NIST Internal Report
NIST IR 8618

Workshop Summary Report for "Cybersecurity for IoT Workshop: Future Directions"

Michael Fagan
Jeffrey Marron
Barbara Cuthill

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8618

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

NIST Internal Report
NIST IR 8618

Workshop Summary Report for "Cybersecurity for IoT Workshop: Future Directions"

Michael Fagan
Jeffrey Marron
Barbara Cuthill
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8618

June 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST IR 8618
June 2026

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.

Publication History
Approved by the NIST Editorial Review Board on 2026-06-03

How to Cite this NIST Technical Series Publication
Fagan M, Marron J, Cuthill B (2026) Workshop Summary Report for “Cybersecurity for IoT Workshop: Future Directions”. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8618. https://doi.org/10.6028/NIST.IR.8618

Author ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Jeffrey Marron: 0000-0002-7871-683X
Barbara Cuthill: 0000-0002-2588-6165

Contact Information
IoTSec@nist.gov

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8618/final, including related content, potential updates, and document history.

Abstract

This report summarizes the presentations and feedback received by the NIST Cybersecurity for the Internet of Things (IoT) Program at the hybrid workshop on "Cybersecurity for IoT Workshop: Future Directions" held March 31 – April 1, 2026. The purpose of this workshop was to consider emerging and future trends for IoT technologies and their impact to IoT cybersecurity. Additionally, the workshop was intended to inform updates to NIST Special Publication (SP) 800-213 and the development of future IoT cybersecurity guidelines.

Keywords

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

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.

Acknowledgements

The authors wish to thank Danna O'Rourke Herrick for participating in the preparation of this document.

Table of Contents

List of Tables

List of Figures

1. Introduction

On March 31-April 1, 2026, NIST hosted a workshop titled “Cybersecurity for Internet of Things (IoT) Workshop: Future Directions.” The workshop discussed emerging and future trends for IoT technologies and how they will impact both enterprise IoT cybersecurity, and management of IoT products. Stakeholders from across government, industry, international bodies, and academia participated as speakers and attendees. NIST will use feedback collected from the workshop in the update of *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirement,* NIST Special Publication (SP) 800-213 [1]; a new publication documenting considerations for securely integrating healthcare IoT products into clinical environments; and determining next steps for providing clear, actionable guidelines for securing IoT products.

1.1. About the NIST Cybersecurity for Internet of Things Program

The mission of the NIST Cybersecurity for the IoT Program (“Program”) is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale. 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 strengthen these connections and foster an environment that enables innovation on a global scale.

The IoT Program Principles are founded in the understanding that: no product operates in a vacuum, desired outcomes and usability have to drive approaches, and there’s no one-size-fits-all approach.

1.2. Background

The NIST Cybersecurity for the IoT Program was established in 2017 to help real-world practitioners navigate the gray areas between information technology (IT) and connected products. This provides clarity when it comes to challenges, existing resources that are available, and understanding where we can provide further guidelines to help fill in the gaps.

Underlying this work has been a foundational understanding that connected products differ from traditional IT. This has implications for their use, as well as how they must be secured.

This “metro map” (see Fig .1) illustrates how the IoT cybersecurity publications fit together. While not strictly chronological, the “map” illustrates how these publications connect and have built upon one another. The “transfer points” show where there is an overlap of audiences.

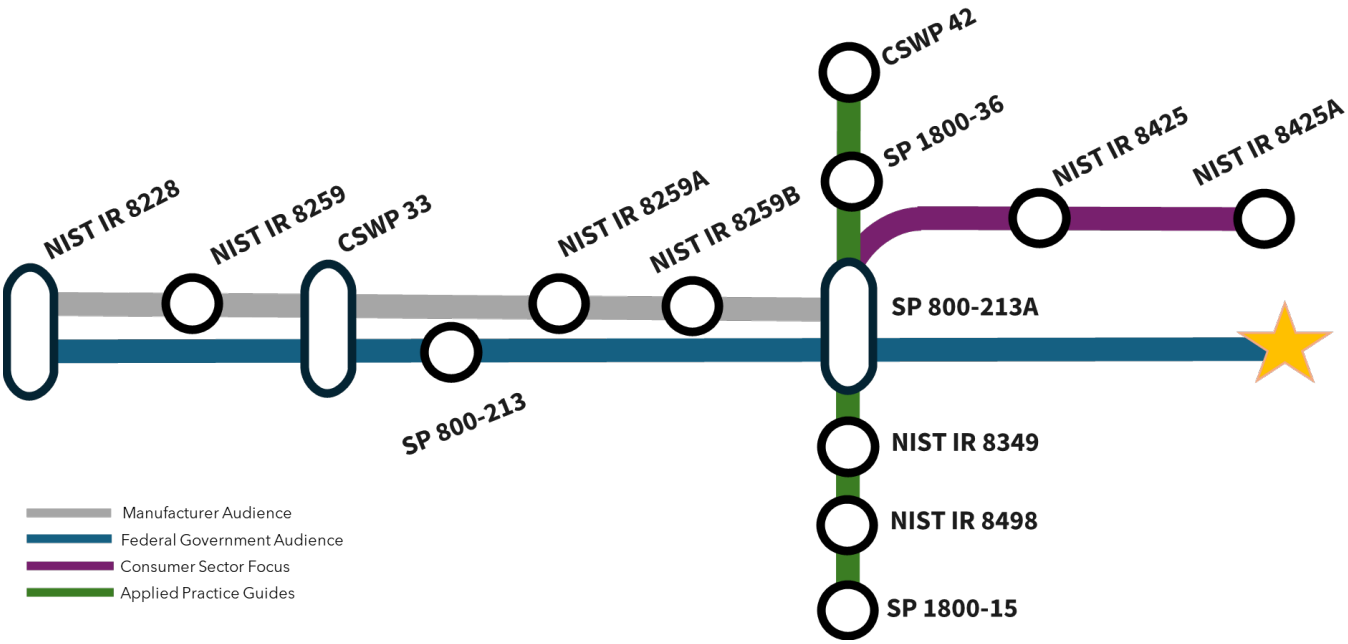

Figure 1: Cybersecurity for IoT Program Publication Map

One of the earliest publications (NISTIR 8228 [2]) illuminated how IoT products differ from traditional IT, common cybersecurity challenges seen across organizations, and the need to protect product security, data security, and individual privacy. From there, we continued along the "Blue Line" and "Silver Line" to focus on enabling innovation through: (1) working with IoT product manufacturers on creating securable products, and (2) working with federal practitioners to understand their needs, both for mission support and service delivery, as well as technical and regulatory needs.

These have moved towards more applied practice guides, running along the "Green Line," and consumer-focused resources on the "Purple Line." Of course, federal audiences, and a wide range of associated stakeholders (e.g., owners and operators of critical infrastructure with IoT products in the ecosystem and manufacturers selling to federal agencies) have always remained a priority.

1.3. About the Workshop

With this Workshop, the NIST Cybersecurity for IoT Program sought to better understand which IoT needs and considerations are most relevant to specific stakeholders. That way we can provide practical guidelines with a common language to manage connected products. Additionally, stakeholders have expressed the need for an approach to securing their IoT products and systems that helps them effectively navigate the large range of available documentation. This often becomes an academic exercise, like “homework” on top of their already busy job of managing technology to support mission needs and efficient use of cybersecurity resources. As such, the Workshop was intended to provide stakeholders an update on the NIST Cybersecurity for IoT Program, as well as to collect input on selected topics

to understand priorities for updating NIST SP 800-213 and creation of future guidance. Table 1 documents the Workshop agenda.

Table 1. Agenda for the Workshop

Time	Title	Speakers / Facilitators
Day 1 – Tue, March 31, 2026		
9:00-9:30am	Speaker: Welcome & Opening Remarks	Mike Fagan (NIST)
9:30-9:45am	Speaker: NIST IoT Cybersecurity Priorities & Background on the Program Priorities	Kat Megas (NIST)
9:45-10:00am	Speaker: Setting the Stage	Mike Fagan (NIST)
10:00-10:45am	Presentation: Identity of Things	Nick Allott (Nquiring Minds)
10:45-11:00am	Break	
11:00-12:00pm	Fireside Chat: Discussion of Light-Weight Cryptography, Post Quantum Cryptography and IoT	Mike Fagan (NIST) Kerry McKay (NIST) Colin Soutar (Deloitte)
12:00-1:30pm	Lunch	
1:30-3:30pm	Breakout Sessions: NIST SP 800-213 – Feedback	Mike Fagan (NIST) Ian Fleming (Deloitte)
Day 2 – Wed, April 1, 2026		
9:00-9:30am	Speaker: Welcome & Focus on the Future	Mike Fagan (NIST)
9:30-9:35am	Introduction for Speaker	Kathleen McTigue (NIST)
9:35-10:30am	Keynote: The Evolution of IoT in the Age of AI: How AI-Native Systems Redefine Cybersecurity and Trust	Benson Chan (Strategy of Things)
10:30-11:45am	Panel: Healthcare Considerations – Real World application and IoT Cybersecurity Controls	Jeff Marron (NIST) Nadia Elkaissi (Veteran's Affairs Central Office) Nastassia Tamari (Food and Drug Administration) Connor Walsh (Siemens Healthineers)
1:45 - 1:00pm	Lunch	
1:00- 2:00pm	Panel: IoT Risk In Context	Mike Fagan (NIST) Ian Fleming (Deloitte) Rishabh Das (Ohio University)
2:00-3:30pm	Breakout Session: IoT Risk Considerations	Mike Fagan (NIST)
3:30 - 3:45pm	Wrap-up & Conclusion	Mike Fagan (NIST)

Ultimately, the Program identified a number of broadly applicable considerations for developing and securely deploying IoT products across sectors and use cases – and to extend NIST's work to consider the cybersecurity of IoT product components beyond the IoT device. NIST understands the need to be agile and consider the needs of the product, the environment it's deployed in, and how the two interact. Ultimately, the goal is to provide useable, common language approaches to manage IoT products based on the context of their use.

Videos of each workshop segment are available on the event web page. Based on the participant presentations and feedback collected from stakeholders, this report provides a summary of key points and a general discussion of possible follow-on activities for the Program.

2. Speaker Summaries

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

2.1. Day 1: Welcome and Opening Remarks | Mike Fagan (NIST)

Mike Fagan, the Cybersecurity for IoT Program technical lead, described the focus of the two-day workshop on: NIST SP 800-213 updates, particularly for audiences handling federal government information systems; and wider future-looking IoT cybersecurity discussions.

Fagan discussed how NIST's SP 800-series fits under the Federal Information Security Modernization Act (FISMA) by providing information system guidelines for federal agencies and those who do business with the federal government. NIST SP 800-213 sits under this umbrella.

2.2. Day 1: NIST IoT Cybersecurity Priorities and Background on the Program| Katerina Megas (NIST)

Kat Megas provided context on the Cybersecurity for IoT Program's work to date, observations from the work, and how that intersects with emerging trends as the Program looks forward to what is next.

The Program was founded to address "how is IoT introducing new risks"; by focusing on identifying outcomes that help mitigate risks and encourage stakeholder engagement. In the course of the work, the Program learned that there was a lack of security on the devices themselves and worked to help organizations address this. Since then, NIST has published over 20 IoT cybersecurity documents, including the IoT cybersecurity core technical and non-technical baselines, and baselines tailored for specific sectors. All of the IoT cybersecurity work has been informed by extensive stakeholder comments.

IoT will continue evolving, as we see innovative new use cases: increasing productivity in manufacturing, applying new capabilities in critical infrastructure, supporting elderly to age in place, healthcare and connected medical devices. IoT continues to play a role in strengthening the U.S. economy

Today, many technologies are converging with IoT, including artificial intelligence (AI)-enabled robotics and post-quantum cryptography. NIST's role is to look to the future, where these emerging technologies are headed, and how they will impact IoT.

2.3. Day 1: Setting the Stage| Mike Fagan (NIST)

As IoT advancements and deployment continue to scale, there are changes in how we think about cybersecurity, in the context of the ecosystem of things. IoT devices are being used for increasingly important use cases, including to support and secure critical infrastructure; these use cases have heightened implications for risk and down time. The Program's approach to IoT cybersecurity – including for NIST SP 800-213 – is informed by these contexts.

The Program's aim is to help distill necessary considerations within the user's context to help manage IoT cyber risks, and to stay up-to-date with the guidelines.

NIST SP 800-213 was written in response to the IoT Cybersecurity Act of 2020, taking shape as a set of guidelines focused on the understanding that an IoT device would be incorporated into a system. The current revision under development responds to the evolving marketplace of IoT products with additional components beyond the device and new technical challenges. This revision will incorporate feedback heard since NIST SP 800-213 was published.

NIST's goal is to help adopters build or acquire securable systems that deliver the intended capabilities needed to meet mission requirements especially in critical infrastructure, where even a short downtime or disruption in command or data flows can have a large impact.

2.4. Day 1: Identity of Things | Nick Allott (Nquiring Minds)

Device identity is a foundational part of effective risk management, particularly as organizations face increasingly nuanced security, operational, and lifecycle challenges – today and moving into the future.

Trusted IoT Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security, NIST SP 1800-36 highlights several of the most important considerations.

The use of shared, often hard-coded passwords on devices across a network, creates a significant security vulnerability as compromise of a single device can expose the broader network. Regarding usability, limited or nonexistent user interfaces on many IoT devices make no-touch or low-touch provisioning a usability necessity, while also introducing challenges for secure onboarding at scale.

Policy encapsulation – particularly the use of device onboarding policies as a risk management approach – supports flexibility in operational risk management by enabling organizations to make informed decisions based on their understanding of risk. Rather than applying a single uniform response in every situation, it allows policies to reflect the specific context, risk profile, and operational needs associated with a device, system, or scenario.

Supply chain integration provides critical business and security information that can inform those policy decisions, including the data needed to assess device provenance, integrity, and trustworthiness.

2.5. Day 1: Discussion of Lightweight Cryptography, Post Quantum Cryptography and IoT | Mike Fagan (NIST), Kerry McKay (NIST), Colin Soutar (Deloitte)

Lightweight cryptography provides for efficient implementation on constrained IoT devices, while post-quantum cryptography (PQC) is about addressing the future breakage of current public-key cryptography. Organizations' decisions should include considerations of architecture, device constraints, lifecycle, and trust requirements, not treat them as the same problem.

Considerations of devices' long lifecycles and trust matter as much as encryption strength. Organizations should plan for long-term deployments, upgrade paths, and whether partners, customers, or government users will continue to trust interconnected systems that have not modernized their cryptography.

The panelists emphasized architecture-based decision-making, and not assuming every IoT device needs native PQC. This included dividing systems into zones and deciding where PQC belongs (often backend/external communications) versus where lightweight crypto fits best (often on-device).

Lightweight cryptography is not "weaker" cryptography, it is designed to keep strong security while reducing implementation cost and improving performance on constrained devices, including limits on RAM, ROM, battery, power, latency, and throughput. Its main use case is constrained IoT devices, where it may not make sense to use a large, expensive implementation to protect relatively low-value data or functions.

The panelists also discussed concern about the current danger of "collect now, decrypt later" attacks with PQC. Data protected using today's encryption could be intercepted now and decrypted later once quantum-capable attacks become feasible.

2.6. Day 2 Keynote: The Evolution of IoT in the Age of AI: How AI-Native Systems Redefine Cybersecurity and Trust | Benson Chan (Strategy of Things)

IoT is no longer best understood as a standalone technology category, as it is becoming part of broader AI-enabled operations. As such, IoT's primary role is to generate the data that powers intelligent operational decisions. The end goal is not just connected devices, but systems that move from sensing to action in a more automated, embedded way. He argued this evolution points toward "AI-native operations," where intelligence is designed into the operating model from the start rather than added later.

Many organizations are not operationally ready for this shift, as they still have fragmented data, limited ability to extract or structure machine data, and weak controls and capabilities, meaning they are "barely doing IoT" while feeling pressure from boards, investors, and potential gains to move into AI. Part of the adoption challenge is the gap between executive expectations and enterprise readiness.

Trust is the real adoption barrier: systems must produce outcomes that are relevant, accurate, safe, ethical, and fair. He emphasized that cybersecurity is not enough, as consumers do not differentiate between whether an issue was due to product design or cybersecurity flaws. Cybersecurity is one pillar of trust but is not on its own enough for consumers.

Trust must be built across infrastructure, operations, and people—including governance, skills, and change management. AI-native IoT was described as the future, where intelligence is built in from the start, while humans still set boundaries and remain accountable.

2.7. Day 2: Healthcare Considerations – Real World Application and IoT Cybersecurity Controls | Jeff Marron (NIST), Nadia Elkaissi (Veteran's Hospitals), Nastassia Tamari (FDA), Connor Walsh (Siemens Healthineers)

Panelists focused on the practical question: how can healthcare delivery organizations (HDOs) securely integrate medical devices into clinical environments, where risk depends heavily on context and where manufacturers, hospitals, and internal policies all have to work together?

Medical devices are not just IT assets. HDOs cannot always apply standard IT controls the same way they would for servers or workstations because some common IT controls (e.g., encryption, automatic updates) can affect device availability and subsequently patient care. HDOs consequently often rely on segmentation, isolation, and other alternate controls that achieve the same spirit as the IT control without the negative impact on medical devices and patient care. The discussion shifted from acquisition to integration, using healthcare as the example: the real challenge was how HDOs can securely incorporate medical devices into clinical environments.

Shared responsibility is needed, as risk cannot be managed by one party alone. There needs to be responsibility shared among manufacturers, healthcare providers, and internal organizational policies, as each shapes the overall security.

VA noted patient safety and mission continuity come first; with a very large device footprint, the challenge is securing innovative technology without disrupting care delivery. Additionally, FDA's message was that cybersecurity is part of safety and effectiveness, not a one-time compliance check. Devices should be secure by design, supported with required documentation and patching processes, and monitored across the full lifecycle because vulnerabilities can directly affect patient care.

2.8. Day 2: IoT Risk In Context | Mike Fagan (NIST), Ian Fleming (Deloitte), Rishabh Das (Ohio University)

The panel discussed how IoT security differs fundamentally from traditional IT security, highlighting how IoT and operational technology (OT) environments are inherently more distributed and shaped by physical constraints. Whereas IT security is built around data, IoT and OT security is built around physics. Unlike IT where data is more easily centralized, IoT often depends on mesh networking and local operation, so security models based in simple client-server assumptions can miss how these systems actually function.

Considering the context of use for a device (or a component) is necessary for securing these devices, with mention that traditional CIA (confidentiality, integrity, availability) need to be flipped in this instance to Security, Availability, Integrity and Confidentiality mattering in that order. They warned that cybersecurity controls can backfire if applied without operational context. While remote access capability from a device like a camera or drone is not necessarily a problem, it can become a security risk if organizations are not taking into consideration the full operational consequences of using the devices as such.

Sensor networks are a strong opportunity area for IoT, as acoustic, ultrasonic, and other specialized sensors can help detect equipment degradation, faults, or abnormal conditions in operational environments. This provides better visibility into asset health and system behavior, including for legacy devices that are often at the core of these systems. When combined with AI and heuristic-based detection, cybersecurity can shift to more predictive models, using IoT data to infer which devices are present, how they are behaving, and whether something abnormal may be happening in the physical process.

IoT cybersecurity will increasingly intersect with engineering, predictive maintenance, and operational resilience. Even when IoT adoption and integration go well, foundational differences between IT and OT still exist. Successful convergence still leaves architectural and governance challenges, as OT and IoT have different performance, reliability, and physical constraints than standard enterprise technology.

3. Workshop Takeaways

This section provides high-level descriptions of the main takeaways from the workshop, collected across the speaker sessions and the two in-person facilitated dialogues. Please note these takeaways are based on what NIST heard during speaker presentations, participant questions, and break-out discussion and are being reported here to document what was learned at the Workshop. Their inclusion does not directly reflect and should not be taken to imply any commitment from NIST, but the Cybersecurity for IoT Program will use these takeaways along with other information to plot future directions.

3.1. Product-Focused Approach

A product-based approach to IoT security was generally well received, with emphasis on the understanding that a device's functionality often depends on external software, services, and connected components. This more holistic view of security moves beyond traditional device-focused approaches and aligns with how IoT systems commonly operate today. There was discussion that NIST SP 800-213 and NIST SP 800-213A [3] could provide more clarity about an IoT product comprising the full set of interdependent components, not just the physical device itself.

3.2. Technological Convergence

As IoT products increasingly serve operational technology needs, they are being integrated into environments that were once relatively isolated. In some cases, agencies are even developing their own in-house IoT devices to expand upon commercial off-the-shelf requirements.

This is especially visible in remote monitoring contexts, where organizations deploy large networks of custom-built devices to collect geographically distributed data (e.g., waterway conditions, buoy-based water level measurements, and earthquake activity). These use cases highlight both the operational value of IoT and the privacy concerns that can arise from pervasive monitoring technologies.

Organizations need practical guidance to understand: where they are in their journey of integrating IT, IoT, and OT; which standards apply; and how to map product, device, and operational concerns to a comprehensive cybersecurity strategy.

3.3. Impacts of AI Integration and Emerging Technologies

IoT is increasingly understood not just as a collection of connected devices, but as a sensor network that feeds data into AI and machine learning systems, which can then have physical impacts. As AI-enabled capabilities evolve, security requirements can change for products and accelerate the need for stronger cyber controls, especially for devices with actuation capabilities.

Participants discussed the cybersecurity implications of using AI to control IoT systems, as well as in gathering additional perspectives on this issue across specialized environments such as

medical systems, utilities, and earthquake monitoring. They additionally noted the challenge of applying Zero Trust Architecture (ZTA) principles to IoT and OT environments, especially in light of OMB M-22-09 (Moving the U.S. Government Toward Zero Trust Cybersecurity Principles) and the wide range of interpretations for how such guidance should extend into operational settings.

3.4. Flexibility over checklists for managing device cybersecurity risk

There was strong support for staying away from rigid compliance checklists and toward a more flexible, risk-based model that accounts for specific device capabilities and operational use cases. This approach best accommodates the differences between products that only monitor conditions and those that can also control or actuate systems. More flexibility could also help address cybersecurity challenges in high-stakes environments, such as medical IoT and utilities, where emergency use requirements can complicate standard security practices.

Some discussion also centered on the use of zoning concepts, such as those found in IEC 62443, to assign security target levels based on the role of a device within a system. By separating cyber considerations from operational physics and evaluating devices within defined zones, organizations may be able to apply product security requirements in a more tailored and practical way.

4. Conclusion and Next Steps

IoT cybersecurity is becoming increasingly complex, due in part to the advancement of emerging technologies, IoT and OT convergence, and the quick rise of AI use and integration. The Cybersecurity for IoT Program remains committed to providing guidance for securing IoT, focused on cybersecurity for IoT, and the use of IoT for cybersecurity.

Stakeholders are seeking more clarity in IoT cybersecurity guidelines, and organizations are looking for guidance on securing their full suite of IoT devices, beyond what NIST SP 800-213 has to offer on integrating new devices. There is also a stated need for guidelines beyond how to integrate new devices. There is a stated need for guidelines that provide insight on how to manage risk, with flexibility to suit multiple use cases, but enough authority to avoid needing to make a patchwork using disparate documents. Considerations should include encryption needs for today, and the future as quantum technologies continue to advance; they should also acknowledge and take into account the impacts of convergence with OT.

Upon finishing updates to NIST SP 800-213, the NIST Cybersecurity for IoT Program will focus on providing guidelines with sufficient flexibility, context-based use cases, and referencing the appropriate existing documents. While there is a need for more centralized, authoritative guidelines, there is no need to reinvent the wheel. NIST remains committed to our Program Principles of considering the ecosystem of things, focusing on outcomes, and drafting guidelines to support practitioners as they navigate increasingly complex challenges.

References

[1] Fagan M, Megas KN, Marron J, Brady KG, Jr., 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) 800-213. https://doi.org/10.6028/NIST.SP.800-213

[2] Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas K, Nadeau E, Piccarreta B, Gabel O'Rourke D, Scarfone K (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[3] Fagan M, Megas KN, Marron J, Brady KG, Jr., Herold R, Lemire D, Hoehn, B (2021). IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A