CSA Guide to the IoT Security Controls Framework Version 2

cloud security alliance®

The permanent and official location for Cloud Security Alliance Internet of Things research is https://cloudsecurityalliance.org/working-groups/internet-of-things/

Acknowledgments

Initiative Leads:

Aaron Guzman
Michael Roza
Brian Russell

Contributors:

Renu Bedi
Ramon Codina
Umesh Jaiswal
Raj Sachdev
Ashish Vashishtha

CSA:

Hillary Baron
AnnMarie Ulskey (Graphic Design)

Table of Contents

Introduction 5
Goal 5
Target Audience 5
Versioning 6
How to Use the IoT Security Controls Framework 7
- Security Control Objectives (Columns A, B, C, D, E, F) 8
- IoT System Risk Impact Levels (Columns G, H, I) 10
- Supplemental Control Guidance (Columns J, K) 11
- Implementation Guidance (Columns L, M, N) 11
- Device, Network, Gateway and Cloud Assignment (O, P, Q, R) 13

Additional Resources 15

Introduction

The Internet of Things (IoT) market continues to expand with newly introduced advances in connectivity and autonomy across industry sectors. A reliance on IoT-generated data and features is rapidly increasing, requiring enterprise organizations that adopt these new technologies to plan for accessible, secure, and resilient deployments. Given the rapid evolution of connected technologies and the constant flow of new threats, these aspirations are challenging. Creating a safe IoT environment requires security engineering that addresses unique risks and employs appropriate implementation mitigation measures. The *Cloud Security Alliance (CSA) IoT Security Controls Framework* provides a starting point for organizations that wish to better understand and implement security controls within their IoT architecture. This accompanying guide explains how enterprise organizations can use the framework to evaluate and implement IoT systems securely.

The *IoT Security Controls Framework* is relevant for enterprise IoT systems that deploy a diverse set of connected devices and associated cloud services, networking technologies and application software. The framework has utility across many IoT domains, ranging from systems processing only "low-value" data with limited impact potential to highly sensitive systems that support critical services. System owners classify components based on the value of data being stored and processed and the potential impact of various physical security threats.

The framework helps users identify appropriate security controls and allocates them to specific architectural components, including:

- Devices
- Networks
- Gateways
- Cloud Services

Controls allocated to each layer in the architecture represent best-case security postures. In some cases, architectural components cannot implement certain recommended controls in this framework. In these cases, the system security architect should identify those shortcomings and develop plans to mitigate residual risk using alternative measures.

Goal

The *IoT Security Controls Framework* provides a tool to evaluate implementations› security as they progress through the development lifecycle to ensure they meet industry-specified best practices.

Target Audience

The *IoT Security Controls Framework* is a resource for system architects, developers, and security engineers tasked with designing secure IoT ecosystems. IoT system evaluators such as auditors and penetration testers may leverage the framework to validate controls and their deployed implementations.

Versioning

Version 1 of the *IoT Security Controls Framework* introduces 155 base-level security controls required to mitigate many risks IoT systems face operating in various threat environments.

Version 2 of the *IoT Security Controls Framework* evolves the Version 1 framework to better categorize controls into a new set of domains and minimize control allocation to components within an IoT architecture. The significant changes include developing a new domain structure and infrastructure, explained in the pages below.

- Updated controls: All controls have been reviewed and updated for technical clarity.
- New domain structure: Control domains have been reviewed and updated to better categorize each control.
- New legal domain: Introduces relevant legal controls.
- New security testing domain: Introduces security testing of architectural allocations.
- Simplified infrastructure allocations: Device types have been consolidated to a single category to simplify the distribution of controls to architectural components.

Future Changes - Version 3 will include the following noteworthy improvements:

- IoT Framework Shared Responsibility Matrix
- Safety specific controls
- Indicators of compromise
- IoT Framework to European Union Agency for Network and Information Security (ENISA) Guidelines for Securing the Internet of Things
- IoT Framework to National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and 800-53 Mappings

How to Use the IoT Security Controls Framework

Figure 1 below details the flow that users of the CSA *IoT Security Controls Framework* should follow as they assess and then implement security controls for a unique environment. The letters in this illustration correspond to columns in the framework (spreadsheet).

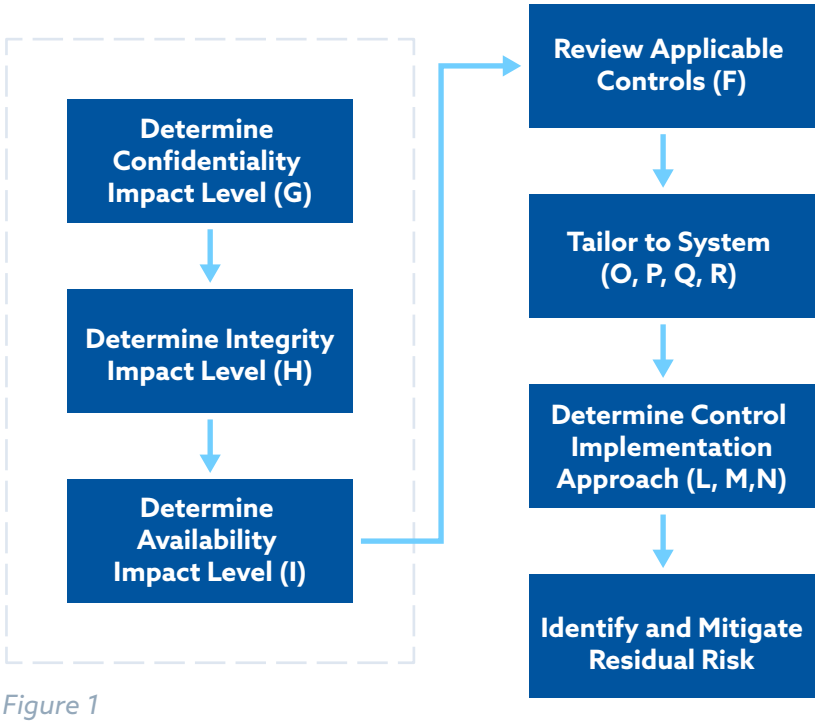


Figure 1

Evaluation begins through an understanding of the system architectures' security and data impact levels. These are characterized based on standard processes, such as *Federal Information Processing Standard Publication (FIPS)* 199. Once impact-level determinations are made for system confidentiality, integrity, and availability, the framework can be filtered to show only the controls applicable to those impact levels.

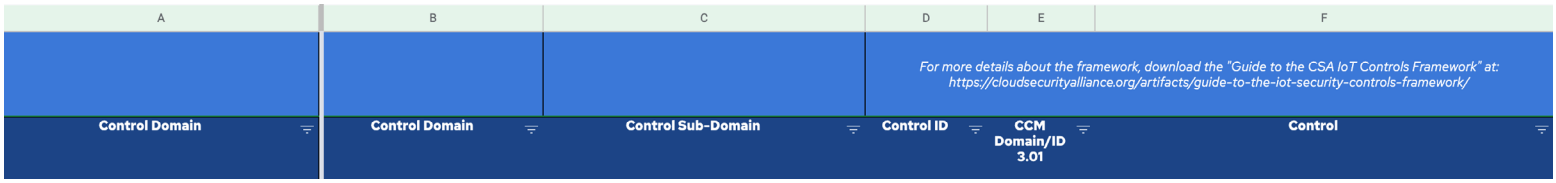
Review each of the resulting controls in Column F and review any additional guidance in Column J. Columns O, P, Q, and R include a tool for allocating controls to different architectural components.

These columns allow users to filter controls based on whether they apply to the device, the network that hosts the device, a gateway, or cloud services.

Users can also understand how to implement each control using columns L, M, and N. These columns offer control-type recommendations, whether controls should be manual, automated, or a combination of both, and how often controls should be exercised.

Following this initial process, the framework provides insight into an idealized version of a secure baseline tailored to an IoT system architecture. Some components within an IoT architecture may not be capable of meeting a subset of the controls. In these cases, the security architect must understand the residual risk and identify compensating controls to mitigate that risk.

Security Control Objectives (Columns A, B, C, D, E, F)



Control Domain (Column A): Organized by logical groupings of the individual security control measures (**see table below**) and detailed in column F (Control), the name of each corresponding control specification is italicized below the category of "Control Domain."

Control Domain (Column B): Domains are categorized for filtering purposes.

Control Sub-Domain (Column C): Sub-domains provide granularity for filtering purposes.

#	Control Domain Name	Abbr.	Sub-Domains
1	Asset Management	ASM	Naming Convention, Inventory Assets, Monitor Assets
2	Configuration Management	CCM	Configuration Files, Firmware Updates, Configuration Control, End-of-Life Planning
3	Secure Communications	COM	Trusted Communications, Message Queuing Telemetry Transport (MQTT) Security, Encrypted Communications
4	Secure Data	DAT	Data Classification and Taxonomy, Data Cleansing, Encrypted Data at Rest
5	Governance	GVN	Governance Framework, Regulatory and Legal Requirements, Compliance Management, Privacy, Business Continuity, Safety
6	Identity and Access Management	IAM	Password Mgmt, Authentication, Authorization, Access Control, Certificate Mgmt, Key Mgmt, Trust Anchor Management, Bootstrap, Account Audit
7	Incident Management	IMT	Incident Response
8	IoT Device Security	IOT	Certified Devices, Secure Platform, Secure Configuration
9	Legal	LGL	Legal Assessment, Legal Implementation Plan, Document Measures for Legal Purposes, Terms and Conditions and Privacy Policy, Contracts, Disclaimers, Disclosures, Notifications Waivers, Liability, Data Transfer
10	Monitoring and Logging	MON	Threat Intelligence, Threat Hunting, Automated Malware Log Mgmt., Analytics, Event Definition, Radio Frequency (RF) Monitoring

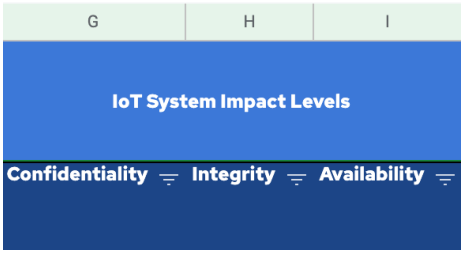
11	Operational Availability	OPA	Maintenance, Fail-Over, Distributed Denial of Service (DDoS) Protection, Service-Level Agreements
12	Physical Security	PHY	Physical Access Controls
13	Policy	POL	Policy Definition, Acquisition Security Policy, Secure Disposition
14	Risk Management	RSM	Risk Management Strategy, Risk Management Execution, Limit Liability
15	Secure Applications	SAP	Mobile Applications, Cloud Services, Autonomous Systems
16	Secure System Development Lifecycle	SDV	Process Security, Supply Chain/ Acquisition, Secure Development Practices, Security Testing
17	Secure Networks	SNT	Secure Discovery, Network Hardening, Zero Trust, Network Visualization
18	Secure Wireless	SWS	RF Architecture, Bluetooth Security, Near Field Communication (NFC) Security, Zigbee Security
19	Training	TRN	Administrator Training, User Training
20	Vulnerability Management	VLN	Responsible Disclosure Program, Vulnerability Scanning, Updates and Patches
21	Security Testing	SET	Assessment Scoping and Planning, Penetration Testing, Red Teaming, Third-Party Assessments, Bug Bounty, IoT Applications and Services (Internally Developed)

Control ID (Column D): The control identification (ID) is the official identifier of a specific security control. The ID (e.g., "RSM-01") allows controls to be referenced elsewhere by their position in the framework.

CCM ID (Column E): Security controls in the framework are associated, or mapped, in this column to the identifiers from the CSA Cloud Controls Matrix (CCM). When the IoT security control is derived or linked to a CCM control, one or more entries are identified. The associated controls involve partial to full coverage of the control specifications in each framework.

Control Specification (Column F): Specifications are written as mitigations or countermeasures addressing specific risk areas for an IoT system. For usability, each control is separated into a simplified action to address unique IoT environments.

IoT System Risk Impact Levels (Columns G, H, I)



Columns G through I: This information enables the initial tailoring of security controls to a user's unique environment. Before beginning the process of tailoring individual security controls, users should review two U.S. Department of Commerce publications: "Standards for Security Categorization of Federal Information and Information Systems" *(FIPS 199)*[1] and "Minimum Security Requirements for Federal Information and Information Systems" *(FIPS 200)*[2]. The FIPS 199 and 200 publications categorize risk impact levels as "low," "moderate," or "high" in three areas: confidentiality, integrity, and availability.

Confidentiality (Column G): Some data in an IoT system, such as personal privacy and proprietary information, necessitates restricted access via various security controls to remain appropriately confidential. To evaluate components of an IoT system's confidentiality risk, it is necessary to estimate the potential impact (low, moderate, or high) if system data were made public or compromised by an attacker.

Integrity (Column H): To protect data integrity, an enterprise must guard against improper data modification or destruction and ensure information authenticity. To evaluate an IoT system's integrity risks, assess the impact (low, moderate, or high) if system data were destroyed or inappropriately modified.

Availability (Column I): To assess the degree to which system information must remain accessible in a timely and reliable manner, evaluate the system›s potential risks if it became inoperable for any duration.

To assess whether specific risks regarding confidentiality, integrity, and availability of system data is low, moderate, or high, consult "Table 1" on page six of "FIPS 199: 'POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES.'

After determining these risk impact levels, the IoT Security Controls Framework can identify all needed security controls for a specific environment.

Note that when an impact level is high, all available security controls should be applied—including those for low, moderate and high-risk levels. When an impact level is moderate, apply all controls for moderate and low-risk levels.

[1] FIPS 199: "Standards for Security Categorization of Federal Information and Information Systems," Federal Information Processing Standards Publication, Computer Security Division, U.S. Department of Commerce; February 2004. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

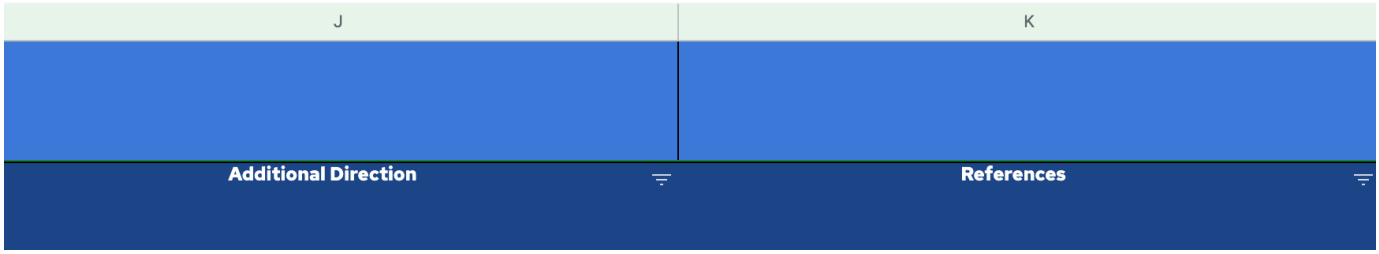
[2] FIPS 200: "Minimum Security Requirements for Federal Information and Information Systems," Federal Information Processing Standards Publication, Computer Security Division, U.S. Department of Commerce; March 2006. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Below are examples of three impact ratings and the necessary corresponding controls.

Type of Security Risk →	Risk Impact Level →	Necessary Security Controls
Confidentiality	High	High, Moderate and Low
Integrity	Moderate	Moderate and Low
Availability	Low	Low Only

Figure 2

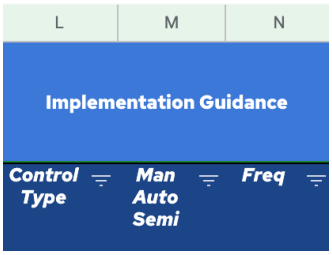
Supplemental Control Guidance (Columns J, K)



Additional Direction (Column J): When assessing or implementing any of the individual security protocols in the IoT Security Controls Framework, be sure to view this supplementary information detailing special requirements, explanations of terms, helpful operating tips, and more.

References (Column K): Consult this section for professional source information, such as government publications, regulatory information, and other references necessary to understand and implement a control specification fully.

Implementation Guidance (Columns L, M, N)



When implementing an enterprise's security plan, use the framework's "Implementation Guidance" section to determine control types for unique environments (Column J). This insight will include how organizations can implement the controls (Column K) and the frequency with which each security control measure should be enacted (Column L).

Types of Security Controls (Column L)

The *IoT Framework's* security controls are classified into three types, based on when, where, and how the measures work to increase security.

Preventive controls: Stop something from happening (i.e., limiting physical access to a room through a locked door or require higher-level biometric identification protocols).

Detective controls: Identify and then characterize incidents. Examples include researching an inventory discrepancy after a physical count, recording video, and using motion sensors to detect trespassing.

Corrective controls: Mitigate damage caused by security incidents. For example, utilize a fire extinguisher to limit fire damage or ensure a duplicate data center's availability if a primary data center crashes.

Control Implementation Guidance (Column M)

Security controls are implemented in three ways, depending on the level of automation.

Manual controls: A human performs manual controls. For example, in a risk management process review, someone evaluates the process to confirm it has been executed in accordance with policy.

Automatic controls: A system performs automatic controls without human intervention. For example, in a user access check, a user logs in with a username and password. The system then verifies the combination before granting access.

Semi-automatic controls: Semi-automatic controls combine automated and manual efforts. For example, in a physical inventory, items are counted, and the results are compared to a system-generated list. Differences are then reconciled through an investigation, which may involve paper and electronic records.

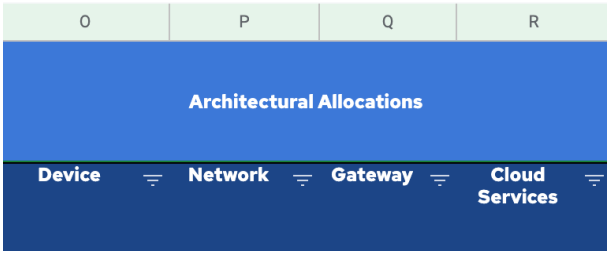
Control Frequency (Column N)

Some organizations require more frequent controls based on internal risk priorities or regulatory compliance requirements. The following frequencies are recommended for different situations (depending on individual enterprise needs).

- Annually
- Quarterly
- Monthly
- Weekly
- Daily
- Event: Control performed irregularly (e.g., a software update)
- Continuously: Control performed many times per day (e.g., user access)

Device, Network, Gateway and Cloud Services (O, P, Q, R)

The *IoT Framework* guides the application of architectural element controls in an IoT system. These architectural elements represent standard layers within an IoT architecture, as shown in the below figure.



Implementers should consult these document sections to determine if controls are applicable at each layer. Each column describes opportunities to create trust boundaries within IoT architecture. Discrete controls should be applied at each layer.

Device (Column O)

Controls applied directly at the device layer that focus on the data processed, stored, and/or generated by the device. A generic IoT device will incorporate sensors, actuators, and potentially a minimal user interface. The device may also be capable of collecting and storing events or security logs, using configuration files that must be integrity-protected.

Network (Column P)

At the network layer, components such as wireless access points (WAPs) support device WiFi connectivity. Other network components may include key management servers that support protocols such as ZigBee. Additionally, network security controls may consist of zero trust designs, virtual local area network (VLAN) segmentation, firewalling, and intrusion detection. Consider data encryption and integrity protection as data traverses an IoT network.

Gateway (Column Q)

The gateway represents a high potential IoT network entry point for threat actors. The gateway may have additional security controls applied that exceed what devices typically implement.

Cloud Services (Column R)

Most IoT devices require cloud environments to operate. Devices may send data directly to the cloud or managed through a cloud service. Data transmitted to the cloud must be protected during transit and persistently within cloud provider storage volumes. In some cases, anonymity protections must be applied within the cloud to ensure identities cannot be linked to IoT data.

The figure below provides a visual depiction of these architectural layers.

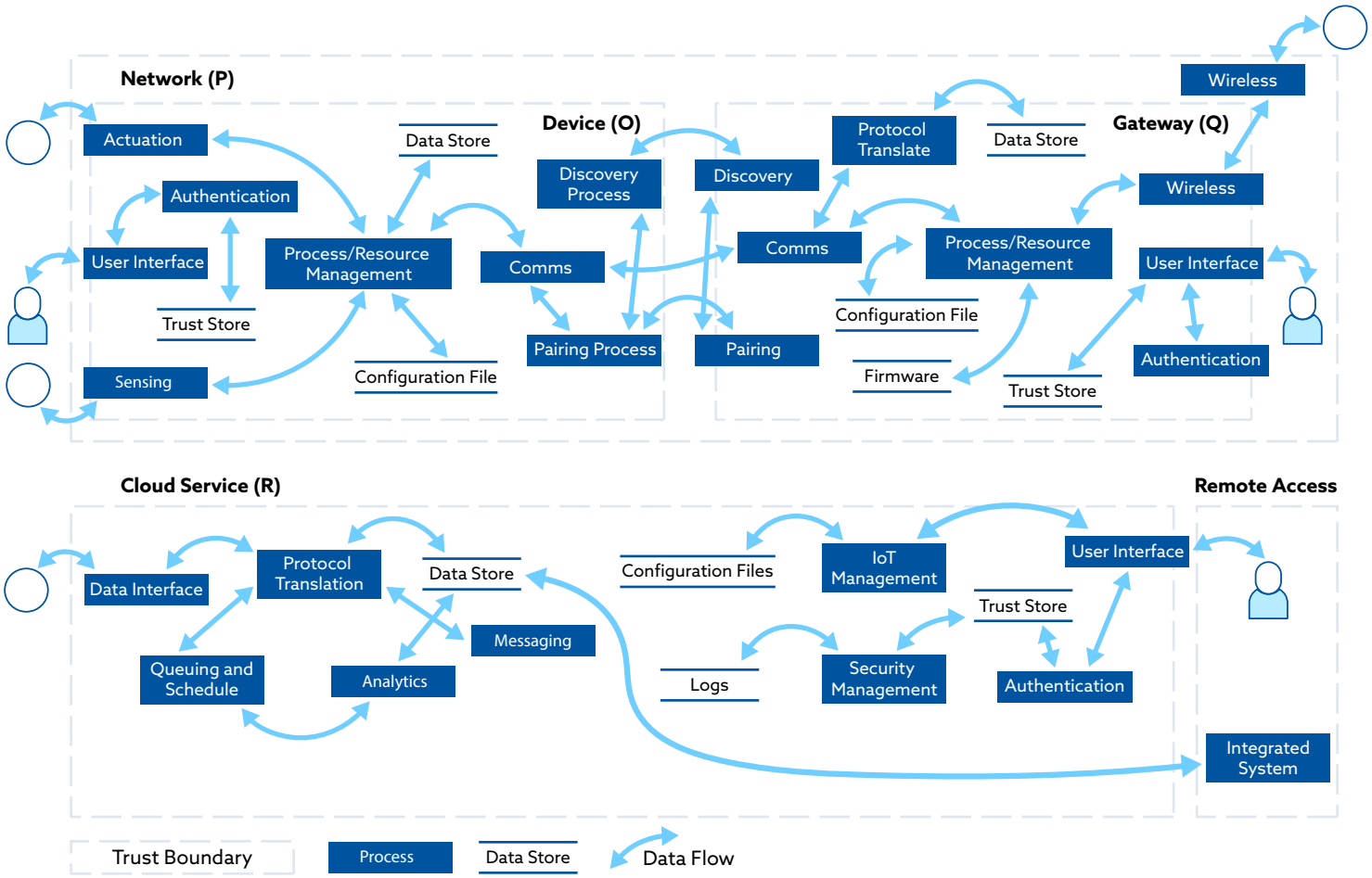


Figure 3

Additional Resources

Fagan, Michael. Megas, Katerina N. Scarfone, Karen. Smith, Matthew. "Foundational Cybersecurity Activities for IoT Device Manufacturers." https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf May 2020. NISTIR 8259, National Institute of Standards and Technology.

Fagan, Michael. Megas, Katerina N. Scarfone, Karen. Smith, Matthew. "IoT Device Cybersecurity Capability Core Baseline." https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf May 2020. NISTIR 8259A, National Institute of Standards and Technology.

Boeckl, Katie. Fagan, Michael. Fisher, William. Lefkovitz, Naomi. Megas, Katerina N. Nadeau, Ellen. Piccarreta, Ben. Gabel O'Rourke, Danna. Scarfone, Karen. "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks." https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf June 2019. NISTIR 8228, National Institute of Standards and Technology.

Iorga, Michaela. Feldman, Larry. Barton, Robert. Martin, Michael J. Goren, Nedim. Mahmoudi, Charif. "Fog Computing Conceptual Model: Recommendations of the National Institute of Standards and Technology." https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf March 2018. NIST SP 500-325, National Institute of Standards and Technology.

Interagency International Cybersecurity Standardization Working Group. "Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)." https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf November 2018. NISTIR 8200, National Institute of Standards and Technology.

Voas, Jeffrey. Kuhn, Richard. Laplante, Phillip. Applebaum, Sophia. "Internet of Things (IoT) Trust Concerns." https://csrc.nist.gov/publications/detail/nistir/8222/draft September 2018. NISTIR 8222, National Institute of Standards and Technology.

European Union Agency for Cybersecurity (ENISA). "Good Practices for Security of IoT: Secure Software Development Lifecycle." https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1 November 2019.

European Union Agency for Cybersecurity (ENISA). "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures." https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot November 2017.

ISO/IEC JTC 1/SC 41. "Internet of Things—Reference Architecture." https://www.iso.org/standard/65695.html August 2018.

Microsoft Azure. "Security best practices for Internet of Things (IoT)." https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-best-practices October 2018.