NIST Interagency Report
NIST IR 8562

Summary Report for “Workshop on Updating Manufacturer Guidance for Securable Connected Product Development”

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.8562

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

NIST Interagency Report
NIST IR 8562

Summary Report for "Workshop on Updating Manufacturer Guidance for Securable Connected Product Development"

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

Brad Hoehn
HII

Evie Petrella
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8562

April 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

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

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.

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on 2025-03-21

How to Cite this NIST Technical Series Publication

Megas K, Fagan M, Cuthill B, Hoehn N, and Petrella E (2025) Summary Report for "Workshop on Updating Manufacturer Guidance for Securable Connected Product Development" (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8562. https://doi.org/10.6028/NIST.IR.8562

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

Abstract

This report summarizes the feedback received by the NIST Cybersecurity for the Internet of Things (IoT) program at the in-person and hybrid workshop on "Updating Manufacturer Guidance for Securable Connected Product Development" held in December 2024. The purpose of this workshop was to consider how to update *Foundational Cybersecurity Activities for IoT Device Manufacturers* (NIST Internal Report (IR) 8259) based on concepts in risk management, operational technology concerns, product end of life concerns and recent trends in IoT cybersecurity and privacy. Over time, the NIST volume of work has built upon the concepts introduced in NIST IR 8259,to add technical (NIST IR 8259A) and nontechnical (NIST IR 8259B) concepts to help manufacturers and customers consider the cybersecurity of IoT devices. The NIST IR 8259 series has been used to inform and develop subsequent publications that elaborate on IoT cybersecurity across sectors and use cases (e.g., federal agency uses cases reflected in NIST SP 800-213 and consumer use cases reflected in NIST IR 8425 and the U.S. Cyber Trust Mark).

Keywords

cybersecurity baseline; Internet of Things (IoT); IoT products; manufacturing; privacy; risk management; securable products; security requirements; software development; threat modelling.

Table of Contents

List of Tables

1. Introduction

On December 4th, 2024, NIST hosted a workshop titled "Workshop on Updating Manufacturer Guidance for Securable Connected Product Development" to introduce and discuss potential areas to update as the NIST Cybersecurity for Internet of Things (IoT) program revises *Foundational Cybersecurity Activities for IoT Device Manufacturers,* NIST IR 8259. The workshop was structured into two portions: a morning colloquium of plenary speakers and afternoon discussion sessions to dive deeper into the topics highlighted in the morning. The workshop yielded many discussions and significant feedback for NIST. This report summarizes what was discussed at the workshop and provides these insights to the broader public.

The table of takeaways below illustrates the takeaways from the workshop from Section 3.

Table 1 - Table of Takeaways

1. Government actions to support strengthening IoT cybersecurity need to be coordinated with industry.
2. The use of robust frameworks and the adoption of open standards are crucial for effectively managing risks across heterogeneous environments.
3. The dynamic nature of threats requires more context aware inputs, more proactive tracking and mitigation measures, and more examination into the inputs of the threat modeling approach.
4. There are market opportunities to securely design the next wave of products with cybersecurity through end of life and instill incentives into the maintenance of existing products.
5. The balance of shared responsibility between manufacturers and users for improving security varies by sector and needs the right incentives for both.
6. There are broad challenges to integrating privacy objectives into IoT cybersecurity risk management.
7. There is an increased awareness for evolving cybersecurity responsibilities across the players of the IoT ecosystem from manufacturers to users of the ecosystem.

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

The mission of the NIST Cybersecurity for the Internet of Things (IoT) program is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidelines, and related tools.

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. The program collaborates with stakeholders across government, industry, international bodies, and academia.

1.2. 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, the NIST volume of work has built upon the concepts introduced in the NIST IR 8259 series to introduce technical, *IoT Device Cybersecurity Capability Core Baseline* (NIST IR 8259A) and nontechnical, *IoT Non-Technical Supporting Capability Core Baseline* (NIST IR 8259B) concepts to help manufacturers and customers consider the cybersecurity of IoT devices. The NIST IR 8259 series has been used to inform and develop subsequent publications that elaborate on IoT cybersecurity across sectors and use cases (e.g., federal agency uses cases reflected in *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (NIST SP 800-213) and consumer use cases reflected in *Profile of the IoT Core Baseline for Consumer IoT Products* (NIST IR 8425) and the U.S. Cyber Trust Mark).

NIST IR 8259 serves as a foundational document for these publications—providing these a conceptual and contextual basis. But in the extension of the documents over time, these subsequent publications introduced new concepts which would benefit the broader community in the foundational NIST IR 8259 series.

1.3. About the Workshop

The purpose of this workshop was to consider how to better align NIST IR 8259 with concepts introduced in later publications. For example, NIST IR 8425 explicitly discusses IoT products and the relationship among product components. NIST IR 8259 needs to align with these concepts. Additionally, some topics have consistently come up in discussions with the community that NIST considers as potential areas to add to a revision of NIST IR 8259, including:

- Broaden the discussions from a focus on the IoT system device component to considerations of entire IoT products (and connected products) to better reflect the wide variety of applications and use cases that exist.
- Develop the relationship between risk assessment and threat modeling activities.
- Address the different cybersecurity considerations among Information Technology (IT), Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT)
- Identify insights, considerations, approaches, etc. for IoT based on the NIST Privacy Framework, NIST Cyber Physical Systems/IoT Framework, NIST Cybersecurity Framework 2.0, and the NIST Secure Software Development Framework.

- Incorporate lessons learned and techniques developed in the execution of several IoT-related National Cybersecurity Center of Excellence (NCCoE) projects.
- Address emerging connected product technologies more directly (i.e., Immersive Tech, Artificial Intelligence).
- Discuss any relationship that may exist between the repairability of connected products and cybersecurity.
- Provide guidelines on balancing cybersecurity with device support considerations, especially when there is a significant mismatch between the expected end of support of the IT components and the end of life of the mechanical components of the connected products.

NIST held the publicly available hybrid workshop with virtual morning plenary sessions and afternoon in-person discussion sessions as detailed in the table below.

Table 2 - Agenda for the Workshop

Time	Title	Speaker(s)/Facilitators
9:00AM – 9:15AM	Welcome, Agenda, Goals for the day	Michael Fagan, NIST
9:15AM – 9:55AM	Building More Secure Devices Using Threat Modeling with MITRE EMB3D	David Keppler, Senior Principal Cybersecurity Engineer, MITRE Jack Cyprus, Cybersecurity Engineer, MITRE
9:55AM – 10:35AM	Secure by Design considerations for OT	Matthew Rogers, Industrial Control System (ICS) Expert, CISA
10:35AM – 11:15AM	Life in Maintenance Mode: What it means to keep connected devices secure	Stacey Higginbotham, Policy Fellow at Consumer Reports
11:15AM – 11:55AM	Getting Smart: An Overview of IoT Privacy	Dylan Gilbert, Privacy Policy Advisor, NIST
11:55AM – 12:00PM	Closing of the Morning Hybrid Session	Michael Fagan, NIST
12:00PM – 1:00PM	Break	
1:00PM – 2:00PM	Discussion Session 1 - NIST IR 8259 Post-Market Activities update	Greg Witte, Palydin, Facilitator
2:00PM – 2:15PM	Break	
2:15PM – 3:15PM	Discussion Session 2 – NIST IR 8259 Pre-Market Activities	Christine Abruzzi, Cacapon Cyber Solutions, Facilitator
3:15PM – 3:30PM	Break	
3:30PM – 4:00PM	Closing including thoughts from the breakouts	Michael Fagan

2. Speaker Summaries

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

2.1. Jack Cyprus and David Keppler, MITRE Corporation, presented 'Building More Secure Devices Using Threat Modeling with MITRE EMB3D'

David Keppler and Jack Cyprus, both from the MITRE Corporation, discussed building more secure devices through threat modeling with MITRE EMB3D[1]. They emphasized that threat modeling is crucial for identifying potential vulnerabilities and determining appropriate security measures. This process, which is increasingly used in industries such as industrial automation, automotive, and medical, involves defining the device, identifying key components and trust boundaries, and measuring the return on investment (ROI) of defenses.

There are various tools and processes for threat modeling, such as adversary models and attack trees. One prominent model, the MITRE EMB3D, fills gaps in existing data sources and offers a consistent understanding of threats and mitigations. This model categorizes threats based on device properties, such as hardware, system software, application software, and networking. It also includes references to the CWE and CVE databases for additional information and threat details.

The EMB3D model provides a common language for device vendors, users, and security researchers to communicate threats and mitigations. It includes three mitigation tiers—foundational, intermediate, and leading—that guide actions throughout a device's lifecycle. These mitigations are grounded in real-world information and provide a defensive starting point as well as steps for ongoing security improvements. By adopting a comprehensive threat modeling process like EMB3D, organizations can better protect their devices against potential threats and build more secure systems.

2.2. Matthew Rogers, Cybersecurity and Infrastructure Security Agency (CISA), presented, 'Secure by Design considerations for OT'

Matthew Rogers from CISA presented on the agency's Secure-By-Design pledge [2]and related efforts. Secure-by-design incentivizes security professionals to drive meaningful security changes and equips consumers with the knowledge to demand necessary security features. Establishing a secure and upgradeable foundation is crucial to avoid legacy infrastructure issues. Shared responsibility between asset owners and device manufacturers is essential, as software vulnerabilities are increasing and basic, preventable vulnerabilities can cause significant harm.

The Cybersecurity and Infrastructure Security Agency (CISA) introduced the 'Secure-By-Design' Pledge, with over 200 software manufacturers committing to deploy more secure products. Secure-by-design goals focus on secure software development and basic security functionality.

[1] See MITRE EMB3d at https://emb3d.mitre.org/
[2] See CISA Secure-by-Design Pledge at https://www.cisa.gov/securebydesign/pledge

Security is a collective responsibility involving manufacturers, integrators, and asset owners and operators. CISA helps clarify security roles and ensures all parties uphold their responsibilities. The key component of secure by design is seeing where manufacturers can embed cyber security from the start to make it more difficult or impossible for an integrator or asset owner to open a cyber security risk.

Current US critical infrastructure contains legacy systems without security functionality that inherently complicate adding security today. Infrastructure improvement options include the present 'Bubble Boy' method, which segments all traffic, targeted improvements, and the 'rip and replace' method. Secure operational technology (OT) devices need to be available to provide that defense in depth, so that any failures in segmentation do not result in total compromise. Secure-by-design for OT considers threat categories like vulnerability handling and data protection. It emphasizes open standards and autonomy at the asset and operator level. Resilience features should resemble those in the enterprise space, including secure communications, resilience, logging, and end-device capabilities.

2.3. Stacey Higginbotham, Fellow with Consumer Reports, presented, 'Life in Maintenance Mode: What it means to keep connected devices secure.'

Stacey Higginbotham of Consumer Reports noted that connected devices establish an ongoing relationship between the buyer, seller, and manufacturer. The lifetime of a connected product is often separate from its physical state. While physical products fail in visible ways, software degrades more quickly, often without consumer awareness. The industry also lacks adequate support for maintenance. Stacey's discussion highlighted three key areas: zombie hordes of end of life devices, supported devices with unsupportive owners, and herd immunity against malicious actors.

"Zombie devices" are those that no longer receive software support and security updates. Higginbotham noted that unsupportive owners can neglect cybersecurity issues, leading to vulnerabilities. Herd immunity in cybersecurity requires collective action from manufacturers and consumers. Most consumers are unaware or indifferent to the end of life status of their products, resulting in "zombie hordes". Communicating end of life status and dates is crucial, including proactive notification to consumers, retailers, and third parties. Companies should track devices to address critical vulnerabilities and create structured options for off-ramping zombie devices.

Higginbotham emphasized that company priorities often overlook device security. Manufacturers should implement vulnerability disclosure programs, track issues, conduct comprehensive security audits, and allocate budgets for security maintenance. Buyers must keep products updated or segmented, and legislation should clarify responsibility to ensure herd immunity. Companies should have a dedicated point of contact for security researchers and consider recalls for insecure devices. Stacey also addressed secure repairs, both before and after end of life. Good hardware should not end up in landfills, but unpatched zombie devices pose risks. Consumer Reports advocates for designing products for longevity, including features like hardware upgrades, crypto agility, and increased memory.

2.4. Dylan Gilbert, NIST Privacy Engineering Program Lead, presented, 'Getting Smart: An Overview of IoT Privacy'.

Privacy is a complex and evolving concept that safeguards important values like human autonomy and dignity. It reflects various factors and individual preferences and is highly context-specific, differing between public and private activities. Effective privacy risk management must consider these contexts and the various ways to achieve privacy, such as seclusion, limiting observation, and controlling facets of identity.

Gilbert emphasized that privacy could drive innovation and serve as a market differentiator. However, organizations need to have honest and risk-informed discussions about how best to balance optimizing data utility while protecting individuals' privacy, particularly in cases where privacy risk interacts with other risk domains such as cybersecurity. The NIST Privacy Framework helps organizations understand the relationship between privacy and cybersecurity risks in the context of the Internet of Things (IoT). Problematic data actions, such as deriving inferences about individuals, can pose significant privacy risks, particularly in consumer IoT.

A key factor in managing privacy risks is an organization's role in the data processing ecosystem, which includes the complex relationships among entities involved in data processing. An organization's role(s) in the IoT ecosystem can affect its legal obligations and the measures it should take to manage privacy risk. High-level goals for mitigating cybersecurity and privacy risks include protecting device security, data security, and individual privacy. The privacy engineering objectives of predictability, manageability, and disassociability can be useful to meet these goals by supporting the determination of privacy capabilities in IoT products.

Gilbert also discussed specific privacy risks related to IoT, such as interactions with the physical world leading to reputational harm or safety issues. Data processing might exceed the product's intended scope, and access, management, and monitoring features could result in loss of trust and economic loss. Additionally, privacy capability availability, efficiency, and effectiveness are crucial to prevent issues like discrimination and to maintain trust. IoT products need the capabilities to support configurations such as remote activation, prevention, and data minimization.

3. Workshop Takeaways

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

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

3.1. Examination of Role of Government in Coordination Initiatives

Government actions to support strengthening IoT cybersecurity need to be coordinated with industry.

The government plays a crucial role in strengthening IoT cybersecurity in coordination with industry, in areas such as promoting balancing security with operational needs, and consumer awareness through effective communication and education. In these efforts, the government must work collaboratively with industry stakeholders, recognizing its own limitations while providing expert support for broader cybersecurity objectives.

The speakers highlighted the government's initiatives like Secure by Design and programs like the US Cyber Trust Mark as crucial to encourage industry to balance security requirements with operational constraints in a range of environments from Operational Control (OT) to consumer products. Under such initiatives and programs, government and industry efforts need to align to ensure the effective implementation of cybersecurity measures. Participants voiced support for a unified whole-of-government approach to address the challenges posed across different sectors and use cases ensuring that security initiatives are both comprehensive and adaptable. Discussions highlighted that, while the government can support broad objectives and promote improved cybersecurity, it should be flexible concerning specific product security measures, which are the responsibility of manufacturers.

Instead, participants recommended that the government could provide top-level support for broader cybersecurity objectives, integrating planning approaches to navigate the complexities of different sectors. Tools like effective consumer education awareness campaigns may drive better security practices to ensure consumers are well-informed about cybersecurity measures as they evolve. Participants agreed that one key aspect of government involvement is effective communication, which the participants agreed should be action-based messages directed at consumers. For example, simplifying communication and facilitating customer outreach are ways to promote awareness and understanding of cybersecurity practices. Government-led programs for consumer education were seen as vital by the audience in driving consumer engagement and encouraging consumers to value secure products. It was noted that "one size fits all communications" does not address the varying levels of knowledge in the general public.

Broad understanding of cybersecurity information and what to do with it is essential for improvement in U.S. cybersecurity. This means tailoring the message to the expected audience and collaborating with industry to move toward a more robust cybersecurity ecosystem.

3.2. Importance of Leveraging Standards and Frameworks

The use of robust frameworks and the adoption of open standards are crucial for effectively managing risks across heterogeneous environments.

Throughout the workshop, the importance of established frameworks and open standards was discussed as beneficial to enhancing IoT security and reducing threats. Real-world examples showcased how these tools can effectively mitigate cybersecurity threats while considering interactions between mitigations and device properties. It was noted that there are emerging examples of standards organizations using threat frameworks to discuss risk management.

Open standards were discussed as crucial in fostering interoperability and resilience, particularly within OT and ICS environments. Participants underscored the value of standards in making vulnerability advisories more actionable through enhanced communication across various systems. The need for clear, informative references and robust use case examples was also highlighted, emphasizing their role in clarifying specific points and supporting industry best practices.

As topics of discussion, privacy compliance and risk management emerged as important yet distinct areas of focus. The discussions noted the challenges in defining authority for privacy and managing privacy risks and the value of frameworks such as the NIST Privacy Framework to address these challenges. Additionally, there was a recognized need for a product baseline and specific security controls at varying levels to enhance overall cybersecurity efforts. Participants noted that clear and direct communication, along with formalized sections within documents, would further support the effective implementation of best practices and ensure a comprehensive approach to cybersecurity.

3.3. Addressing Emerging Threats and Vulnerabilities

The dynamic nature of threats requires more context aware inputs, more proactive tracking and mitigation measures, and more examination into the inputs of the threat modeling approach.

During the workshop, discussions highlighted the dynamic nature of threats, emphasizing that threats should be examined within their specific contexts rather than by sector. Participants noted that this approach ensures a comprehensive consideration of threats and their impacts across different use cases. One participant noted the specific example of performing vulnerability analysis on a product and cited the need for comparable examples of threat analysis for manufacturers and customers alike to understand what should be done. Participants also noted that different products and product components have varying capabilities which influence threat boundaries and the nature of risks.

The importance of establishing expected customer use cases to identify threat actors was stressed, alongside the necessity of focusing on threat modeling rather than merely adhering to prerequisites and requirements. Participants discussed what decisions go into threat modeling to help determine 'who' may be attacking as much as 'what' threat(s) manufacturers need to protect against. This prompts an examination of meaningful inputs to threat modeling considering the impact of malicious actors on protocol design and implementation.

Participants also placed emphasis on proactive tracking and mitigation of vulnerabilities in connected devices with some participants noting that leveraging device-level security features can enhance threat detection and response. Discussions suggested focusing on enhancing existing system models, with a critical consideration of safety features, to address the unique threats posed by different products. Also as pointed out earlier, participants emphasized a need for a product baseline and specific security controls to address vulnerabilities comprehensively.

3.4. Lifecycle Management of Connected Devices

There are market opportunities to securely design the next wave of products with cybersecurity through end of life and instill incentives into the maintenance of existing products.

Participants discussed the disconnect between the physical product lifetime and the software and cybersecurity support provided for connected devices. This gap poses a challenge for maintaining the security and functionality of devices throughout their lifecycle. The need to promote transparency around end of life timelines and the structured off-ramping of insecure devices was emphasized. Participants stressed the importance of providing clear end of life information on product web pages and at the point of purchase.

A major concern raised was the lack of industry incentives for maintaining connected devices in maintenance mode. Current business models often do not support the long-term security and maintenance of these products. The workshop highlighted that this problem exists with consumer products as well as for customers of OT products with long life cycles and high replacement costs.

The importance of end of life product communication and management was emphasized, with participants noting that consumers struggle to find end of life dates for their connected devices. Proactive notifications, including vulnerability disclosures and off-ramping options, were deemed essential for managing these products effectively. Addressing IoT security vulnerabilities, enhancing segmentation, and disclosure practices were also key discussion points.

Furthermore, this workshop emphasized the need for designing secure products with a focus on long-term updates and maintenance. Participants recognized that current business models must evolve to incorporate and appropriately prioritize security and support. Incentives for companies to prioritize cybersecurity include brand reputation and customer trust. Ensuring reliable access to physical parts and implementing secure practices, such as code signing for over-the-air updates, were identified as critical steps. The collective action required to address the issue of "zombie devices"(as defined by one of the speakers) was also highlighted as a significant concern.

3.5. Incentivizing Security Improvements

The balance of shared responsibility between manufacturers and users for improving security varies by sector and needs the right incentives for both.

Participants explored various approaches to drive security improvements across all ecosystem participants. One primary focus was on balancing security requirements with cost and usability considerations. It was noted that while security is critical, it often comes with additional negative impacts to product usability. Participants noted the need to strike the right balance to ensure widespread adoption of security practices without compromising user experience.

A significant point of discussion centered around questions of consumer willingness to pay for security features. Participants argued that there is often a reluctance among consumers to invest in security, which underscores the need for expanded consumer education. It was highlighted that educating consumers about the value and benefits of security features could help shift perceptions and increase their willingness to pay for these enhancements.

From a product development perspective, some participants highlighted the lack of incentives to prioritize security unless driven by regulations. One participant pointed out that without regulatory pressure, manufacturers may not make end of life investments into their products or take other long-term security measures. Therefore, while market-driven incentives are valuable, regulatory approaches may be necessary to ensure comprehensive security improvements.

There was also emphasis on manufacturers relaying security information clearly and effectively, potentially leveraging data sharing between retailers and manufacturers. This approach could help bridge gaps and ensure customers are well-informed about the security features and updates related to their products. Customers who are better-informed about cybersecurity may have a greater incentive to look for cybersecurity features in products.

3.6. Integrating Privacy into IoT Security

There are broad challenges to integrating privacy objectives into IoT cybersecurity risk management.

Participants discussed the relationship between privacy and cybersecurity risks within IoT systems, recognizing the need to address unintended consequences from data collection and data processing. Emphasis was placed in the discussion on integrating privacy objectives like predictability, manageability, and disassociability into IoT systems while balancing these with security and operational requirements. The unique challenges of IoT, such as the extensive scale of data processing that often exceeds the original intended scope, were highlighted. Obtaining consent for all data processing activities and limiting data collection to meet user privacy preferences were noted as challenges.

The discussion also distinguished between privacy compliance and risk management, asserting that privacy engineering presents a broader challenge that should be addressed separately from cybersecurity outcomes like those in NIST IR 8425 and required for the US Cyber Trust Mark. The discussion highlighted that privacy considerations need to be embedded in technical design requirements to effectively mitigate risks. Participants advocated for the use of an established taxonomy and terminology for consistency and clarity

The importance of privacy engineering and incorporating technical design requirements was also emphasized. Participants asked for clear, robust examples and informative references within documents to support best practices. Participants also highlighted the need for using an established taxonomy and terminology for consistency and clarity when discussing privacy. Participants also pointed out that a comprehensive understanding of the data processing ecosystem's complexity and interconnectedness is vital for integrating privacy objectives. This includes maintaining confidentiality, integrity, and availability in IoT, and proactively managing privacy risks.

3.7. Shared Responsibility for Cybersecurity

There is an increased awareness for evolving cybersecurity responsibilities across the players of the IoT ecosystem from manufacturers to users of the ecosystem.

Participants indicated the importance of manufacturers communicating what customers can and need to do to maintain the cybersecurity of IoT products especially when there is an action to be taken. This includes notifications about security updates and support requirements for maintaining the product's security.

For example, including a real time assessment with a notification could help to better understand the risk such as notifying customers of a needed update and that failure to perform the update would leave the product in a downgraded cybersecurity state.

There was a suggestion that research into the needs and wants of consumers with respect to cybersecurity communication is needed. One option would be to run focus groups with consumers including those with limited background on cybersecurity. More research could lead to making communications more effective. This led to the question: what should be highlighted as specific actions from the manufacturer to the customer and what responsibility lies with the customer? It was noted that this observation may have different answers in some use cases (e.g., consumer sector) compared to others (e.g., OT and enterprise).

3.8. Conclusion

This workshop was a productive conversation that yielded many discussions and significant feedback for the NIST Cybersecurity for IoT Program to consider for the revision of NIST IR 8259. The morning plenary sessions began with discussions on building more secure devices using threat modeling, examining secure by design considerations for OT, examining the maintenance outlook on devices after end of life requirements, and examining how privacy implications extend beyond traditional IT into IoT. The afternoon breakout sessions featured participant discussions of topics on questions aligned to the pre-market and post-market activities of NIST IR 8259.

NIST heard that effective risk management in the IoT ecosystem requires a balanced approach that aligns industry needs with government capabilities; that utilizing robust frameworks, open standards, and context-aware inputs is vital for tracking and mitigating dynamic threats; that addressing the lifecycle of products and evolving cybersecurity responsibilities among all stakeholders are crucial elements; that enhanced coordination and innovative approaches in IoT cybersecurity can significantly improve risk management and security incentives which ultimately benefit both manufacturers and users.

NIST looks forward to joining industry for a follow-up workshop in March on risk management and threat modeling to obtain more feedback on the continuation of the discussion topics of this workshop and to gather more in-depth insights from the collaboration of the community on updating manufacturer guidelines for securable connected product development.

References

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

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

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

[4] National Institute of Standards and Technology (2024) The NIST Cybersecurity Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[5] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[6] Griffor E, Greer C, Wollman D, Burns M (2017) Framework for Cyber-Physical Systems: Volume 1, Overview. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1500-201. https://doi.org/10.6028/NIST.SP.1500-201

[7] Griffor E, Greer C, Wollman D, Burns M (2017) Framework for Cyber-Physical Systems: Volume 2, Working Group Reports. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1500-202. https://doi.org/10.6028/NIST.SP.1500-202

[8] Wollman D, Weiss M, Li-Baboud Y, Griffor E, Burns M (2017) Framework for Cyber-Physical Systems: Volume 3, Timing Annex, . (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1500-203. https://doi.org/10.6028/NIST.SP.1500-203

[9] Greer C, Burns M, Wollman D, Griffor E (2019) Cyber-Physical Systems and Internet of Things, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 1900-202. https://doi.org/10.6028/NIST.SP.1900-202

[10] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

[11] MITRE (2025) *MITRE EMB3D.* Available at https://emb3d.mitre.org/

[12] CISA (2025)*Secure by Design Pledge*. Available at https://www.cisa.gov/securebydesign/pledge

Appendix A. List of Symbols, Abbreviations, and Acronyms

CISA
Cybersecurity and Infrastructure Security Agency

CVE
Common Vulnerabilities and Exposures

CWE
Common Weakness Enumeration

ICS
Industrial Control System

IR
Interagency/Internal Reports

IT
Information Technology

IIoT
Industrial Internet of Things

IoT
Internet of Things

NIST
National Institute of Standards and Technology

NCCoE
National Cybersecurity Center of Excellence

OT
Operational Technology

ROI
Return on Investment