhancements IPv4.	Approved Standard	
RFC 4347-2006	**IETF**	Datagram Transport Layer Security (TLS) Protocol Version 1.2	Approved Standard	
RFC 6347 January 2012	**IETF**	Specifies version 1.2 of the Datagram Transport Layer Security (DTLS) protocol. Security Considerations: The primary additional security considerations raised by DTLS is that of denial of service. DTLS includes a cookie exchange designed to protect against denial of service. However,	Approved Standard Guidance Available	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		implementation which do not use this cookie exchange are still vulnerable to DoS. In particular, DTLS servers which do not use this cookie exchange may be used as attack amplifiers even if they themselves are not experiencing DoS. Therefore, DTLS servers should use the cookie exchange unless there is good reason to believe that amplification is not a threat in their environment. Clients must be prepared to do a cookie exchange with every handshake.	Commercial Availability Market Acceptance	
RFC 7252 June 2014	**IETF**	Constrained Application Protocol (CoAP) Parsing the Protocol and Processing URIs: CoAP attempts to narrow the opportunities for introducing network-facing application vulnerabilities by: reducing parser complexity, giving the entire range of encodable values a meaning where possible, and by aggressively reducing complexity that is often cause by unnecessary choice between multiple representations that mean the same thing. Risk of Amplification: An attacker might use CoAP nodes to turn a small attack packet into a larger attack packet, an approach known as amplification. There is therefore a danger that CoAP nodes could become implicated in denial-of-service attacks by using the amplifying properties of the protocol. As a mitigating factor, many constrained networks will only be able to generate a small amount of traffic, which may make CoAP nodes less attractive for this attack. Therefore, large amplification factors should not be provided in the response if the request is not authenticated. IP Address Spoofing Attacks: Due to the lack of handshake in UDP, a	Approved Standard Guidance Available Commercial Availability	**What is CoAP?** CoAP is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. The protocol is designed for machine-to-machine (M2M) applications such as smart energy and building automation.

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		rogue endpoint that is free to read and write messages carried by the constrained network may easily attack a single endpoint, a group of endpoints, as well as a whole network. Response spoofing by off-path attackers can be detected and mitigated even without transport later security by choosing a nontrivial, randomized token in the request. *Page 80, Section 11* Note: Like MQTT, CoAP does not provide these services but rather recommends another standard D-TLS. Securing CoAP: The device will be in one of the four security modes: NoSec: There is no protocol-level security (DTLS is disabled) PreSharedKey: DTLS is enabled, there is a list of pre-shared keys, and each key includes a list of which nodes it can be used to communicate with. RawPublicKey: DTLS is enabled and the device has an asymmetric key pair without a certificate (a raw public key) that is validated using an out-of-band mechanism. Certificate: DTLS is enabled and the device has an asymmetric key pair with an X.509 certificate that binds it to its subject and is signed by some common trust root. *Page 71, Section 9.1.3.1*		

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
State of the Art and Challenges for the Internet of Things draft-irtf-t2trg-iot-seccons-02 March 31, 2017	**IETF**	Network Security: SecProf_1: • Network key creating an industry security domain at L2 ensuring authentication and freshness of exchanged data • Inter-domain authentication/secure handoff • Secure routing needed at L3 • Secure multicast requires origin authentication • 6LBR (HTTP-CoAP proxy) requires verification of forwarded messages and messages leaving or entering the 6LoWPAN/CoAP network. Sec_Prof_3: • Network key creating an industry security domain at L2 ensuring authentication and freshness of exchanged data • Secure routing needed (integrity & availability) at L3 within 6LoWPAN/CoAP • Secure multicast requires origin authentication SecProf_4: • Network key creating an industry security domain at L2 ensuring authentication and freshness of exchanged data • Inter-domain authentication/secure handoff • Secure routing needed at L3 • Secure multicast requires origin authentication • 6LBR (HTTP-CoAP proxy) requires verification of forwarded messages and messages leaving or entering the 6LoWPAN/CoAP network. *Page 31 Section 6.5*	Under Development	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
	Insteon	low-cost devices to be networked together using the powerline, radio frequency (RF), or both		
19079:2016	**ISO**	6LoWPAN/IPv6 Security module: Communication security must ensure confidentiality, integrity and authentication between two peers interconnected through the Internet. The IT-S security module shall carry out the following actions: • Communicates with the security entity through the SN-SAP interface • Communicates with other modules in the IoT MSE functional block • Enables the security protocols for the required security services • Reports available 6LoWPAN security capabilities to the security entity through the SN-SAP	Approved Standard	
180003: 2010	**ISO/IEC**	Defines the RFID communication used by Near Field Communication (NFC) devices.	Approved Standard	
X.1362	**ITU**	Recommendation ITU-T X.1362 : Simple encryption procedure for Internet of things (IoT) environments Specifies encryption with associated mask data (EAMD) for the Internet of things devices. It describes EAMD and how it provides a set of security services for traffic using EADM.	Approved Standard	
LoRaWAN	**LoRa Alliance**	Link layer/Physical Layer LoRaWAN is a wireless protocol for IoT applications that is available in integrated circuits. The protocol specification is built on top of the LoRa technology developed by the LoRa Alliance. It uses unlicensed radio	Approved Standard Market Acceptance	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		spectrum in the Industrial, Scientific and Medical (ISM) bands to enable low power, wide area, bi-directionally secure communication between remote sensors and gateways connected to the network.		
MQTT Link Dec 2015	**MQTT**	Note: References to other protocols. Authentication of Clients by the Server: Implementations can choose how to make use of the content of these fields. They may provide their own authentication mechanism, use an external authentication such as LDAP or OAuth tokens, or leverage operating system authentication mechanisms. When TLS is used: SSL Certificates sent from the Client can be used by the Server to authenticate the Client. When VPN is used: between the Clients and Servers, VPN can provide confidence that data is only being received from authorized Clients. Authentication of the Server by the Client: The MQTT protocol is not trust symmetrical; it provides no mechanism for the Client to authenticate the Server, When TLS is used: SSL Certificates sent from the Server can be used by the Client to authenticate the Server. When VPN is used: between Clients and Servers, VPN can provide confidence that Clients are connecting to the intended Server. *Page 61, Sections 5.4.1 & 5.4.3*	Guidance Available Approved Standard	**What is MQTT?** MQTT is a machine-to-machine (M2M)/" Internet of Things" connectivity protocol.

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Note: MQTT does not provide any of these services. The standard recommends that other standards be applied, e.g., TLS. Integrity of Application Messages and Control Packets: Application Messages: applications can independently include hash values in the messages. This can provide integrity of the contents of Publish Control Packets across the network and at rest. When TLS is used: provides hash algorithms to verify the integrity of data sent over the network. When VPN is used: VPNs connecting Clients and Servers can provide integrity of data across the section of the network covered by a VPN. Privacy of Application Messages and Control Packets: Application Messages: an application might independently encrypt the contents of its messages. This could provide privacy of the Application Message both over the network and at rest. When TLS is used: can provide encryption of data sent over the network. When VPN is used: to connect Clients and Servers, VPNs can provide privacy of data across the section of the network covered by a VPN. Non-repudiation of message transmission: Application designers might need to consider appropriate strategies to achieve to end non-repudiation.		

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Page 62 Section 5.4.4, 5.4.5. & 5.4.6		
OCF 1.1.1 Security Specification – 2017	**OCF**	defines security objectives, philosophy, resources and mechanism that impacts base layers of the Core specification	Approved Standard	
OCF SPEC 1.0 June 28, 2017	**OCF**	Security Theory of Operation: 1. The OIC Client establishes a network connection to the OIC Server. The connectivity abstraction layer ensures the devices are able to connect despite differences in connectivity options. 2. The OIC Client and OIC Server establishes a secure end-to-end channel that protects the exchange of OIC messages and resources passed between OIC devices. Encryption keys are stored securely in the local platform. 3. ACL permission is applied to the requested resource where the decision to allow or deny access is enforced by the OIC Server's Secure Resource manager. OIC resource protection includes protection of data both while at rest and during transit *Page 14, Section 5*	Approved Standard Guidance Available Reference Implementation	The Open Interconnect Consortium (OIC) has been re-launched in early 2016 as the Open Connectivity Foundation (OCF) The goal for the OCF security architecture is to protect OCF resources and all aspects of Hardware and Software that are used to support the protection of

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
				OCF resource.
OMA Device Management Security – May 2016	OMA	Open Mobile Alliance (OMA) specifies protocols and mechanisms to achieve the management of mobile devices, services access and software on connected devices for mobile networks and the Internet of Things (IoT). describes requirements in general; provides description of transport layer security application layer security, etc.; and describes security mechanisms for integrity, confidentiality and authentication	Approved Standard	
OMA M2M	**OMA**	Lightweight Machine to Machine Technical Specification Approved Version 1.0 – 08 Feb 2017 DTLS: CoAP is secured using the DTLS protocol which is based on TLS. DTLS is a communication security solution for datagram based protocols (such as UDP). It provides a secure handshake with session key generation, mutual authentication, data integrity and confidentiality. *Page 58, Section 7.1.2*	Approved Stanard Guidance Available	**What is OMA M2M?** OMA's LightweightM2M is a device management protocol designed for sensor networks and the demands of a machine-to-machine (M2M) environment.
OpenFog RA	**OpenFog Consortium**	Network Based Security Threats and Mitigation: The fog node needs to be protected from various network-based security threats, which may include:	Guidance Available (has a few use	**What is Fog?** A system-level horizontal

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• Denial of Service attacks • Intrusion • DNS spoofing • ARP spoofing or poisoning • Buffer overflows *Page 64, Section 5.5.1.4*	cases)	architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.
	SigFox	Link Layer/Physical Layer Dedicated low-power, low-bandwidth proprietary cellular network optimized for short data transmissions common with IoT devices. Specializing in industrial networking, e.g., home security systems.		
Doc 1: RFC 4919 August 2007 Doc 2: Thread Specs Feb 13 2017	**Thread Group**	TLS: A TLS (Transport Layer Security) handshake is used for EC-JPAKE, which can be used in both TLS and DTLS. *Doc 2, Page 28, Section 1.3.3.1* 6LoWPAN: IPv6 over LoWPAN (6LoWPAN) applications often require confidentiality and integrity protection. This can be provided at the application, transport, network, and/or at the link layer (i.e., within the 6LoWPAN set of specifications).	Guidance Available Commercial Availability Conformity Assessment Market Acceptance	**What is Thread?** Securely and reliably connects products around the home using a robust mesh network and an open IPv6 based protocol.

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		IEEE 802.15.4: Link layer security is used because most IEEE 802.15.4 devices already have support for AES link-layer security. ECB, CBC, OFB, and CFB provide only confidentiality for encrypting longer messages, CCM* mode is designed to ensure both confidentiality and message integrity. *Doc 1, Page 9, Section 6*		
TIA/EIA-95-B (March 1999)	**TIA/EIA**	code division multiple access modulation for digital radio voice and data	Approved Standard	
XMPP	**XSF**	E**x**tensible **M**essaging and **P**resence **P**rotocol (XMPP) XMPP Standards Foundation XMPP is designed for real-time instantaneous messaging applications and uses a federated network of XMPP servers as message brokers to allow communication between clients. Servers provide each client with an authenticated identity and clients are authenticated by the servers when they connect. The XMPP Standards Foundation (XSF) publishes a set of extensions which are openly reviewed and discussed within the forum and free for anybody to use. These extensions are called XMPP Extension Protocols (XEPS). There are several XEPs to support XMPP's role in IoT, e.g., XMPP-IoT.	Approved Standards Under Development	The core specifications for XMPP are developed at the Internet Engineering Task Force (IETF) - see RFC 6120, RFC 6121, and RFC 7622 (along with a WebSocket binding defined in RFC 7395). ISO/IEC/IEEE

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
				P21451-1-4 XMPP INFC WG is the IEEE initiative tying the XMPP-IoT initiative into the IEEE standards structure.
ZigBee Pro Link March 2014 ZigBee IP Link	**Zigbee Alliance**	ZigBee Pro: Security Architecture: the ZigBee security architecture includes security mechanisms at two layers of the protocol stack. The NWK and APS layers are responsible for the secure transport of their respective frames. Furthermore, the APS sublayer provides services for the establishment and maintenance of security relationships. The ZigBee Device Object (ZDO) manages the security policies and the security configuration of a device. *Page 401, Section 4.2.1.4* ZigBee IP: ZigBee IP offers extensive security features, including PANA/EAP based network authentication and admission control, network re-keying, AES-128-CCM based layer 2 encryption, and TLS application layer authentication and encryption. ZigBee IP is the first open standards-based IPv6 specification for wireless sensor networks. The ZigBee alliance made a significant investment to bring IPv6 network protocols to IEEE 802.15.4 wireless	Approved Standard Guidance Available Commercial Availability Market Acceptance	

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		mesh networks. The ZigBee IP specification offers a scalable architecture with end-to-end IPv6 networking based on standard Internet protocols, such as 6LowPAN, IPv6, PANA, RPL, TCP, TLS and UDP to a create cost-effective and energy-efficient wireless mesh network. The ZigBee specification enhances the IEEE 802.15.4 standard by adding network and security layers and an application framework. From this foundation, Alliance developed standards can be used to create a multi-vendor interoperable solutions. For custom application where		
ZigBee Application Standards Link	**Zigbee Alliance**	Building Automation: Secures Building Automation networks by the use of AES 128 encryption, keys, and device authentication. Encryption secures access to critical building management information from eavesdropping. Health Care: AES 128 encryption secures personal information. Regional regulatory compliance simplifies implementation. Home Automation: Easily add devices to create an integrated smart home security system. Built-in security ensures integrity of smart home. Input Light Link: AES 128 encryption used to protect lighting network against	Guidance Available Commercial Availability	**What is ZigBee?** A specification for a suite of high-level communication protocols used to create personal area networks built from small, low-power digital radios

Network Security: **Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		unauthorized use. Device authentications secures networks from neighboring networks. Uses selected Zigbee channels to maximize performance and coexistence with other wireless devices in homes. Conformance guaranteed with Zigbee Certified testing conducted by independent test facilities. Retail Services: Integrated security. AES 128 encryption secures personal information. Server-driven – no personal data on handheld employee or consumer devices. Smart Energy: Support for consumer-only, utility-only or shared networks. Automatic, secure network registration using either pre-installed keys or standard public-key cryptography methods. Support for ECC public key infrastructure for authentication and mobility. Data encryption.		
Z-Wave Link August 2016	**Z-Wave**	Tier Z-Wave security: Z-WaveSec. – Z-Wave Security Command Class v2: Target: nodes exchanging non-personal data By employing the AES128 block cipher technology, Z-Wave is protected against modification, fabrication, and replay attacks. Authentication: 128-bit authentication key with a 64-bit MAC.	Guidance Available Commercial Availability	**What is Z-wave?** A wireless communications protocol used primarily for home automation.

Network Security: Standards that provide security requirements and guidelines on processes and methods for the secure management, operation and use of information, information networks, and their inter-connections. Such standards-based technologies can help to assure the confidentiality and integrity of data in motion, assure electronic commerce, and provide for a robust, secure and stable network and Internet.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Confidentiality: encryption with a 128-bit encryption key. Single Network Key, In-band initial symmetrical key exchange Z-WaveSecIP – Hybrid Security Command Class v1 and Security Link Key Extension: Target: nodes exchanging personal data Confidentiality, Authentication, Fabrication robust – AES128 based. Asymmetric key exchange, Network + Link Keys Certifications installed in nodes. Z-WaveSecSmartCard – Prepayment Encapsulation Command Class Target: nodes exchanging payment data Allows Smartcard payment & Security information to be exchanged via Z-Wave *Page 181, Section 7.2.3*		

2183

2184

2185

Security Automation and Continuous Monitoring (SACM): Standards that describe protocols and data formats that enable the ongoing, automated collection, monitoring, verification, and maintenance of software, system, and network security configurations, and provide greater awareness of vulnerabilities and threats to support organizational risk management decisions. Automation protocols also include standards for machine-readable vulnerability identification and metrics, platform and asset identification, actionable threat information and policy triggers for actions to respond to threats and policy violations. Automated activities would include a Security Operation Center (SOC) to ensure autonomous and continuing monitoring and evolution of the security state of assets based upon prescribed events				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
Remote Provisioning Architecture for Embedded UICC Technical Specification – 2016	**GSMA**	provides a technical description of the GSMA's 'Remote Provisioning Architecture for Embedded Universal Integrated Circuit Card'	Approved Standard	
Remote Provisioning Architecture for Embedded UICC Test Specification - 2015	**GSMA**	provides a technical description of the 'over the air' remote provisioning mechanism for machine-to-machine devices	Approved Standard	
HITRUST CSF v9 10 September 2017	**HITRUST Alliance**	Monitoring: Objective: ensure information security events are monitored and recorded to detect unauthorized information processing activities in compliance with relevant legal requirements. Audit Logging: Specification: Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. Implementation: audit logs shall include: • A unique user identifier • A unique data subject identifier	Approved Standard Under Revision Guidance Available	

Security Automation and Continuous Monitoring (SACM): **Standards that describe protocols and data formats that enable the ongoing, automated collection, monitoring, verification, and maintenance of software, system, and network security configurations, and provide greater awareness of vulnerabilities and threats to support organizational risk management decisions. Automation protocols also include standards for machine-readable vulnerability identification and metrics, platform and asset identification, actionable threat information and policy triggers for actions to respond to threats and policy violations. Automated activities would include a Security Operation Center (SOC) to ensure autonomous and continuing monitoring and evolution of the security state of assets based upon prescribed events**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		• The function performed by the user • The time and date that the function was performed. Monitoring System Use: Specifications: procedures for monitoring use of information processing systems and facilities shall be established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly. Implementation: items that shall be monitored include: • Authorized access • Unauthorized access attempts Administrator and Operator Logs: Specification: System administrator and system operator activities shall be logged and regularly reviewed. Clock Synchronization: Specification: The clocks of all relevant information processing systems within the organization or security domain shall be synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines. *Page 414, Section 9.10*		
TR 62443-2-3:2015	**IEC**	describes requirements for asset owners and industrial	Approved	

Security Automation and Continuous Monitoring (SACM): Standards that describe protocols and data formats that enable the ongoing, automated collection, monitoring, verification, and maintenance of software, system, and network security configurations, and provide greater awareness of vulnerabilities and threats to support organizational risk management decisions. Automation protocols also include standards for machine-readable vulnerability identification and metrics, platform and asset identification, actionable threat information and policy triggers for actions to respond to threats and policy violations. Automated activities would include a Security Operation Center (SOC) to ensure autonomous and continuing monitoring and evolution of the security state of assets based upon prescribed events				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program	Standard	
Definition of the ROLIE Software Descriptor Extension	**IETF**	This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type category and related requirements needed to support Software Record and Software Inventory use cases. The 'software-descriptor' information type is defined as a ROLIE extension. Additional supporting requirements are also defined that describe the use of specific formats and link relations pertaining to the new information type.	Under Development	
IETF RFC 7632	**IETF**	Endpoint Security Posture Assessment: Enterprise Use Cases his memo documents a sampling of use cases for securely aggregating configuration and operational data and evaluating that data to determine an organization's security posture. From these operational use cases, we can derive common functional capabilities and requirements to guide development of vendor-neutral, interoperable standards for aggregating and evaluating data relevant to security posture.	Under Development	Submitted to IESG for Publication
Security Automation and Continuous Monitoring (SACM) Documents	**IETF**	A set of standards to enable assessment of endpoint posture. A set of standards for interacting with repositories of content related to assessment of endpoint posture.	Under Development	

Security Automation and Continuous Monitoring (SACM): Standards that describe protocols and data formats that enable the ongoing, automated collection, monitoring, verification, and maintenance of software, system, and network security configurations, and provide greater awareness of vulnerabilities and threats to support organizational risk management decisions. Automation protocols also include standards for machine-readable vulnerability identification and metrics, platform and asset identification, actionable threat information and policy triggers for actions to respond to threats and policy violations. Automated activities would include a Security Operation Center (SOC) to ensure autonomous and continuing monitoring and evolution of the security state of assets based upon prescribed events				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Includes: RFC 7632, Endpoint Security Posture Assessment: Enterprise Use Cases 2015-09 RFC 8248 Security Automation and Continuous Monitoring (SACM) Requirements 2017-09	Approved Standard	
IIC Industrial Internet of Things, Volume G4: Security Framework - 2016	**IIC**	security framework identifies and explains how risks associated with security and privacy threats may be identified, evaluated and mitigated using technologies and processes	Approved Standard	
Dependability Assurance Framework for Safety-Sensitive Consumer Devices Specification Version 1.0 February 2016	**OMG**	Defines a metamodel for representing structured assurance cases. An Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements. An Assurance Case is a document that facilitates information exchange between various system stakeholder such as suppliers and acquirers, and between the operator and regulator, where the knowledge related to the safety and security of the system is communicated in a clear and defendable way. Each assurance case should communicate the scope of the system, the operational context, the claims, the safety and/or security arguments, along with the corresponding evidence.	Approved Standard	

2186
2187

2188

Software Assurance: **Standards that describe requirements and guidance for significantly decreasing the likelihood of software having vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web, software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
TIR 80001-2-4 2012	**AAMI IEC**	Application of risk management for IT-networks incorporating medical devices -- Part 2-4: General implementation guidance for Healthcare Delivery Organizations	Approved Standard	
TIR36:2007	**AAMI**	Validation of software for regulated processes Applies to any software used to automate device design, testing, component acceptance, manufacturing, labeling, packaging, distribution, and complaint handling or to automate any other aspect of the quality system as defined by the Quality System Regulation (21 CFR 820). In addition, it applies to software used to create, modify, and maintain electronic records and to manage electronic signatures that are subject to the validation requirements (21 CFR 11).	Approved Standard	
TIR45:2012	**AAMI**	Guidance on the use of agile practices in the development of medical device software Provides recommendations for complying with international standards and U.S. Food and Drug Administration (FDA) guidance documents when using agile practices to develop medical device software.	Approved Standard	
TIR80001-2-5 2014	**AAMI IEC**	Application of risk management for IT-networks incorporating medical devices - Part 2-5: Application guidance - Guidance on distributed alarm systems	Approved Standard	
TR 80001-2-6 2014	**AAMI ISO**	Application of risk management for IT-networks incorporating medical devices -- Part 2-6: Application guidance -- Guidance for responsibility agreements Provides guidance on implementing RESPONSIBILITY AGREEMENTS, which are described in IEC 80001-1 as used to establish the roles and responsibilities among the stakeholders	Approved Standard	

Software Assurance: **Standards that describe requirements and guidance for significantly decreasing the likelihood of software having vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web, software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		engaged in the incorporation of a MEDICAL DEVICE into an IT-NETWORK in order to support compliance to IEC 80001-1.		
AUTO13 February 18, 2003	**CLSI**	Identifies important factors that designers and laboratory managers should consider when developing new software-driven systems and selecting software user interfaces. Also included are simple rules to help prepare validation protocols for assessing the functionality and dependability of software.	Approved Standard	
62304: 2006	**IEC**	medical device software – software life cycle process, including Software Risk Management Process This standard defines the life cycle requirements for medical device software. The set of processes, activities, and tasks described in this standard establishes a common framework for medical device software life cycle processes *Section 1.1*	Approved Standard	
82304-1:2016	**IEC**	the safety and security of health software products designed to operate on general computing platforms and intended to be placed on the market without dedicated hardware Uses the life cycle of IEC 62304 while giving eases in verification activities. This standard is for health software that runs on general purpose hardware that may be acquired and controlled by the customer	Approved Standard	
TR 80002-1:2009	**IEC**	Guidance on the application of ISO 14971 to medical device software Aimed at risk management practitioners who need to perform risk management when software is included in the medical device/system,	Approved Standard	

Software Assurance: **Standards that describe requirements and guidance for significantly decreasing the likelihood of software having vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web, software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		and at software engineers who need to understand how to fulfil the requirements for risk management addressed in ISO 14971.		
27036-1:2014	**ISO/ IEC**	information security for supplier relationships (Part 1: Overview and concepts)	Approved Standard	
27036-2:2014	**ISO/ IEC**	information security for supplier relationships (Part 2: Common requirements);	Approved Standard	
27036-3: 2013	**ISO/ IEC**	information security for supplier relationships (Part 3: Guidelines for ICT supply chain security)	Approved Standard	
19770-2:2015	**ISO/IEC**	software identification (SWID) tagging	Approved Standard	
20243:2015	**ISO/IEC**	identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains	Approved Standard Conformity Assessment	
27035-1:2016	**ISO/IEC**	guidance on information security incident management for large and medium-sized organizations	Approved Standard	
29147:2014	**ISO/IEC**	Information technology – Security techniques – Vulnerability disclosure.	Approved Standard	
30111:2013	**ISO/IEC**	guidelines for how to process and resolve potential vulnerability information in a product or online service	Approved Standard	
90003:2014	**ISO/IEC**	Provides guidance for organizations in the application of ISO 9001:2008 to the acquisition, supply, development, operation and maintenance of computer software and related support services.	Approved Standard	
Dependability Assurance	**OMG**	Provides a new system assurance methodology for the dependability argumentation for consumer devices, which is achieved by integrating	Approved Standard	

Software Assurance: **Standards that describe requirements and guidance for significantly decreasing the likelihood of software having vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web, software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
Framework for Safety-Sensitive Consumer Devices Specification Version 1.0 February 2016		conventional system assurance approaches such as risk analysis and assessments with a new way of approaching unique characteristics of consumer devices. The scope of this specification supports the objectives of the integration, and includes the dependability case for argumentation, as well as the dependability development process to be newly defined. The focus is to include the dependability argumentation particularly for consumer devices. In the future, it may be desirable to introduce additional argumentation methodology for other systems such as avionics or railways. However, they are outside of the scope for the current effort as the authors are not experts in other systems rather than consumer devices.		
AS5553B - 2016	**SAE International**	counterfeit electrical, electronic, and electromechanical (EEE) parts; avoidance, detection, mitigation, and disposition	Approved Standard	
AS6462A - 2014	**SAE International**	verification criteria for fraudulent/counterfeit electronic parts; avoidance, detection, mitigation, and disposition	Approved Standard	
UL 2900-1 2017-07-05	**UL**	Product Management: The product shall be designed and implemented such that it is possible to perform an update of the product's software, and to roll back an update *Page 11, Section 11*	Guidance Available	UL 2900 outlines offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses,

Software Assurance: **Standards that describe requirements and guidance for significantly decreasing the likelihood of software having vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This includes custom software, commercial off-the-shelf software, firmware, operating systems, utilities, databases, applications and applets for the Web, software/platform/infrastructure as a service (SaaS, PaaS, IaaS), mobile and consumer devices, etc.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
				minimize exploitation, address known malware, review security controls and increase security awareness.
UL 2900-2-1	**UL**	Security evaluation standard applies to the testing of network connected components of healthcare systems. It applies to, but is not limited to, the following key components: a) Medical devices; b) Accessories to medical devices; c) Medical device data systems; d) In vitro diagnostic devices; e) Health information technology; and f) Wellness devices.		

2189

2190

2191

Supply Chain Risk Management (SCRM): Standards that provide the confidence that organizations will produce and deliver information technology products or services that perform as required and mitigate supply chain-related risks, such as the insertion of counterfeits and malicious software, unauthorized production, tampering, theft, and poor quality products and services. IT SCRM standardization requirements include methodologies and processes that enable an organization's increased visibility into, and understanding of, how technology that they acquire and manage is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. IT SCRM standardization lies at the intersection of cybersecurity and supply chain management and provides a mix of mitigation strategies from both disciplines for a targeted approach to managing IT supply chain risks.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
TIR57:2016	**AAMI**	Association for the Advancement of Medical Instrumentation (AAMI) This TIR provides guidance for addressing information security within the risk management framework defined by ANSI/AAMI/ISO 14971. This guidance is intended to assist manufacturers and other users of the standard in the following: • Identifying threats, vulnerabilities, and assets associated with medical devices • Estimating and evaluating associated security risks • Controlling security risks • Monitoring effectiveness of the risk controls	Approved Standard	
28000:2007	**ISO**	Specification for security management systems for the supply chain Specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that affect supply chain security.	Approved Standard	

Supply Chain Risk Management (SCRM): Standards that provide the confidence that organizations will produce and deliver information technology products or services that perform as required and mitigate supply chain-related risks, such as the insertion of counterfeits and malicious software, unauthorized production, tampering, theft, and poor quality products and services. IT SCRM standardization requirements include methodologies and processes that enable an organization's increased visibility into, and understanding of, how technology that they acquire and manage is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. IT SCRM standardization lies at the intersection of cybersecurity and supply chain management and provides a mix of mitigation strategies from both disciplines for a targeted approach to managing IT supply chain risks.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.		
20243:2015	**ISO/IEC**	Information Technology -- Open Trusted Technology Provider Standard (O-TTPS) Identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains	Approved Standard Conformity Assessment	
27036-1:2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts Provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. ISO/IEC 27036-1:2014 addresses perspectives of both acquirers and suppliers	Approved Standard	
27036-2:2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements	Approved Standard	

Supply Chain Risk Management (SCRM): **Standards that provide the confidence that organizations will produce and deliver information technology products or services that perform as required and mitigate supply chain-related risks, such as the insertion of counterfeits and malicious software, unauthorized production, tampering, theft, and poor quality products and services. IT SCRM standardization requirements include methodologies and processes that enable an organization's increased visibility into, and understanding of, how technology that they acquire and manage is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. IT SCRM standardization lies at the intersection of cybersecurity and supply chain management and provides a mix of mitigation strategies from both disciplines for a targeted approach to managing IT supply chain risks.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.		
27036-3:2013	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security Provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance.	Approved Standard	
27036-4:2016	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services Provides cloud service customers and cloud service providers with guidance.	Approved Standard	
UL 2900-1 Feb 2016	**UL**	Prior to its initial operation in production, the product shall require changes of any system defaults that play a role in product security, such as passwords and keys. The product shall have an indicator when still operating with any system default of passwords, keys,	Guidance Available	UL 2900 outlines offer testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation,

Supply Chain Risk Management (SCRM): Standards that provide the confidence that organizations will produce and deliver information technology products or services that perform as required and mitigate supply chain-related risks, such as the insertion of counterfeits and malicious software, unauthorized production, tampering, theft, and poor quality products and services. IT SCRM standardization requirements include methodologies and processes that enable an organization's increased visibility into, and understanding of, how technology that they acquire and manage is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. IT SCRM standardization lies at the intersection of cybersecurity and supply chain management and provides a mix of mitigation strategies from both disciplines for a targeted approach to managing IT supply chain risks.				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		certifications, etc., that would be considered sensitive security parameters. *Page 11, Section 11*		address known malware, review security controls and increase security awareness.

2192

2193

2194

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
Common Criteria Link April 2017	**Common Criteria**	Class FDP: User Data Protection: User data protection is split into four groups of families that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data. User Data Protection security function policies: Access control policy and Information flow control policy Forms of user data protection: Access control functions, Informational flow control functions, Internal TOE transfer, Residual information protection, Rollback and Stored data integrity. Off-line storage, import and export: Data authentication, Export from the TOE, Import from outside of the TOE Inter-TSF communication: Inter-TSF user data confidentiality transfer protection and Inter-TSF user data integrity transfer protection. *Page 54, Section 11* Definitions:	Guidance Available	**What is Common Criteria?** Provides a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation.

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		TOE: a set of software, firmware and/or hardware possibly accompanied by user and administrator guidance documentation. **TSF:** consists of all hardware, software and firmware of a TOE that is either directly or indirectly relied upon for security enforcements.		
HITRUST CSF v9 10 September 2017	**HITRUST Alliance**	security framework in the U.S. healthcare industry	Approved Standard Under Revision Guidance Available	
15288:2015	**IEEE ISO/IEC**	Defines a set of processes and associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure.	Approved Standard	There are hooks to cybersecurity in the processes.
P2413	**IEEE**	an Architectural Framework for the IoT	Under Development	
P360	**IEEE**	Provides an overview and architecture for a series of standards that define technical requirements and testing methods for wearable devices and their functions. Gives overview, terminology and categorization for Wearable Consumer Electronic Devices (or Wearables in short). It further outlines an architecture for a series of	Under Development	

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		standard specifications that define technical requirements and testing methods for different aspects of Wearables, from basic security and suitableness of wear, to various functional areas like health, fitness and infotainment etc.		
RFC 7641	**IETF**	Observing resources can dramatically increase the negative effects of amplification attacks. That is, not only can notifications messages be much larger than the request message, but the nature of the protocol can cause a significant number of notifications to be generated. Without client authentication, a server therefore MUST strictly limit the number of notifications that it sends between receiving acknowledgements that confirm the actual interest of the client in the data; i.e., any notifications sent in non-confirmable messages MUST be interspersed with confirmable messages. Note that an attacker may still spoof the acknowledgements if the confirmable messages are sufficiently predictable. *Page 21, Section 7*	Proposed Standard	

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
State of the Art and Challenges for the Internet of Things	**IETF**	Reviews security building blocks available for securing the different layers of the Internet protocol suite; documents IoT security threats and the challenges to protect against these threats; and discuss the next steps needed to ensure roll out of secure IoT services	Under Development	
62443	**ISA/IEC**	Industrial Automation and Control Systems (IACS) standards and technical reports includes security management requirements	Status for Each Part	See: The 62443 series of standards Industrial Automation and Control Systems Security
13485:2016	**ISO**	requirements for a quality management system where an organization needs to demonstrate its ability to provide medical devices and related services that consistently meet customer and applicable regulatory requirements	Approved Standard	
12207:2008	**ISO/IEC**	Systems and software engineering – Software life cycle processes Contains processes, activities, and tasks that are to be applied during the acquisition of a software product or service and during the supply, development, operation, maintenance and disposal of software products. Software includes the software portion of firmware.	Approved Standard Under Revision	There are hooks to cybersecurity in the processes and the current FDIS has a SwA Process View.

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
15026-1:2013	**ISO/IEC**	defines assurance-related terms and establishes an organized set of concepts and their relationships, thereby establishing a basis for shared understanding of the concepts and principles central to all parts of ISO/IEC 15026 across its user communities.	Approved Standard	
15026-2:2011	**ISO/IEC**	systems and software engineering – systems and software assurance (Part 2: Assurance Case)	Approved Standard	
15026-4:2012	**ISO/IEC**	systems and software assurance (Part 4: Assurance in the life cycle)	Approved Standard	
20243:2015	**ISO/IEC**	identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains	Approved Standard Conformity Assessment	
20243:2015	**ISO/IEC**	Information Technology -- Open Trusted Technology Provider Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products identifies secure engineering best practices, including secure management of the IT products, components, and their supply chains	Approved Standard Conformity Assessment	
27036-1:2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts	Approved Standard	

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. ISO/IEC 27036-1:2014 addresses perspectives of both acquirers and suppliers		
27036-1:2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts Provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. ISO/IEC 27036-1:2014 addresses perspectives of both acquirers and suppliers	Approved Standard	
27036-2:2014	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.	Approved Standard	
27036-2:2014	**ISO/IEC**	Information technology – Security techniques – Information security	Approved	

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		for supplier relationships – Part 2: Requirements Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships.	Standard	
27036-3:2013	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security Provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance.	Approved Standard	
27036-3:2013	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security Provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance.	Approved Standard	
27036-4:2016	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud	Approved Standard	

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		services Provides cloud service customers and cloud service providers with guidance.		
27036-4:2016	**ISO/IEC**	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services Provides cloud service customers and cloud service providers with guidance.	Approved Standard	
oneM2M Specifications	**M2M**	oneM2M is a worldwide standards initiative that covers requirements, architecture, API specifications, security solutions, and interoperability for Machine-to-Machine and IoT technologies. oneM2M aims to define a comprehensive IoT service layer solution to enable scalable and economic IoT solutions. The oneM2M consolidates its IoT service layer platform into a three layer model. The oneM2M horizontal platform architecture has a middleware layer where capabilities such as security are common across all verticals and is designed to support resource sharing and interoperability. oneM2M was formed in 2012. The main partners include eight of the world's preeminent standards development organizations (ARIB-	Approved Standard	

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
		Japan, ATIS-N. America, CCSA-China, ETSI-Europe, TIA-America, TSDSI-India, TTA-Korea, TTC-Japan.		
AEP-67 2010-02-04	**NATO**	engineering for system assurance in NATO programs; guidance in how to build assurance into a system throughout its life cycle	Approved Standard	
Structured Assurance Case Metamodel	**OMG**	Documents Associated with Dependability Assurance Framework for Safety-Sensitive Consumer Devices (DAF), version 1.0 Defines a metamodel for representing structured assurance cases. An Assurance Case is a set of auditable claims, arguments, and evidence created to support the claim that a defined system/service will satisfy the particular requirements.	Approved Standard	
UL 2900-1 Feb 2016	**UL**	Prior to its initial operation in production, the product shall require changes of any system defaults that play a role in product security, such as passwords and keys. The product shall have an indicator when still operating with any system default of passwords, keys, certifications, etc., that would be considered sensitive security parameters. *Page 11, Section 11*	Guidance Available	UL 2900 outlines testable cybersecurity criteria for network-connectable products and systems to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and

System Security Engineering: **Standards that describe planning and design activities to meet security specifications or requirements for the purpose of reducing system susceptibility to threats, increasing system resilience, and enforcing organizational security policy. A comprehensive system security engineering effort: includes a combination of technical and nontechnical activities; ensures all relevant stakeholders are included in security requirements definition activities; ensures that security requirements are planned, designed, and implemented into a system during all phases of its lifecycle; assesses and understands susceptibility to threats in the projected or actual environment of operation; identifies and assesses vulnerabilities in the system and its environment of operation; identifies, specifies, designs, and develops protective measures to address system vulnerabilities; evaluates/assesses protective measures to ascertain their suitability, effectiveness and degree to which they can be expected to reduce mission/business risk; provides assurance evidence to substantiate the trustworthiness of protective measures; identifies quantifies, and evaluates the costs and benefits of protective measures to inform engineering trade-off and risk response decisions; and leverages multiple security focus areas to ensure that protective measures are appropriate, effective in combination, and interact properly with other system capabilities.**				
Documents	**SDO**	**Description**	**Maturity Level (Table 6)**	**Notes**
				increase security awareness.
UL 2900-2-1	**UL**	This security evaluation standard applies to the testing of network connected components of healthcare systems. It applies to, but is not limited to, the following key components: a) Medical devices; b) Accessories to medical devices; c) Medical device data systems; d) In vitro diagnostic devices; e) Health information technology; and f) Wellness devices.		

2195

Annex E—NIST Federal Information Processing Standards (FIPS) and NIST Special Publication 800 Series Relevant to IoT

The applicability sections of each FIPS publication should be reviewed to determine if the publication is mandatory for federal agency use. FIPS publications do not apply to national security systems (as defined in Title III, Information Security, of FISMA).

Federal government statutes (e.g., FISMA 2014), regulations, and policies (e.g., Office of Management and Budget [OMB] Circular A-130) may specify whether federal agencies are required, or encouraged, to comply with NIST's SP 800-series publications. NIST's SP 800 series publications shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems.

Federal Information Processing Standards Publication (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

Federal Information Processing Standards Publication (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems

Federal Information Process Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems

Federal Information Process Standards Publication (FIPS) 186-4, Digital Signature Standard (DSS)

Federal Information Process Standards Publication (FIPS) 180-4, Secure Hash Standard (SHS)

Federal Information Process Standards Publication (FIPS) 140-2, Security Requirements for Cryptographic Modules

NIST Special Publication 800-184, Guide for Cybersecurity Event Recovery

NIST Special Publication 800-183, Networks of 'Things'

NIST Special Publication 800-177, Trustworthy Email

NIST Special Publication 800-175A, Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies

NIST Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms

NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

NIST Special Publication 800-163, Vetting the Security of Mobile Applications

NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations

NIST Special Publication 800-160, Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

NIST Special Publication 800-153, Guidelines for Securing Wireless Local Networks (WLANs)

NIST Special Publication 800-152, A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)

NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing

NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations

NIST Special Publication 800-145, The NIST Definition of Cloud Computing

NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing

NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations

NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems

NIST Special Publication 800-125, Guide to Security for Full Virtualization Technologies

NIST Special Publication 800-124 Rev. 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise

NIST Special Publication 800-123, Guide to General Server Security

NIST Special Publication 800-121 Rev. 2, Guide to Bluetooth Security

NIST Special Publication 800-119, Guidelines for the Secure Deployment of IPv6

NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment

NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices

NIST Special Publication 800-101 Rev. 1, Guidelines on Mobile Device Forensics

NIST Special Publication 800-98, Guidelines for Securing Radio Frequency Identification (RFID) Systems

NIST Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to

IEEE 802.11i

NIST Special Publication 800-95, Guide to Secure Web Services

NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)

NIST Special Publication 800-92, Guide to Computer Security Log Management

NIST Special Publication 800-83 Rev.1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops

NIST Special Publication 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security

NIST Special Publication 800-81-2, Secure Domain Name System (DNS) Deployment Guide

NIST Special Publication 800-77, Guide to IPsec VPNs

NIST Special Publication 800-70 Rev. 3, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

NIST Special Publication 800-64 Rev. 2, Security Considerations in the System Development Life Cycle

NIST Special Publication 800-63A, Digital Identity Guideline: Enrollment and Identity Proofing

NIST Special Publication 800-63B, Digital Identity Guideline: Authentication and Lifecycle Management

NIST Special Publication 800-63C, Digital Identity Guideline: Federation and Assertions

NIST Special Publication 800-63-3, Digital Identity Guidelines

NIST Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide

NIST Special Publication 800-58, Security Considerations for Voice Over IP Systems

NIST Special Publication 800-57 Part 1 Rev. 4, Recommendation for Key Management, Part 1: General

NIST Special Publication 800-57 Part 2, Recommendation for Key Management, Part 2: Best Practices for Key Management Organization

NIST Special Publication 800-57 Part 3 Rev. 1, Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance

NIST Special Publication 800-54, Border Gateway Protocol Security

NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-52 Rev. 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

NIST Special Publication 800-48 Rev. 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks

NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems

NIST Special Publication 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST Special Publication 800-45 Version 2, Guidelines on Electronic Mail Security

NIST Special Publication 800-44 Version 2, Guidelines on Securing Public Web Servers

NIST Special Publication 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy

NIST Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies

NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

NIST Special Publication 800-37 Rev. 1, Guide for applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach

NIST Special Publication 800-36, Guide to Selecting Information Technology Security Products

NIST Special Publication 800-35, Guide to Information Technology Security Services

NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems

NIST Special Publication 800-33, Underlying Technical Models for Information Technology Security

NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure

NIST Special Publication 800-30 Rev. 1, Guide for Conducting Risk Assessments

NIST Special Publication 800-29, A Comparison of the Security Requirements for Cryptographic modules in FIPS 140-1 and FIPS 140-2

NIST Special Publication 800-28 Version 2, Guidelines on Active Content and Mobile Code

NIST Special Publication 800-27 Rev. A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A

NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems

NIST Special Publication 800-12, An Introduction to Information Security

Annex F—Acronyms

3GPP	3rd Generation Partnership Project
AAMI	Association for the Advancement of Medical Instrumentation
AES	Advanced Encryption Standard
CD	Committee Draft
CIP	Critical Infrastructure Protection
CLSI	Clinical and Laboratory Standards Institute
COSO	Committee of Sponsoring Organizations
CPS	Cyber Physical Systems
CSA	Canadian Standards Association
DASH7	Developers Alliance for Standards Harmonization
DDoS	Distributed Denial of Service
DIS	Draft International Standard
DOT	Department of Transportation
DSA	Digital Signature Algorithm
DSS	Data Security Standard
DTS	Diabetes Technology Social
ESDSA	Elliptic Curve Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FDA	U.S. Food and Drug Administration
FDIS	Final Draft International Standard
FIDO	Fast Identity Online
FIPS	Federal Information Processing Standard
GSMA	Groupe Speciale Mobile Association
EHR	Electronic Health Records
HL7	Health Level 7
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIT	Health Information Technology
HITRUST	Health Information Trust Alliance
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IDMEF	Intrusion Detection Message Exchange Format
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IICSWG	Interagency International Cybersecurity Standardization Working Group
IIC	Industrial Internet Consortium
IODEF	Incident Object Description Exchange Format
IoT	Internet of Things
IPv6	Internet Protocol version 6

ISA	International Society of Automation
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
ITS JPO	Intelligent Transportation System Joint Program Office
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication
LDAP	Lightweight Directory Access Protocol
LoRa Alliance	Long Range Alliance
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Message Authentication Code
MQTT	MQ Telemetry Transport
NATO	North Atlantic Treaty Organization
NERC	North American Electric Reliability Corporation
NHTSA	National Highway Traffic Safety Administration
NS/EP	National Security and Emergency Preparedness
NSC's Cyber IPC	National Security Council's Cyber Interagency Policy Committee
NSTAC	President's National Security Telecommunications Advisory Committee
OASIS	Organization for the Advancement of Structured Information Standards
OCF	Open Connectivity Foundation
OMA	Open Mobile Alliance
OMG	Object Management Group
OpenFog RA	OpenFog Reference Architecture
OTA	Open Travel Alliance
O-TTPS	Open Trusted Technology Provider Standard
PCI	Payment Card Industry
PHR	Personal Health Records
PID	Proportional Integral Derivative
PII	Personally Identifiable Information
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSS	Probabilistic Signature Scheme
RFC	Request for Comments
RID	Real-time Inter-network Defense
SACM	Security Automation and Continuous Monitoring
SAE	SAE International
SAML	Security Assertion Markup Language
SCMS	Security Credential Management System
SCRM	Supply Chain Risk Management

SDO	Standards Developing Organizations
STIX	OASIS Structured Threat Information Expression
SWID	Software Identification
TAXII	OASIS Trusted Automated Exchange of Indicator Information
TCG	Trusted Computing Group
TIA/EIA	Telecommunications Industry Association. Electronic Industries Alliance
TLS	Transport Layer Security
TR	Technical Report
TTP	Tactics, Techniques, and Procedures
UI	User Interface
UL	Underwriters Laboratories
WD	Working Draft
XSF	XMPP Standards Foundation

2322

2323 # Annex G—References

[1] NIST Interagency Report (NISTIR) 8074 Volume 1, *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2015, 22 pp. https://doi.org/10.6028/NIST.IR.8074v1.

[2] NIST Interagency Report (NISTIR) 8074 Volume 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, Maryland, Dec 2015, 72 pp. https://doi.org/10.6028/NIST.IR.8074v2

[3] Office of Management and Budget (OMB), *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, Circular A-119, Office of Management and Budget, Executive Office of the President. Washington, DC, January 2016, 28 pp. https://www.federalregister.gov/documents/2016/01/27/2016-01606/revision-of-omb-circular-no-a-119-federal-participation-in-the-development-and-use-of-voluntary

[4] The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things*, Washington, DC, November 2014, 24 pp. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A119/revised_circular_a-119_as_of_1_22.pdf

[5] Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 2016, 90 pp. https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

[6] NIST Interagency Report (NISTIR) 8074 Volume 1, *Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, Maryland, December 2015, 28 pp. https://doi.org/10.6028/NIST.IR.8074v1.

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

[8] OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, Office of Management and Budget, Executive Office of the President. Washington, DC, January 2016, 28 pp. https://www.federalregister.gov/documents/2016/01/27/2016-01606/revision-of-omb-circular-no-a-119-federal-participation-in-the-development-and-use-of-voluntary

[9] S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau, *NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems*, National Institute of Standards and Technology, Gaithersburg Maryland, January 2017, 41 pp. https://doi.org/10.6028/NIST.IR.8062

[10] Kevin Gay, *Security Credential Management System – Operations and Management*, U.S. Department of Transportation, 15 pp. https://www.its.dot.gov/pilots/pdf/ITSA2016_security_Gay.pdf

[11] Connected Vehicle Basics, *How Does Connected Vehicle Technology Work?*, U.S. Department of Transportation, Washington DC, 1 pp. https://www.its.dot.gov/cv_basics/cv_basics_how.htm

[12] Guidance Summary for Connected Vehicle Deployments, *Security Operational Concept, Final Report*, U.S. Department of Transportation, Washington DC, July 2016, 20 pp. https://rosap.ntl.bts.gov/view/dot/3599/dot_3599_DS1.pdf

[13] K. Gay, *Security Credential Management System – Operations and Management*, U.S. Department of Transportation, 15 pp. https://www.its.dot.gov/pilots/pdf/ITSA2016_security_Gay.pdf

[14] Security Credential Management System Proof-of-Concept Implementation, *EE Requirements and Specifications Supporting SCMS Software Release 1.1*, U.S. Department of Transportation, May 2016, 553 pp. https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf

[15] D. Fred, *A Brief History of the Internet of Things*, FireceMobileIT, July 2014. http://www.fiercemobileit.com/story/brief-history-internet-things/2014-07-23

[16] S. Gupta, *Implantable Medical Devices – Cyber Risks and Mitigation Approaches*, NIST Cyber Physical Systems Workshop April 23-24, 2012, https://csrc.nist.gov/presentations/2012/implantable-medical-devices-cyber-risks-and-miti

[17] J. Bresnick, *Internet of Things, Precision Medicine, NLP Drive Market*

Growth, Precision Medicine News, October 2015, 1 pp. https://healthitanalytics.com/news/internet-of-things-precision-medicine-nlp-drive-market-growth

[18] *What is Precision Medicine?*, National Institute of Health, U.S. National Library of Medicine, April 2015, 1 pp. https://ghr.nlm.nih.gov/primer/precisionmedicine/definition

[19] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski, J. McCarthy, *NISTIR 8183: Cybersecurity Framework Manufacturing Profile*, National Institute of Standards and Technology, Gaithersburg Maryland, January 2017, 50 pp. https://doi.org/10.6028/NIST.IR.8183

[20] K. McKay, L. Bassham, M. Turan, N. Mouha, *NISTIR 8114: Report on Lightweight Cryptography*, National Institute of Standards and Technology, Gaithersburg, Maryland, March 2017, 21 pp. https://doi.org/10.6028/NIST.IR.8114

[21] Health Information Technology, https://www.healthit.gov/

[22] The Industrial Internet of Things, *Volume G8: Vocabulary* Industrial Internet Consortium, 2017, 32 pp. http://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.0.pdf

[23] NIST Interagency Report (NISTIR) 8074 Volume 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, National Institute of Standards and Technology, Gaithersburg, Maryland, Dec 2015, 72 pp. https://doi.org/10.6028/NIST.IR.8074v2

[24] *IoT Security Threat Map*, Beecham Research, London, Maryland, March 2015, 1 pp. http://www.beechamresearch.com/download.aspx?id=43

[25] DoD CIO, *Policy Recommendations for the Internet of Things*, U.S. Department of Defense, December 2016, 6 pp. https://www.hsdl.org/?view&did=799676

[26] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, NIST Special Publication 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security*, Natonal Institute of Standards and Technology, Gaithersburg, Maryland, May 2015, 41 pp. https://doi.org/10.6028/NIST.SP.800-82r2

[27] NIST Special Publication 800-30 Revision 1, Joint Task Force Transformation Initiative Interagency Working Group, *Guide for Conducting*

Risk Assessments, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95 pp. https://doi.org/10.6028/NIST.SP.800-30r1

[28] Committee on National Security Systems Glossary Working Group, *Committee On National Security Systems (CNSS) Glossary,* April 2010, 160 pp. https://cryptosmith.files.wordpress.com/2015/08/glossary-2015-cnss.pdf

[29] NIST Special Publication 800-30 Revision 1, Joint Task Force Transformation Initiative Interagency Working Group, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 95 pp. https://doi.org/10.6028/NIST.SP.800-30r1

[30] D. Klinedinst and C. King, *On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle,* Software Engineering Institute, Carnegie Mellon University, March 2016, 20 pp. https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf

[31] *Connected Vehicle Pilot Deployment Program Phase I Security Management Operational Concept*, Federal Highway Administration, Mary 2016. https://ntl.bts.gov/lib/59000/59200/59264/FHWA-JPO-16-312.pdf

[32] Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Healthcare Industry*, Public Health Emergency, June 2017, 88 pp. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

[33] The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on the Internet of Things*, Washington, DC, November 2014, 24 pp. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A119/revised_circular_a-119_as_of_1_22.pdf

[34] ISO/IEC CD 20924, *Information technology – Internet of Things – Definition and Vocabulary*. https://www.iso.org/standard/69470.html

[35] IEEE P2413, *Standard for an Architectural Framework for the Internet of Things (IoT).* https://standards.ieee.org/develop/project/2413.html

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

[37] *Fostering the Advancement of the Internet of Things*, The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, National Telecommunications and Information Administration, Washington DC, January 2017, 65 pp. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

[38] J. Voss, NIST Special Publication 800-183 Revision 1, *Network of 'Things'*, National Institute of Standards and Technology, Gaithersburg, Maryland, July 2016, 25 pp. https://doi.org/10.6028/NIST.SP.800-183

[39] *Overview of the Internet of Things*, International Telecommunication Union, Next Generation Networks – Frameworks and functional architecture models, 2013, 15 pp. http://handle.itu.int/11.1002/1000/11559-en?locatt=format:pdf&auth

2324