NIST Internal Report
NIST IR 8572

Workshop Summary Report for "Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers"

Katerina N. Megas
Michael Fagan
Barbara Cuthill
Brad Hoehn
Evie Petrella

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8572

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8572

Workshop Summary Report for "Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers"

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

Brad Hoehn
HII

Evelyn Petrella
Electrosoft

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8572

May 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2025-05-06

How to Cite this NIST Technical Series Publication
Megas, K, Fagan M, Cuthill B, Hoehn B, Petrella E (2025) Workshop Summary Report for "Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers". (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8572.
https://doi.org/10.6028/NIST.IR.8572

Author ORCID iDs
Katerina Megas: 0000-0002-2815-5448
Michael Fagan: 0000-0002-1861-2609
Barbara Cuthill: 0000-0002-2588-6165

Contact Information
iotsecurity@nist.gov

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

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8572/final, including related content, potential updates, and document history.

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

Abstract

This report summarizes discussions held at the March 5, 2025 "Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers” organized by the NIST Cybersecurity for the Internet of Things (IoT) program. This workshop follows an earlier event held in December 2024 titled “Workshop on Updating Manufacturer Guidance for Securable Connected Product Development” to identify major update areas to NIST IR 8259. Similarly, the purpose of this more recent workshop was to discuss planned updates to NIST IR 8259 and gather additional feedback on taking a product viewpoint with greater emphasis on the IoT product lifecycle, expanded discussion of risk analysis, application to industrial contexts, and cybersecurity considerations around data management to support privacy goals. Over time, NIST work has built upon the concepts introduced in the NIST IR 8259, as reflected in subsequent publications that elaborate on IoT cybersecurity for specific sectors and use cases (e.g., federal agency use of IoT, consumer use of IoT in the home or in small businesses).

Keywords

Internet of Things; IoT products; manufacturing; risk assessment; product lifecycle; securable products; security requirements; software development; threat modelling.

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.

Table of Contents

List of Tables

1. Introduction

On March 5, 2025, NIST's Cybersecurity for Internet of Things (IoT) program hosted "Workshop on Foundational Cybersecurity Activities for IoT Device Manufacturers" to continue discussion of potential updates to Foundational Cybersecurity Activities for IoT Device Manufacturers, NIST IR 8259 [1]. The March workshop follows the December 4th, 2024, workshop titled "Workshop on Updating Manufacturer Guidance for Securable Connected Product Development" which first explored potential updates to NIST IR 8259.

The March 5th workshop documented in this report featured an overview of the status of updates to NIST IR 8259, extensive question and answer opportunities and invited two keynote speakers to discuss current cybersecurity and IoT topics relevant to the NIST IR 8259 updates. The workshop had both in-person and virtual participants, with both groups participating in the discussions that yielded significant feedback for NIST. This report summarizes what was discussed at the workshop to provide these insights to the broader community.

The table below illustrates the takeaways from the workshop, which are discussed in Section 3.

Table 1 - High-Level Summary of Workshop Takeaways.

1.	There is broad support for expanding the discussion of IoT products in NIST IR 8259 to make products more central to the IoT cybersecurity baseline and allow further exploration of the cybersecurity considerations of other IoT product components beyond the device.
2.	Many cybersecurity challenges are aggravated by the limited visibility each role in the IoT ecosystem (e.g., manufacturer, integrator, customer) has into the cybersecurity of the whole system**.**
3.	Performing risk analysis for IoT products remains a challenge due to the potential for unintended use or unexpected environments of use.
4.	In understanding the magnitude of a risk, it is important to understand the scale of the potential impact from a threat.
5.	Communicating effectively throughout IoT pre-market and post-market activities involves bridging gaps between manufacturer knowledge and customer ability to use the information.
6.	Transparency and traceability are foundational to maintaining product cybersecurity throughout the IoT product lifecycle.
7.	Discussions throughout the workshop highlighted challenges in IoT product lifecycle management emphasizing IoT product risks, vulnerabilities, and evolving ecosystem demands.

1.1. About the NIST Cybersecurity for the Internet of Things Program

This workshop was planned and executed by NIST's Cybersecurity for IoT program. The Cybersecurity for IoT program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale. One aspect of the

program's work is creation and maintenance of guidelines for IoT cybersecurity, including, but not limited to the focus of this workshop: NIST IR 8259.

1.2. NIST IR 8259 Background

In May 2020, NIST published Foundational Cybersecurity Activities for IoT Device Manufacturers, NIST IR 8259, which describes recommended cybersecurity activities that manufacturers should consider integrating into their product development and support lifecycle. These foundational cybersecurity activities can help manufacturers lessen the cybersecurity-related efforts needed by customers, which in turn can reduce the prevalence and severity of IoT device compromises and the attacks performed using compromised devices.

Over time, subsequent work has built upon the concepts introduced in NIST IR 8259 to introduce technical (IoT Device Cybersecurity Capability Core Baseline, NIST IR 8259A [2]) and non-technical (IoT Non-Technical Supporting Capability Core Baseline, NIST IR 8259B [3]) concepts to help manufacturers and customers consider the cybersecurity of IoT devices. The NIST IR 8259 series has been used to inform and develop further publications that elaborate on IoT cybersecurity across sectors and use cases (e.g., federal agency use cases and the U.S. Cyber Trust Mark).

NIST IR 8259 serves as a foundational document providing the conceptual and contextual basis for all of these publications. However, these subsequent publications introduced new concepts that, along with IoT and cybersecurity technologies and trends that have developed since 2020, could be beneficial to updating NIST IR 8259.

1.3. Workshop Event Details

The purpose of the March 5th workshop was to continue discussions from the December workshop related to a major update of NIST IR 8259. The planned updates include a greater emphasis on:

- Consistently taking a product viewpoint rather than a device-centric approach
- Emphasizing risk analysis in determining needed product cybersecurity capabilities
- Adding maintenance, end-of-support, and end-of-life considerations
- Enhancing discussion of application to industrial contexts
- Explicitly considering cybersecurity needs for data management to support privacy goals

The agenda for the event is provided in Table 2.

Table 2 – Workshop Agenda.

Time	Title	Speaker(s)
9:00 AM – 9:15 AM	**Welcome**	Katerina Megas, NIST
9:15 AM – 10:00 AM	**Morning Keynote Presentation:** *Fortifying the Future: Enhancing IoT Security Frameworks*	Jon Boulos (Kimberly-Clark)
10:00 AM – 10:45 AM	**IR 8259 Rev. 1 Preliminary Update: Overview**	Mike Fagan, NIST
10:45 AM – 11:00 AM	Break	
11:00 AM – 11:55 AM	**IR 8259 Rev. 1 Preliminary Update: Session 1** Activity 1: *Identify Expected Customers and Define Expected Use Cases* and Activity 2: *Research Customer Cybersecurity Needs and Goals*	Mike Fagan, NIST
11:55 AM – 1:00 PM	Lunch Break	
1:00 PM – 1:45 PM	**Afternoon Keynote Presentation:** *Leveraging FIDO Alliance cybersecurity standards in support of IR8259*	Brad Goodman (Fast Identity Online Alliance and Dell)
1:45 PM – 2:45 PM	**IR 8259 Rev. 1 Preliminary Update: Session 2** Activity 3: *Determine How to Address Customer Needs and Goals* and Activity 4: *Plan for Adequate Support of Customer Needs and Goals*	Mike Fagan, NIST
2:45 PM – 3:00 PM	Break	
3:00 PM – 3:45 PM	**IR 8259 Rev. 1 Preliminary Update: Session 3** Activity 5: *Define Approaches for Communicating to Customers* and Activity 6: *Decide What to Communicate to Customers and How to Communicate It*	Mike Fagan, NIST
3:45 PM – 4:00 PM	**Closing Remarks**	Mike Fagan, NIST

The rest of this report is organized as follows:

- Section 2 summarizes each invited speaker's remarks given on the day of the workshop.
- Section 3 summarizes the takeaways and observations across the entire workshop.
- Section 4 concludes the report.

2. Speaker Summaries

The summaries below highlight significant points from the speakers and identify discussion topics.

2.1. Jon Boulos, Kimberly-Clark and Wisconsin IoT Council, "Fortifying the Future"

Mr. Jon Boulos focused on considering cybersecurity risks and controls from a product and ecosystem perspective. Many of today's traditional IoT security programs focus on a device-centric approach. His presentation provided an overview of cybersecurity activities that should take place in each step of the product life cycle. Performing a risk assessment during the planning and design stages should accommodate growth within the expanding IoT ecosystem within its lifecycle stages. By adopting a product-centric approach, IoT device manufacturers can ensure comprehensive cybersecurity measures that are proactive, user-centric, and better aligned with the overall product lifecycle and user needs.

This discussion included the integration of IoT devices into industrial systems and how it requires a comprehensive approach to address the complexities and security challenges. He pointed out that integration of IoT devices into industrial systems significantly increases the complexity of those systems. Adopting IoT technology and developing these secure systems requires a unique skillset and often is seen as a significant investment. Ensuring interoperability and security can be difficult without established standards and protocols.

Mr. Boulos went on to highlight opportunities to help device manufacturers succeed and move faster:

- Create clear standards and guidelines from a cybersecurity and privacy perspective for IoT device manufacturers and solution providers.
- Certification and labeling programs are emerging for both devices and overall solutions.
- Data standards, integration, and communication protocols can help facilitate ecosystem compatibility to ensure devices can communicate.
- Dependable supply chains are important.
- Clear and consistent standards increase device interoperability and decrease cost.
- Providing direction on "mandatory" requirements would benefit manufacturers.
- Educating the workforce and/or future workforce for the digital transformation of the economy, such as developing training initiatives to increase skilled resources to implement and maintain IoT solutions.
- Public and private partnerships strengthen IoT security by leveraging the strengths, knowledge, and resources from both industry and government.

The overall goal is to provide adequate flexibility for innovation while maintaining an appropriate level of security based on the context of the use case, data, risk, etc. Manufacturers

would also benefit from clarification on where the US Cyber Trust Mark applies as well as the standardization of protocols and network infrastructure.

2.2. Brad Goodman, FIDO Alliance and Dell, "Leveraging FIDO Alliance cybersecurity standards in support of IR8259"

Mr. Brad Goodman discussed the Fast Identity Online (FIDO) Alliance's work on the FIDO Device Onboarding (FDO) Initiative and on FIDO's Passkey credentials. FIDO is an open industry association with a focused mission to reduce the world's reliance on passwords. The central concern is that while techniques and methods already exist to secure point-to-point communication, systems can still be easily exploited.

FDO addresses the question of establishing trust between two points to communicate securely, reliably, and in an automated fashion. It is a method for secure, zero-touch IoT device onboarding. Zero-touch means that it does not require a user to perform any operation. FDO provides mutual assurance between cloud and device that each is genuine and should interoperate with the other. It is all public key based.

FIDO's principal project is Passkey which is a password replacement based on FIDO protocols that provide faster, easier, more secure sign-ins to online services. A passkey may be synced across a secure cloud so that it is readily available on all of a user's devices, or it can be bound to a dedicated device such as a FIDO security key. Passkeys are a user authentication system. In the IoT space, this would most probably be used to secure user-to-cloud components of an IoT product to control the product.

Mr. Goodman spoke on the technical protocols of how FIDO device onboarding works from factory to owner. Identity of a device should always be done through key-based mechanisms. FDO provides a way to initiate a strong, binding enrollment or security between device and cloud, whereas passkeys provide phishing-resistant password-less user authentication to that cloud. Mr. Goodman indicated that the scope of the process is designed to work across a spectrum of use cases and hardware types and that FDO provides a rigid and provable mechanism to establish ownership.

3. Workshop Takeaways

This section summarizes the takeaways and observations across the entire workshop from invited speaker presentations to breakout sessions.

The following takeaways are the ideas, observations, and suggestions that NIST heard from workshop discussion participants, and which received significant support from participants. This workshop was not a forum for developing consensus; rather, the takeaways represent recurrent themes which emerged during discussions—not formal positions taken by participants. This document cannot capture every thought, opinion, and suggestion provided during the workshop. These takeaways do not represent NIST recommendations or guidelines; rather, they provide important feedback to the program and serve as a basis for future conversations within the community.

3.1. Support for a focus on product level cybersecurity in NIST IR 8259

There is broad support for expanding the discussion of IoT products in NIST IR 8259 to make products more central to the IoT cybersecurity baseline and allow further exploration of the cybersecurity considerations of other IoT product components beyond the device.

The workshop discussion participants were supportive of NIST IR 8259 taking a product viewpoint to approach cybersecurity and recognized the value in moving from the existing document's device-centric focus. Discussions indicated that IoT product components, which may be remote, have important access privileges to and control over the IoT device or devices within the IoT product. It was recognized that the special relationship between IoT product components creates new cybersecurity risks. These risks arise due to product components sharing potentially sensitive data and having control responsibilities over the IoT device's behavior.

3.2. Roles and their effect on cybersecurity challenges in the IoT ecosystem

Many cybersecurity challenges are aggravated by the limited visibility each role in the IoT ecosystem (e.g., manufacturer, integrator, customer) has into the cybersecurity of the whole system.

When discussing IoT cybersecurity, the participants frequently returned to the challenge of the varying information and visibility available to different roles across the IoT ecosystem. Manufacturers are best positioned to understand the cybersecurity capabilities of their IoT products including the cybersecurity capabilities of components from across the supply chain that are used to create the IoT product. Customers have highly varying cybersecurity knowledge depending on a number of factors such as whether they are a home consumer, small business, or large enterprise. Participants noted that additional roles are often needed in heterogeneous systems where components from various manufacturers must function securely together. System integrators, brand owners, retailers and other specialized support services can be mediators between the manufacturer and customer. These discussions also emphasized the role of third-party platform providers.

Clarifying expectations and collaborating among roles is critical for securing the IoT ecosystem. With manufacturers, brand owners, integrators, and customers all having unique responsibilities, participants stressed the need to clearly define these roles to help streamline collaboration, communication, and risk management. Integrators were noted in particular as key intermediaries, responsible for adapting manufacturers' security protocols to customer-specific demands and helping bridge communication gaps effectively.

Some participants identified a need for worked examples to help clarify potential collaborations across roles in the ecosystem such as integrators and manufacturers. For example, an integrator may need to analyze the risk of incorporating multiple systems from multiple manufacturers for a specific deployment.

3.3. Challenges of IoT product risk analysis

Performing risk analysis for IoT products remains a challenge due to the potential for unintended use or unexpected environments of use.

Participants discussed the challenges manufacturers face in conducting risk assessments without full visibility into customer environments. It was noted that in large enterprises or high security environments, there is a need for collaboration among manufacturers, system integrators, and customers due to shared responsibility and the need for customers to also perform some risk analyses. NIST's *Risk Management Framework for Information Systems and Organizations,* NIST SP 800-37 Rev. 2 [4], *Security and Privacy Controls for Information Systems and Organizations,* NIST SP 800-53 rev. 5 [5], and *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements,* SP 800-213 [6] provide information for manufacturers, system integrators and enterprise customers in the performance of risk assessment and mitigations. Several participants responded that these resources were helpful, but additional guidelines or standards are needed that take the manufacturer's perspective and consider varying risk levels across diverse deployment environments. Participants noted that current risk assessment mechanisms are aimed at addressing vulnerabilities within known, specific environments, which does not easily fit the typical manufacturer viewpoint of seeking to consider a range of possible product deployments. Participants highlighted the importance of these clarifications to ensure risks are properly identified, prioritized, and mitigated.

Alternatively, small business customers or home consumers cannot be expected to have the knowledge needed for detailed risk analysis and rely on the manufacturers who must assume greater responsibility. It was noted that the US Cyber Trust Mark program for certifying the cybersecurity of consumer IoT products only covers products as the manufacturer ships and maintains them and does not consider that installers or other IT professionals acting on behalf of the customer might have a role. The discussion underscored the complexities of the manufacturer-customer relationship emphasizing the need for careful communication to collaboratively navigate risk challenges.

Some participants noted that there are scalability concerns with tailoring products to individual customer needs or deployment scenarios. Customization to individual deployments could strain

resources. It was suggested that integrators could play a critical role in adapting products to meet specific operational demands.

3.4. Scaling threat impacts and relating to the magnitude of risks

In understanding the magnitude of a risk, it is important to understand the scale of the potential impact from a threat.

Risk is defined as "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." [7] While threat taxonomies exist (e.g., MITRE EMB3D), there are no widely recognized taxonomies for discussing the potential impact of a threat. In the workshop discussions, participants discussed the impact of threats in terms of:

1. Operational impacts to the specific local networks, IoT devices, and Information Technology (IT) experiencing the cybersecurity event; and
2. Environmental impacts that use the resources of compromised local networks to launch broader attacks on critical infrastructure or industries (e.g., botnets).

The participants also used terms such as "vertical" versus "horizontal," respectively, when discussing these two scenarios, illustrating the lack of consensus on the terminology. Though risks are generally categorized as having either operational or environmental impacts, environmental impacts could be a step towards operational impacts or vice versa.

3.5. Communicating effectively involves bridging gaps between manufacturers and customers

Communicating effectively throughout IoT pre-market and post-market activities involves bridging gaps between manufacturer knowledge and customer ability to use the information.

Communication emerged as pivotal to both the pre-market and post-market stages across multiple discussions with participants regarding challenges, strategies, and roles. While some emphasized the limitations manufacturers face in direct communication with customers, especially for products sold through retailers or installed by integrators, others agreed that raising broader cybersecurity awareness is critical.

Discussions indicated pre-market efforts should include setting clear expectations about device capabilities, operational lifespans, end-of-life plans, and modular upgrade paths to provide clarity to customers and integrators.

For post-market communication efforts, participants discussed the importance of communication planning including:

- How to tailor communication strategies to align with the expected customers' knowledge, and

- Education and awareness strategies targeting both consumer and workforce users that focuses on explaining IoT product behavior, mitigating anomalies, and practicing strong cybersecurity hygiene.

As part of post-market communication, participants further emphasized the need for ongoing communication about vulnerabilities, fault tolerance, updates, and product behaviors. Participants discussed the importance of manufacturers ensuring that messages are clear and are delivered using effective notification systems. One participant suggested that automation with tools like the Open Security Controls Assessment Language (OSCAL) can provide real-time monitoring and updating, ensuring consistent and accurate communication.

Difficulties maintaining direct communication with customers and users limit the ability to convey critical product updates, vulnerabilities, or lifecycle plans. This gap necessitates that manufacturers acknowledge what limitations to communication exist and acknowledge that some ability to reach customers may be lost when retailers or integrators act as mediators between the manufacturer and customer.

3.6. Transparency and traceability throughout the IoT product lifecycle

Transparency and traceability are foundational to maintaining product cybersecurity throughout the IoT product lifecycle.

Participants emphasized the importance of both transparency and traceability in IoT product lifecycle management. In this context, transparency is open communication about cybersecurity practices and lifecycle expectations, and traceability is the ability to track and verify IoT components throughout their lifecycle**.**

Transparency was noted as foundational for addressing vulnerabilities, setting expectations, and fostering trust among stakeholders; however, transparency can also bring risks. Participants discussed the potential risks resulting from attackers exploiting publicly disclosed information (e.g., vulnerabilities). It was further noted that the customer and the attacker might be one and the same, such as when a malicious actor purchases a product for the purpose of identifying its vulnerabilities and exploiting other instances of the product. While acknowledging these challenges, it was noted that transparency helps mitigate long-term risks by providing the customer and others in the ecosystem the insights and solutions needed to maintain the products' cybersecurity. Some participants pointed out that transparency in reporting problems is particularly vital to customers, and that information gained when manufacturers are transparent can be utilized by proactive customers.

Participants noted the value of traceability when securing the supply chain, ensuring chain of custody, and implementing tamper-proof mechanisms. Participants pointed out tools like Secured Component Verification (SCV) certificates and device keys are mechanisms to help improve traceability. Zero-trust architectures using techniques like real-time continuous monitoring were suggested as ways to enhance traceability across IoT ecosystems, but these could pose a challenge in operational environments which are sensitive to latency.

3.7. Additional cybersecurity related challenges

Discussions throughout the workshop highlighted challenges in IoT product lifecycle management emphasizing IoT product risks, vulnerabilities, and evolving ecosystem demands.

Participants discussed a number of evolving challenges related to cybersecurity that have emerged for IoT products:

- Risks posed by unsupported "zombie devices" that lack updates or patches, compensating controls to address the additional risk from this status, and continue to operate on the network, creating security blind spots;
- Lack of secure disposal for decommissioned IoT products and product components to prevent exploitation of sensitive data or credentials as a weakness in the IoT ecosystem;
- Absence of modular replacement strategies for IoT products in long-term use cases such as industrial or healthcare settings where lifespans for products may be long;
- Concerns raised regarding replay attacks during ownership transitions that can make the prior owner’s data accessible to the new owner;
- Potential for unexpected or nefarious activity from IoT products such as collecting unintended data continues to impede trust in IoT;
- Practical complexities of integrating IoT products into diverse ecosystems; and
- Technical challenges to supporting post-quantum cryptography for most IoT products, particularly on IoT devices.

While some ideas for means of addressing these challenges came up during discussions, all need further evaluation to identify the right mix of technical capabilities, manufacturer support, and public education to address.

4. Conclusion

The March 5th workshop was a productive conversation that yielded many discussions and significant feedback. The workshop was structured to walk through the NIST IR 8259 document pre-market and post-market activities, starting with an overview and intertwined with keynote speakers who added context from their unique technical perspectives.

From the participant discussions, NIST received feedback that will be important to the revision of NIST IR 8259. Continuing communication across the roles in the IoT ecosystem is essential to building robust IoT cybersecurity documents that apply in a wide range of deployment scenarios. In the long term, greater communication across these roles remains critical to understanding IoT cybersecurity challenges and potential means of addressing those challenges.

References

[1] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259. https://doi.org/10.6028/NIST.IR.8259

[2] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259A. https://doi.org/10.6028/NIST.IR.8259A

[3] Fagan M, Marron J, Brady K, Cuthill B, Megas KN, Herold R (2021) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259B. https://doi.org/10.6028/NIST.IR.8259B

[4] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[5] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[6] Fagan MJ, Marron JA, Brady KG, Jr., Cuthill BB, Megas KN, Herold R, Lemire D, Hoehn B (2021) IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-213. https://doi.org/10.6028/NIST.SP.800-213

[7] Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessments. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-30, Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

Appendix A. List of Symbols, Abbreviations, and Acronyms

FIDO
Fast Identity Online

FDO
FIDO Device Onboarding

IR
Interagency/Internal Reports

IT
Information Technology

IoT
Internet of Things

MITRE
MITRE Corporation

NIST
National Institute of Standards and Technology

NCCoE
National Cybersecurity Center of Excellence

OT
Operational Technology

OSCAL
Open Security Controls Assessment Language

SCV
Secured Component Verification

SP
Special Publication