NIST Internal Report
NIST IR 8431

Workshop Summary Report for "Building on the NIST Foundations: Next Steps in IoT Cybersecurity"

Katerina N. Megas
Michael Fagan
Barbara Cuthill
Brad Hoehn
David Lemire
Rebecca Herold

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8431

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

NIST Internal Report
NIST IR 8431

Workshop Summary Report for "Building on the NIST Foundations: Next Steps in IoT Cybersecurity"

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

Brad Hoehn
David Lemire
HII Mission Technologies

Rebecca Herold
The Privacy Professor

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8431

September 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

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

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

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

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on 2022-09-08

How to Cite this NIST Technical Series Publication:

Megas KN, Fagan M, Cuthill B, Hoehn B, Lemire D, Herold R (2022) Workshop Summary Report for “Building on the NIST Foundations: Next Steps in IoT Cybersecurity”. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8431. https://doi.org/10.6028/NIST.IR.8431

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

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

Reports on Computer Systems Technology

Abstract

This report summarizes the feedback received on the work of the NIST Cybersecurity for the Internet of Things (IoT) program on IoT product cybersecurity criteria at a virtual workshop in June 2022. The purpose of this workshop was to obtain feedback on specific considerations—and techniques for addressing those considerations—around cybersecurity in IoT products. These considerations have broad applicability across IoT product sectors, including the consumer IoT products sector and the industrial IoT sector. For consumer IoT, these considerations arose in moving the criteria presented in *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* into draft NIST IR 8425, *Profile of the IoT Core Baseline for Consumer IoT Products*, along with a discussion paper on the complexity of risk identification for IoT published before the workshop.

Keywords

Consumer IoT; Industrial IoT (IIoT); consumer profile; cybersecurity; Internet of Things (IoT); IoT products; privacy; Risk Management Framework; securable products; security requirements.

Audience

The main audiences for this publication are product security officers and security architects at IoT product manufacturers and those in their supply chain; cybersecurity test and evaluation experts; and other stakeholders in the IoT product market. This publication may also help customers or integrators of IoT products who are adopting IoT technologies in their residence or business, especially small business networks, as well as organizations concerned with conformity assessment of IoT products to published guidance.

Table of Contents

List of Tables

1. Introduction

On June 22, 2022, the National Institute of Standards and Technology (NIST) conducted a virtual workshop entitled *Building on the NIST Foundations: Next Steps in IoT Cybersecurity*. [1] The event included stakeholders from across government, industry, international bodies, and academia. The goal was to review recent work by the Cybersecurity for the Internet of Things (IoT) program [2] in defining cybersecurity requirements for consumer IoT products and gather feedback to aid the program in defining next steps. Over 170 people participated from the U.S. and 19 other countries, representing a broad mix of government, industry, and academia.

1.1. About the NIST Cybersecurity for IoT Program

The mission of the NIST Cybersecurity for IoT program is to cultivate trust in IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools. The program supports the development and application of these standards, guidelines, and tools to improve the cybersecurity of connected products and the environments in which they are deployed. By collaborating with stakeholders across government, industry, consumer advocacy groups, international bodies, and academia, the program aims to fulfill this mission and foster an environment that sparks innovation on a global scale.

1.2. About the Next Steps in IoT Cybersecurity Workshop

In response to Executive Order (EO) 14028 on Improving the Nation's Cybersecurity [3], NIST developed a set of cybersecurity criteria for consumer IoT products. These criteria were published in February 2022 along with discussions of considerations for product cybersecurity labels and associated conformity assessment needs as *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products* [4]. NIST received feedback on the criteria during the subsequent pilot program phase called for in the E.O.

In June 2022, NIST released two new documents:

- *Profile of the IoT Core Baseline for Consumer IoT Products* (NIST IR 8425 [DRAFT]) [5], and
- *Ideas for the Future of IoT Cybersecurity at NIST: IoT Risk Identification Complexity* [6]

The goal of the June 22 workshop was to discuss the concepts in the recent draft documents and gather stakeholder feedback to assist the Cybersecurity for IoT program in defining next steps.

The workshop agenda together is presented in Table 1. The agenda, short biographies of the keynote speakers, and the recording of the workshop are available on the NIST event information page [1].

Table 1. Workshop Agenda

Time	Activity and Presenters
10:00 - 10:15am	Welcome and Introduction • **Kat Megas**, NIST • **Kevin Stine**, NIST
10:15am - 10:45pm	Keynote: **David Barzilai**, Karamba Security, VP Sales & Marketing, Chairman and Co-Founder
10:45 - 11:15am	Keynote: **Jasyn Voshell**, Zebra Technologies, Director Products and Solutions Security
11:15am - 12:30pm	**Panel 1: What's next for the consumer IoT baseline: Considerations we heard for the Consumer IoT cybersecurity criteria.** • **Moderator: Jeffrey Marron**, NIST • **Karin Athanas**, TIC Council • **Amit Elazari**, Intel • **Dave Kleidermacher**, Google • **David Rogers**, Copper Horse LTD
1:00 - 2:30pm	**Panel 2: Product cybersecurity strategy: How do cybersecurity requirements fit into IoT product development** • **Moderator: Mike Fagan**, NIST • **Dave Elfering**, Werner Enterprises • **Daniel Hein**, Garmin • **Larry Ponemon**, Ponemon Institute • **David Wollman**, NIST
2:45 - 3:45pm	**Panel 3: The S in NIST: Using standards to support product cybersecurity outcomes** • **Moderator: Kevin G. Brady**, NIST • **Bryan Cline**, HiTrust Alliance • **Mike Bergman**, Consumer Technology Association • **Carol Muehrcke**, International Society of Automation (ISA) Global Cybersecurity Alliance • **Stephen Quinn**, NIST
3:45 - 4:00pm	Wrap Up and Next Steps Speaker(s) **Kat Megas**, NIST

The workshop drew over 170 participants, panelists, speakers, and moderators. This included representatives from:

- A mixture of government, industry, and academia, as well as researchers, consumer organizations, and the press
- A range of federal government organizations including civil government and defense
- 20 countries, including 2 foreign governments
- At least 2 U.S. state governments

In addition to the ability for participants to submit questions, the workshop included a series of seven polls as a mechanism to gather participants' feedback and influence the panel discussions. The poll questions and poll results are presented in Appendix A. Since workshop survey group participants and poll responses were entirely voluntary, poll results should not be viewed as providing statistically valid sample size results for their questions.

Videos of each workshop segment are available on the event web page [1]. 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. Summary and Key Takeaways

This section summarizes the keynote presentations and describes a set of takeaways developed from the keynote contents and the panel discussions.

2.1. Keynote: David Barzilai, Karamba Security

The first keynote was by David Barzilai, VP Sales & Marketing and Co-Founder, Karamba Security, which conducted a survey of Chief Product Security Officers (CPSOs), and their equivalents, to better understand the challenges of this role. David described the role of a CPSO and the challenges they face, especially when dealing with research and development (R&D) teams seeking to balance functionality and security in their products. He cited brand protection through maintaining consumer trust, customer service-level agreement (SLA) requirements, and regulatory compliance as the principal drivers for the creation of the CPSO role. David described a three-fold approach to improve product security and trustworthiness using standards and certifications, which he described as the "CPSO's best friends"; tools (such as binary analysis for supply-chain security, and vulnerability management systems); and best practices (establishing the manufacturers as being responsible for and monitoring product security). He also identified the reliance on "massive" supply chains as a huge challenge for addressing product security, noting that it is very hard for manufacturers to impose security best practices on their suppliers. He explained that using software bills of materials (SBOMs) would be very beneficial for creating transparency throughout the supply chain and allow manufacturers to more effectively monitor and address IoT product security risks.

David presented the automotive industry as driving "radical change" in the area of product security, creating a life cycle framework with mandatory processes. Failure to comply with these processes and address cybersecurity deficiencies means the resulting products cannot be sold. In that industry, the original equipment manufacturer (OEM) is ultimately responsible for the final product and able to allocate security requirements down to their suppliers. The supplier product security teams are empowered to do what is needed to meet the OEM's security requirements. The OEM must be able to demonstrate to regulators that cybersecurity requirements have been met throughout the supply chain and must address critical security and safety issues prior to moving vehicles to production. David pointed out that putting the manufacturers in control of the supply chain and making the manufacturer ultimately responsible for the security of the products, helped to ensure product security and safety, in this case for vehicles. However, he described how this could also be a way to drive change and improve security and safety for IoT products as well.

2.2. Keynote: Jasyn Voshell, Zebra Technologies

Jasyn Voshell, Director Product and Solutions Security at Zebra Technologies, provided the second keynote. Jasyn described Zebra as providing a diverse line of IoT and IT products, including mobile products, for a range of industries, and explained that his role is to guide the cybersecurity efforts of development teams across Zebra business units.

Jasyn briefly summarized the threat landscape and some recent high-profile events as motivating factors for OEMs to consider product security. He then described in detail Zebra's approach, based on three principles:

- "Secure by Design": Uses Secure Code Storage; Secure Code Training (e.g., training starting on day one, and regularly ongoing); Secure Code Scanning (e.g., tracking vulnerabilities, hard-coded secrets, code leaks and binaries); Policy/Framework (e.g., using System Development Lifecycle (SDLC), Open Web Application Security Project(OWASP), NIST); Industry Maturity Model (using the Software Assurance Maturity Model (SAMM)); Application Lifecycle Management/Product Lifecycle Management (ALM/PLM) Integration into Development Model (using Quality Service Model Operating System (SMOS));
- "Secure in Use": Employs mechanisms such as participating in the Bug90 program, penetration testing, and tracking metrics; and
- "Secure Thru Trust": Seeks to build connections with customers including a broad range of organizational partnerships, direct customer engagements, and the use of media to disseminate information about Zebra product security.

For each of the "Secure by Design" guidelines, Jasyn provided details about the associated activities, describing the guiding principle, as well as the goal, measures of success, and business benefits that mechanism provides. He explained that the overall goal is to design security into all products, which Zebra views as a competitive advantage.

Jasyn also described the relationship of a CPSO to a Chief Information Security Officer (CISO), explaining that while the roles are related and coordination between them is beneficial, their respective domains (product security for a CPSO, versus security of business operations for the CISO) are well defined and there is very little ambiguity about responsibilities.

2.3. Key Takeaways

The following takeaways are the ideas, observations, and suggestions that NIST heard from workshop participants, and which received significant support from attendees and/or panelists. This workshop was not a forum for developing consensus; rather, the takeaways represent recurrent themes that emerged over the course of the event—not formal positions taken by attendees or participants. While this document seeks to summarize discussions and viewpoints expressed by panelists and participants, it cannot capture every thought, opinion, and suggestion provided during the sessions. The supporting quotes and discussion for each takeaway are drawn from across all three panels. The major discussion points of the day are presented in terms of the takeaways that cut across panels. The takeaways do not represent specific recommendations or guidance; rather, they provide important feedback to the program, and serve as a basis for future conversations with the community.

Takeaway 1: The role of CPSO is becoming more prominent and important as manufacturers see the need to comply with various emerging requirements, and not be seen as lacking security. The CPSO and CISO roles are complementary and should have clear delineations of responsibility.

The workshop began with the keynote speakers' observations on this emerging role within organizations to bridge the divide between cybersecurity requirements and product development. Jasyn Voshell, Zebra Technologies, described that having a director of products and solutions security has led to more direction, more use of industry standards and more operational controls with more consistency across different development teams.

When prompted by a participant question on whether all IoT companies need a CPSO, speaker David Barzilai, Karamba Security, indicated that would not always be the case. He suggested that in the case of OEMs focusing on "low-security-awareness markets" or markets where attacks might not necessarily be an issue, the OEM could make a risk-based decision to allocate an architect from R&D who could serve in the CPSO capacity to assure the product security posture.

Takeaway 2: A growing number of OEMs are moving to a model of maintaining contact with purchased and deployed products and taking greater responsibility for monitoring and maintaining the product in operation.

In the second panel, David Elfering provided insights and perspectives from the viewpoint of an IoT product consumer, based upon his long tenure as the VP and CISO at one of the largest transportation and logistics corporations in the U.S. Over the last 25 years, since telematics were introduced, vehicles have become more complex, with their embedded equipment components and related equipment supply chains correspondingly becoming more complex. David pointed out that CISOs at large transportation organizations with smart vehicle fleets are expected to secure the full fleets, including the apps, clouds, and supply chain components where they often have no information and little to no control. He pointed out that such organizations, and all other types of organizations using IoT products in other industries, view these smart vehicles and equipment as products, and the organizations "are consumers like everyone else, even though we have massive amounts of complexity on top [of the traditional vehicle components]". More complexity, with more IoT products incorporated, also brought people together from more diverse areas from within the organization and from outside contracted vendors, to solve the expectations of the business's needs. As a result, this led to more pressure on OEMs to work with organizations throughout the supply chain to understand what is in the technology stack when issues arise. This is especially necessary to meet the new expectations of fast deliveries.

Daniel Hein, Garmin**,** also pointed to the ecosystem of the product including the mobile application, cloud, and back-end services in addition to IoT devices. With this perspective, he pointed out that organizations need more third-party integration at the OEM level. Facilitating the most success with such integration requires customers building and maintaining long-term relationships with the OEM in the ecosystem. OEMs have more incentives in the current ecosystem to support the distributors downstream in the supply chain and this is starting to take shape in different forms. Daniel pointed out that Garmin is being cost effective with what is required to accomplish the goals, needs and expectations of consumers, while also reaching the appropriate people, and doing what is acceptable for specific use cases. The automotive industry is a leading example of this approach, driven by safety compliance requirements that regulate whether or not products can be sold. The security of the diverse range of connected IoT devices, apps, cloud services, and all other components of the IoT products that are engineered within the vehicles impact safety in a significant way. This dependency on technology for a safe vehicle then necessitates that the full vehicle systems development life cycle, including the supply chain entities, have effectively implemented technical and non-technical cybersecurity capabilities.

Takeaway 3: Supply chain security is an on-going and increasing concern. However, the responsibility for product security including components from the supply chain ultimately belongs to the original equipment manufacturer (OEM, i.e., the producer of the final product). This makes it more important for manufacturers to expand their oversight of supply chain security, in addition to providing security requirements to their supply chain vendors and determining how to validate the requirements have been met.

As manufacturers are becoming more concerned over incidents involving their products, IoT product manufacturers are maintaining closer oversight of supply chain vendors and establishing more vendor security requirements for the components they provide. Imposing security requirements on supply chain organizations is difficult but can be supported based on standards and regulations. One challenge of supply chain cybersecurity identified was “how can you trust that the final vendor in the process has done their due diligence across the supply chain elements?” Different providers need information sharing across the supply chain.

There was discussion in Panel 2 on how the shift to just-in-time supply chain operations has caused orders of magnitude changes in efficiencies over the last two decades. David Elfering, Werner Enterprises, and Daniel Hein, Garmin, discussed the transportation sector at length. Larry Ponemon, Ponemon Institute, referenced to the changes that have occurred within the last decade in IoT use. Changes in society have increased the global supply chain, which in turn has been continually challenged at scale. What are the expectations for managing the supply chain and downstream outputs from the process? As David Elfering explained, the ‘need it in a day’ expectation provides different stresses on supply chain dependencies, and organizations today are trying to make supply chain management more important within their overall risk management programs.

There were some discussions on distinctions between IT and IoT, and how some assumptions about how security is implemented in IT products do not hold for IoT products, particularly when addressing safety, privacy, different types of supply chains, and the often unique and highly-diverse and complex environments within which the IoT devices are used. Panelists generally agreed that consideration of complete IoT products, instead of the specific IoT devices, will require changes in the ways in which associated risk assessments are performed, necessarily widening the scope. It will also change the ongoing risk management activities, requiring more types of activities to address the full IoT product instead of just considering the IoT device. This, in turn, will require the ability to obtain more information from throughout the supply chain. For example, how will IoT product manufacturers test components that come from supply chain entities for security and privacy risks? The IoT product manufacturer will need more information from, and possibly more communications with, the supply chain vendors than what has typically occurred to-date. Currently IoT product manufacturers have little-to-no insights about vulnerabilities within the supply chain products, and often little information about the security capabilities and vulnerabilities. Panel members generally agreed that worldwide collaboration for providing cybersecurity and privacy information for IoT product components is necessary, given the large and growing range of supply chain entities involved with each IoT product.

Tools to analyze supply chain outputs (e.g., binary analyzers and SBOMs) are also available, improving, and becoming more common. There was association between binary analysis for supply chain security following NIST recommendations for using SBOM, and vulnerability disclosure reports were viewed by the panel as an excellent source of security information. This provided viewpoints related to a participant question in chat who asked, "Is the EO sufficient in imposing awareness/compliance obligations across the Supply Chain—producers, component producers, acquirers, users (government and industry)?"

Takeaway 4: Standards, certifications, and maturity models are useful tools that can support manufacturers in creating and sustaining a secure IoT product development life cycle process.

Both keynote presentations discussed the importance of standards, and certifications invoking standards, as a crucial driver of product security, providing an essential counterbalance to other product development priorities. The NIST IR 8259 series [7, 8, 9] was designed to identify needs and goals for the manufacturer to consider not only for IoT product risk management, but also when identifying the standards and regulations that the IoT product cybersecurity and privacy requirements must meet. Needs and goals are sometimes influenced by existing limitations (e.g., inability to affect fielded products, or legacy systems that cannot practicably be updated). There is a bigger challenge as more devices become integrated, become a part of a larger infrastructure, and users become reliant upon them.

There is a need to use the existing security standards and guidelines while also looking towards the future, scaling security protections to bridge current risk management and mitigation needs with future evolutions of standards, certifications, and maturity models. A participant asked how to address the challenge of establishing and maintaining an IoT product inventory list given a mixture of IoT products of varying security characteristics, an example of bridging continued use of existing products as new products are incorporated within the digital ecosystem. Karin Athanas, TIC Council, responded “I think there's an awareness that there are going to be legacy devices that don't capture the full SBOM and component list; in these cases you document as much as you can, use conformity assessment to gain confidence in the others, and then set clear policies moving forward to document that information for future devices and products.”

Regulations invoking standards also provide an often-effective mechanism to impose cybersecurity requirements on supply chain providers. Regulations are key in certain industries to imposing such cybersecurity requirements. The rigor of regulations depends on the associated industry, scope of the regulation, and associated enforcement activities. NIST heard across panels that breaking interoperability in standards or regulations could hinder achieving cybersecurity goals.

Takeaway 5: The NIST outcome-based, product-level requirements approach is beneficial in providing guidance that is neither sector-specific nor standards-specific. Outcome-based requirements encourage flexibility for IoT innovation, based upon common security capabilities to meet consumer expectations and needs, and compliance with diverse legal and standards requirements.

There was consensus among the Panel 1 participants that the NIST outcome-based criteria were an effective means of providing clear yet flexible guidance that supports innovation while supporting mapping to more specific requirements to enable conformity assessment. Dave Kleidermacher, Google, explained that the NIST requirements are compatible with other requirements in standards from different standards bodies such as ISO and the European Telecommunications Standards Institute (ETSI). He also drew a parallel between the NIST outcome-oriented standards and the role played by Protection Profiles used in the Common Criteria; each define high-level outcomes that can be mapped to more specific standards to support conformance.

Karin Athanas, TIC Council, reported a similar shift in the conformity assessment space toward starting with outcome-oriented requirements, which provide a streamlined set of criteria that can be applied to multiple products. She noted it was clear that the NIST guidance is meant for other organizations to derive more detailed requirements programs, and said they serve as a useful baseline or benchmark. David Rogers, Copperhorse, noted that the UK had taken a similar approach with their code of practice and said he found the NIST approach very useful.

Amit Elazari, Intel, described the concept of outcome-based (or performance-based) requirements as a fundamental principle that can be found as a common theme in security policies. She pointed out that the pace of technology innovation means that attack surfaces, the cyber threat landscape, and the overall complexity of the technology ecosystem are constantly evolving, so it is valuable to have requirements that provide flexibility for the future. An example here was that the NIST criteria focus on authentication, whereas other post-Mirai guidance often focused on prohibiting default passwords; the more prescriptive approach could preclude moving on to preferable security solutions. She also saw this approach as useful in building trust with consumers.

Complementary to the outcome-oriented criteria, NIST's product-level approach allows for consideration of how all the different components work together to result in a holistic security outcome in various environments. This creates a challenge, though, because using a product-level approach for a diverse ecosystem requires follow-on work to define specific capabilities. David Rogers, Copperhorse, asked, "So how do manufacturers consider all those different options that consumers have and identify all the security parameters to protect the security for the products they are buying where [consumers] might be picking and choosing different things?" Various comments from the panel conveyed agreement that this "pick and choose" scenario is where guidance would be beneficial in addressing situations where components from different manufacturers, as well as for situations in which the same IoT products are used in different ways by the consumers (e.g., individuals, organizations).

Amit Elazari, Intel, pointed out the need to account for different security requirements for the same IoT products. She described how some products are used differently by different types of consumers in different environments. This is not just indicative of the need to be able to use multiple security standards to meet the outcomes; it is also for compliance with regulations and to promote use of the most appropriate protections for threats coming from the attack space. Amit stressed that it is important to recognize that technological innovation is always evolving, and so requirements must be adaptable and flexible to realistically be able to adopt and use for IoT products.

Takeaway 6: Reducing the OEM burden of conformity assessment across multiple markets depends on harmonization and mutual recognition of conformity assessment processes, as security requirements are generally converging.

David Kleidermacher, Google, pointed out that the need for harmonization among standards and requirements is being recognized and stated his belief that such harmonization will help to establish a common way of thinking about security requirements throughout different manufacturers. As an example, he pointed to the challenges that Google has faced in getting products approved under numerous different national conformance and monitoring regimes where they needed to do a great deal of repetitive work. He identified the challenge as dealing with the variety of conformance schemes and process rules, rather than a divergence of requirements. He stated that doing the work to satisfy multiple conformance regimes for a single product is not scalable, especially for smaller developers with limited resources.

Amit Elazari, Intel, described mutual recognition as being critical to enable third-party attestation of the security of IoT devices and products. She described requirements for IOT technical capabilities as largely mutual, but consensus regarding process-oriented and non-technical capability requirements as still emerging. Daniel Hein, Garmin, noted that a question he routinely must address is which IoT cybersecurity requirements are applicable to specific products in the company’s range of offerings. David Rogers, Copperhorse, noted that the community is seeing a consistent defragmentation of security standards, and that many are now well-aligned.

NIST understands that there is still work to be done in collaboration with industry, especially in the conformance space on adjoining outcomes and standards.

Takeaway 7: Mapping standards to a common set of cybersecurity outcomes is a useful tool for IoT product manufacturers, their supply chain providers, and conformity assessors.

NIST heard a need for harmonization and interoperability among cybersecurity and privacy standards and NIST guidance documents. There was discussion overall on how other standards apply to specific industries and to specific device types, and how NIST guidance, which is technology agnostic, would interplay.

Karin Athanas, TIC Council, indicated the way standards are laid out allows more effective grouping of security topics and allows more guidance to be provided for each of the topics. This allows others to take the standards and specify what the requirements should be, based upon the product to which they are going to apply. Such standards are then often used as the basis of technical regulations. Organizations can also use them to create their own programs, and to identify the standards to use for specific categories of technologies. Karin pointed out that, “Conformity assessments rely upon what is specifically listed in the standard. So, if a product [assessed against a specific standard] doesn't contain that, then it would not be certified. For conformity assessment, language is important. Compliance depends upon the language.” This makes it very important to ensure the standards used for conformity assessment include all the necessary language and are worded in a way to reach the intended outcomes.

NIST's Online Informative References (OLIR) Program [10] is a tool for this mapping, but the existence of a common set of cybersecurity outcomes is an important prerequisite to using the tool. While the NIST OLIR program is helpful for mapping standards to NIST guidelines, it could be enhanced to better incorporate standards at different levels of abstraction / detail. NIST encourages more engagement from organizations within specific sectors. Mapping through the NIST OLIR program or other industry standards to NIST guidance would help to determine what specific sector profiles outside of federal and consumer might look like.

Takeaway 8: There is growing acceptance of the need to include non-technical supporting criteria for IoT cybersecurity, but they are rarely addressed outside of NIST guidance.

Jasyn Voshell, Zebra Technologies, pointed out that it is not always information security's role to create non-technical requirements and that Zebra is generally focused on technical capabilities. He indicated that non-technical and process-oriented capabilities are still emerging with respect to consensus on what is needed.

There was also general agreement that most standards do not provide non-technical requirements as clearly, or cover them in depth, as compared to the technical requirements. A participant in chat stated "Design inputs come from [the] customer. Standards are developed to standardize how design inputs are met. These are at many levels. Non-technical requirements may not be in the standard itself."

Documentation, as non-technical security criteria, is valuable for multiple purposes such as product definition (e.g., describing use cases) and cybersecurity characteristics. However, when communicated by the OEM, documentation needs to be in a form that suits the needs of the intended audience (e.g., consumers vs. conformity assessors). For example, customers in enterprise environments may have requirements for understanding the full set of components within the IoT product, which may oblige an OEM to provide an inventory of the product's components. This was highlighted as a need by customers incorporating the IoT products within their business ecosystems.

There was concern expressed about how IoT products are used, and the risk level involved since IoT products could be shipped for one purpose and used for another. For example, a concern among manufacturers is this unintended use and how it relates to 'right to repair'. There was also discussion about the supply chain and how it interrelates to risk, namely information sharing and policy management, which are non-technical in nature. This was identified as an area that could be good to examine in more detail.

Takeaway 9: There is both support for cybersecurity labels for IoT products and recognition that "live labels" are necessary as a means for providing updated, current information about changes in IoT product cybersecurity status over time.

Labels are an important aspect of providing transparency and building customer trust with regard to cybersecurity. In Panel 1, all panelists seemed to agree that electronic "live labels" are an important tool for building consumer trust, using technology such as QR codes to connect to current information. Continued innovations for IoT products depend upon consumer trust and that trust can be gained by providing current information and transparency. For example, summaries about the security capabilities within such electronic labels that are kept updated would be useful in having additional up-to-date information available about security capabilities, risks, supply chain, vulnerabilities, and other issues related to each IoT product.

Panelists generally agreed that standards and certifications that are voluntary for OEMs can be effective. They also generally agreed that there must be incentives for IoT product manufacturers to comply with such standards and certifications

Takeaway 10: Manufacturers face a broad range of challenges in supporting products throughout their entire life cycle.

The ability to maintain life cycle support for deployed IoT products can be complicated by a broad range of factors such as supply chain difficulties, loss of support from associated third parties, supply chain vendors suddenly going out of business, IoT product components' end-of-life issues, and overall market forces. For example, the composition of a product might need to change due to originally selected components becoming unavailable, or due to a change in the interfaces to or availability of a cloud-based service used in the product.

Another life-cycle challenge is the use of IoT products in unanticipated ways. We heard from participants and panelists on different use cases and risks. One of the questions from a participant was "How are multiple [types] of intended uses/users dealt with?" An example provided was that of a medical device used in a hospital versus being used in a home, which could involve different users and create different risks within each of the environments. How these multiple types of users view the cybersecurity label and effect what goes into earning the cybersecurity label can be difficult to extract.

One non-technical supporting capability that has received more attention is the issue of end-of-life documentation. Manufacturers expressed a desire to better understand the consumers' need for receiving documentation about product end-of-life support, and to better understand how it impacts the consumers. Panel members generally indicated that documentation is essential. David Elfering, speaking as a consumer of IoT products, stressed how such documentation and transparency of IoT product components was necessary to enable him, as a large corporation CISO, to effectively manage cybersecurity risks throughout the full enterprise cybersecurity ecosystem where the IoT products were implemented. The participants generally agreed that the types of documentation needed would likely be different for different types of consumers (individuals and businesses), use cases, sectors, geographic locations, and for the ways in which the product will be used.

Takeaway 11: Conformity assessment requires clearly stated and specific requirements statements that enable the demonstration of compliance. Refining the NIST outcome-oriented criteria for particular IoT product types or market segments can provide these statements. This flexibility would allow for conformity assessments that enable the demonstration of compliance to applicable standards for specific IoT products.

Conformity assessments were discussed as transitioning to the full product, not just specific components. This is generally in agreement with why it is desirable to have standards and guidance that address the full scope of the product. In addition, manufacturers desire greater harmonization of conformity assessment across different markets to reduce their burden in presenting their products for assessment.

Panelists agreed that the wording within the guidelines, requirements, and standards is very critical, from both the certification/conformity assessor's point of view, as well as from a compliance point of view. The outcomes must be clearly communicated and understood to enable them to be consistently applied throughout all IoT product manufacturers. This will also ultimately support more consistent representation of the security requirements described on the consumer labels, to help reduce consumer confusion, and increase understanding of the associated security issues.

Karin Athanas, TIC Council**,** pointed out that IoT product requirements will also require smart, expanded testing to ensure the outcomes can be accomplished as described. Considering the full IoT product will require wider manufacturer testing, as well as conformity certification testing, for expected and unexpected outcomes.

Mike Bergman, Consumer Technology Association, indicated that the purpose of the NIST criteria is not for conformity assessment since that would need more specifics. "The NIST criteria establish the guidelines for the anchor to compliance, to which all the other standards are connected. From here then conformity programs and labeling programs can be built. There needs tracing/mapping to the NIST anchors. This is when accreditation can be established." And it is within those standards, and possibly other legal requirements, that the details for conformity assessors will be located.

Takeaway 12: Cybersecurity risk assessment for the full scope of IoT products continues to be a challenge for manufacturers.

There was discussion from some several panelists that risk is hard for humans to assess correctly, and that these challenges are particularly acute for IoT products. Risk assessments for IoT products are contextual, and often focused on end user and customer risks. There are complexities at scale, changing perspectives over time, newly discovered vulnerabilities, expanding types of threats, and different contexts that impact risk levels. There is not a single, or perhaps even a simple, solution to answering the question for how to consistently perform IoT product risk assessment since there are many ways to consider risk from different vantage points. Other complicating factors to keeping risk assessment results current are the realities that components will change over time. The introduction of new technologies, and scaling issues, increase and compound concerns.

There is also the consideration of business organization risk management. Managing IoT risks can be difficult and resource intensive and having IoT applications that are distributed and not contained within a data center increases the risks, and the associated risk mitigation challenges. A related challenge is the potential re-use of installed IoT for multiple parallel applications. An example provided by David Wollman, NIST, was that of smart cities. “There are IoT sensors that have multiple uses. You are building a measurement base for multiple purposes. And you want to reuse and [be] cost effective in that environment.”

Use cases have a place in helping to identify the best assessment of risk from the manufacturer to the end user. Daniel Hein, Garmin, echoed “It’s being cost effective with what's required. Getting hold of the appropriate people and what's acceptable here for use cases. And getting agreement.”

Another important risk issue that was mentioned was the topic of IoT product component interoperability, and right to repair. Beyond the intellectual property legal issues, there was discussion that in some cases the different components in an IoT product only talk by design, and some additional higher-level design would need to be created to allow IoT product consumers to swap components out. Different manufacturers are doing these processes in different proprietary ways. These issues create a situation where not all IoT products are as interoperable as customers might currently need.

3. Next Steps

The workshop resulted in numerous topics where additional actions can be taken. The NIST Cybersecurity for IoT program discussed and identified six next steps based on what they heard in the workshop as being the most beneficial to address in the near term. These are not shown in any priority order. They are enumerated to allow for easier reference.

a) **Finalize the consumer profile in NIST IR 8425.** A final version of the consumer profile is needed to guide OEMs in product development and enable conformity organizations to prepare conformance assessment requirements.

b) **Provide updated guidance on developing profiles**. The Cybersecurity for IoT program has been making updates to the profiling process since publishing the federal and consumer profiles. Those updates should be made available by completing the existing draft publication *NIST IR 8259C, Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*. [11]

c) **Review mappings to standards.** The program continues to examine mappings of other standards and cybersecurity guidance, and encourage new mappings, to existing NIST cybersecurity guidance. NIST engaged in a landscape review of available standards during the development of the consumer profile and continues to determine and document the alignment of relevant standards. This process helps to consider how requirements can be instantiated to meet the specific needs of the communities represented by the standards and guidance.

d) **Evaluate the ways in which risk management including associated risk assessments can consider the complexities of risk throughout the IoT product life cycle.** The workshop reinforced the importance of risk management throughout the IoT product life cycle, including examining downstream supply chain risks through third parties and owners. Addressing IoT product end-of-life/support issues were also identified as important risk concerns. Examining use cases could identify points of alignment between risk mitigation approaches and technical and non-technical capabilities to assist manufacturers in secure development of IoT products.

e) **Identify methods for supporting transparency throughout the full IoT product supply chain**. Use of SBOMs can help to support transparency and documentation. The use of binary analysis may also support such transparency. Expanded oversight from manufacturers of their supply chain vendors and application of more explicit security requirements to those vendors would also raise awareness of component security capabilities and vulnerabilities.

f) **Examine additional routes to engage stakeholders with evolving NIST Cybersecurity for IoT guidance.** As NIST continues to make progress on areas of importance to stakeholders, the program is considering additional outreach and collaboration options. This may include blog posts, white papers, or discussion drafts, in addition to updated NIST guidance on topics of importance.

References

[1] National Institute of Standards and Technology (2022) Building on the NIST Foundations: Next Steps in IoT Cybersecurity. Available at: https://www.nist.gov/news-events/events/2022/06/building-nist-foundations-next-steps-iot-cybersecurity

[2] National Institute of Standards and Technology (2022) Cybersecurity for the Internet of Things (IoT). Available at https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

[3] Executive Order 14028 (2021) Improving the Nation's Cybersecurity. (The White House, Washington, DC), DCPD-201300091, May 12, 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[4] National Institute of Standards and Technology (2022) Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 24. https://doi.org/10.6028/NIST.CSWP.24

[5] Fagan MJ, Megas K, Watrobski P, Marron JA, Cuthill BB (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425 ipd, Initial Public Draft. https://doi.org/10.6028/NIST.IR.8425.ipd

[6] National Institute of Standards and Technology (2022) Ideas for the Future of IoT Cybersecurity at NIST: IoT Risk Identification Complexity (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/document/iot-paper-ideas-future-iot-cybersecurity-nist-iot-risk-identification-complexity

[7] 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) NIST IR 8259. https://doi.org/10.6028/NIST.IR.8259

[8] 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) NIST IR 8259A. https://doi.org/10.6028/NIST.IR.8259A

[9] 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) NIST IR 8259B. https://doi.org/10.6028/NIST.IR.8259B

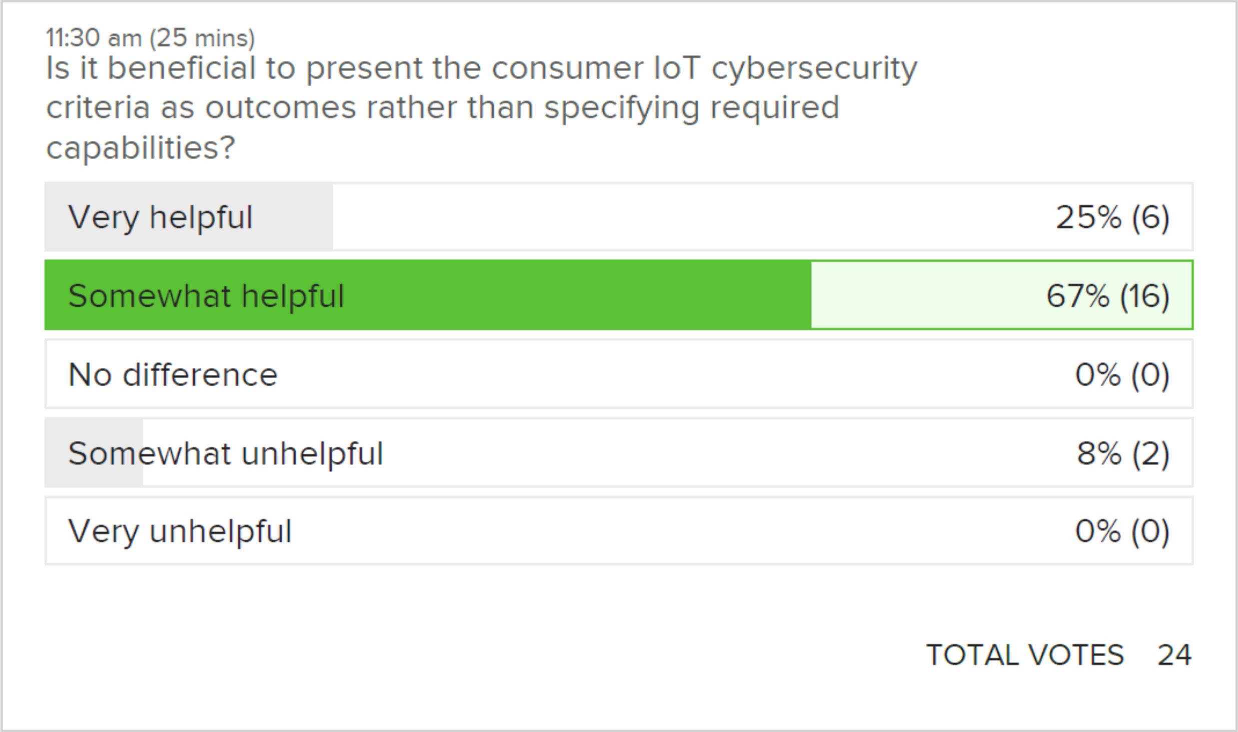
[10] National Institute of Standards and Technology (2022) National Online Informative References Program. Available at https://csrc.nist.gov/projects/olir

[11] Fagan MJ, Marron JA, Brady KG, Jr., Cuthill BB, Megas K, Herold R (2021) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8259C, Draft. https://doi.org/10.6028/NIST.IR.8259C-draft

Appendix A. Poll Results

Seven online polls were conducted during the workshop. The polls gathered participant viewpoints on a variety of topics related to the challenges of cybersecurity for IoT devices. Poll questions and results are provided below. Since workshop survey group participants and poll responses were entirely voluntary, poll results should not be viewed as providing statistically valid sample size results. Note that shading the boxes below is intended to visually depict the percentage for that answer.

A.1. Value of Stating Criteria as Outcomes

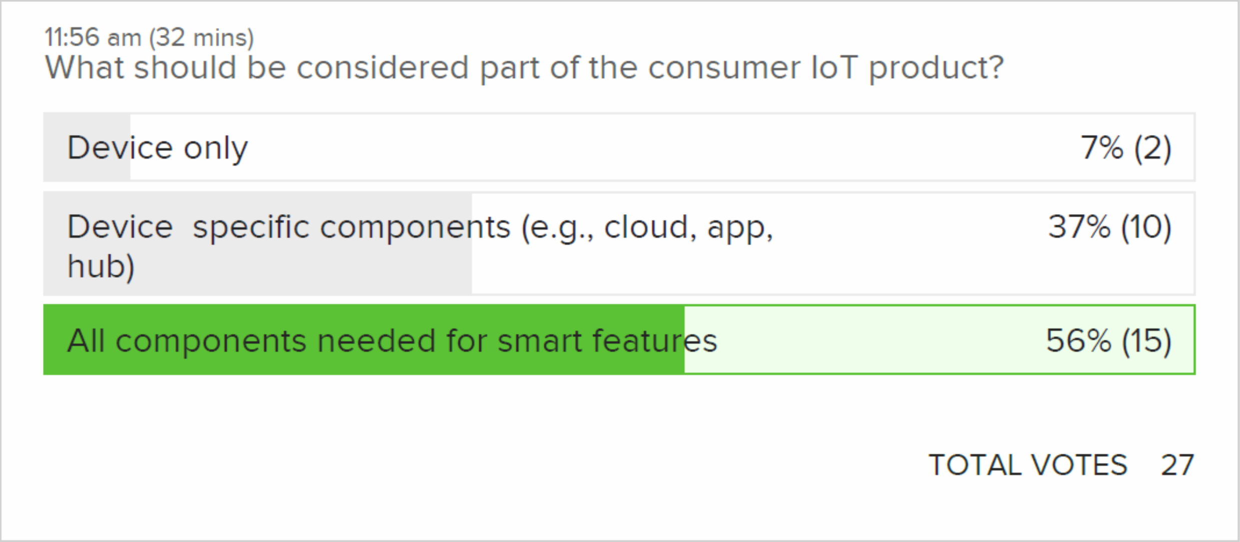


11:30 am (25 mins)
Is it beneficial to present the consumer IoT cybersecurity criteria as outcomes rather than specifying required capabilities?

Very helpful	25% (6)
Somewhat helpful	67% (16)
No difference	0% (0)
Somewhat unhelpful	8% (2)
Very unhelpful	0% (0)

TOTAL VOTES 24

A.2. Scope of Consumer IoT Product



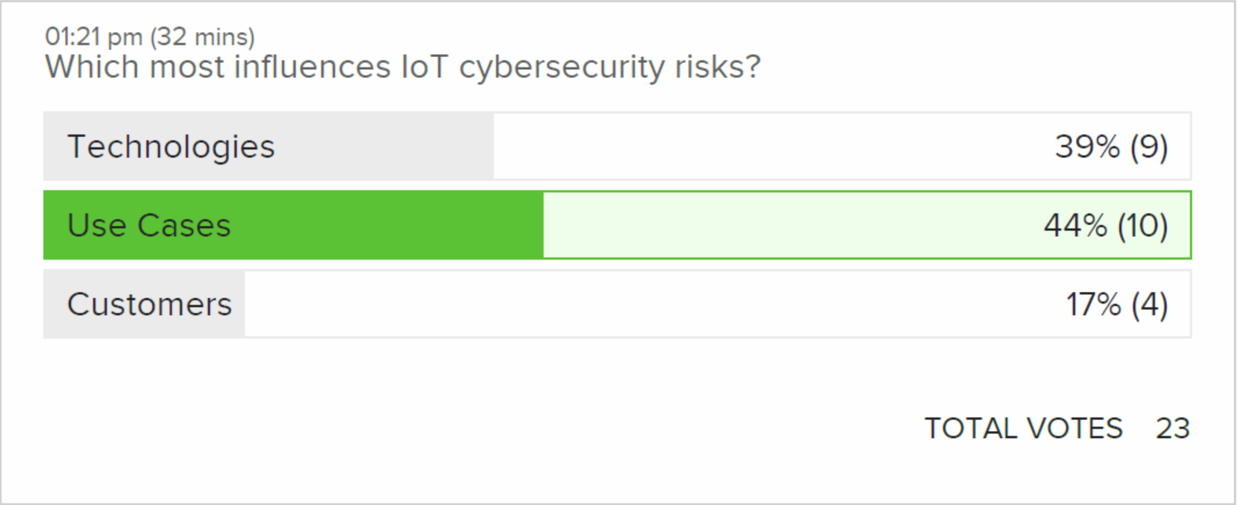
11:56 am (32 mins)

What should be considered part of the consumer IoT product?

Device only	7% (2)
Device specific components (e.g., cloud, app, hub)	37% (10)
All components needed for smart features	56% (15)

TOTAL VOTES 27

A.3. Influences of IoT Cybersecurity Risks



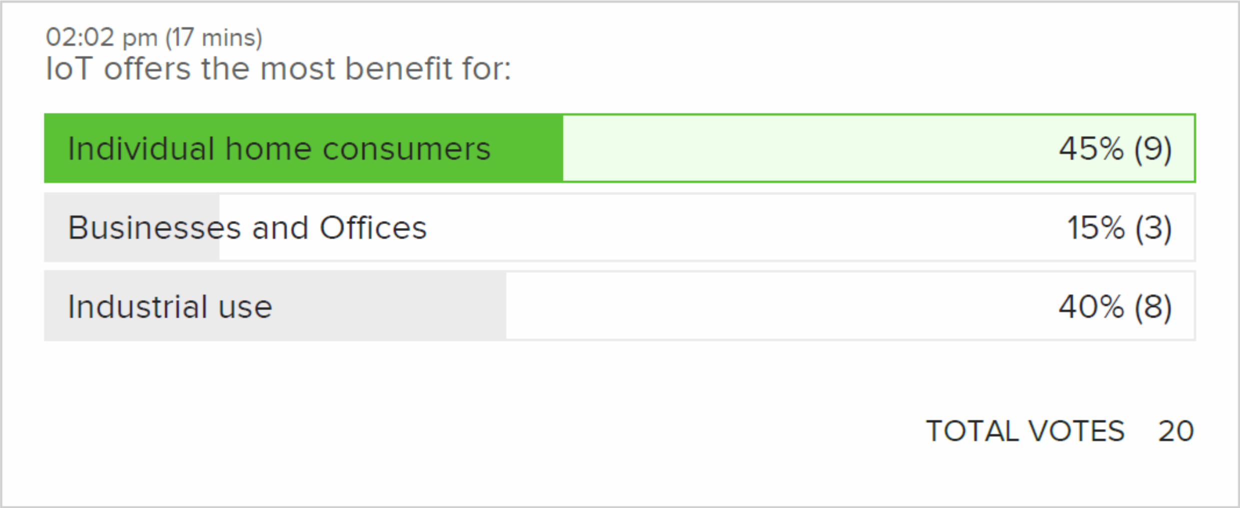
01:21 pm (32 mins)

Which most influences IoT cybersecurity risks?

Technologies	39% (9)
Use Cases	44% (10)
Customers	17% (4)

TOTAL VOTES 23

A.4. Beneficiaries of IoT

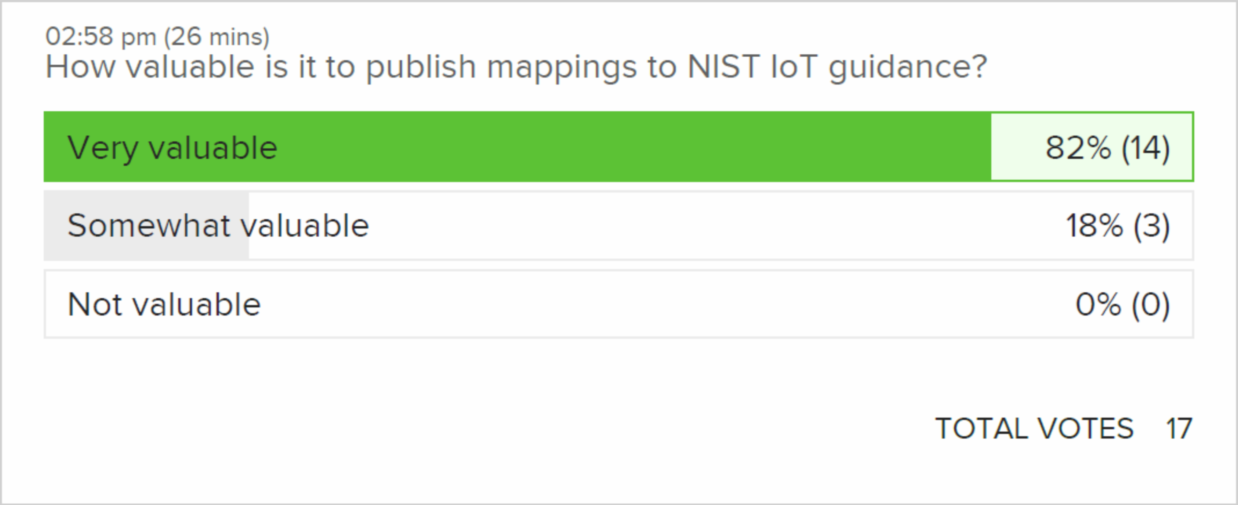


02:02 pm (17 mins)
IoT offers the most benefit for:

Individual home consumers	45% (9)
Businesses and Offices	15% (3)
Industrial use	40% (8)

TOTAL VOTES 20

A.5. Value of Mappings to NIST IoT Guidance

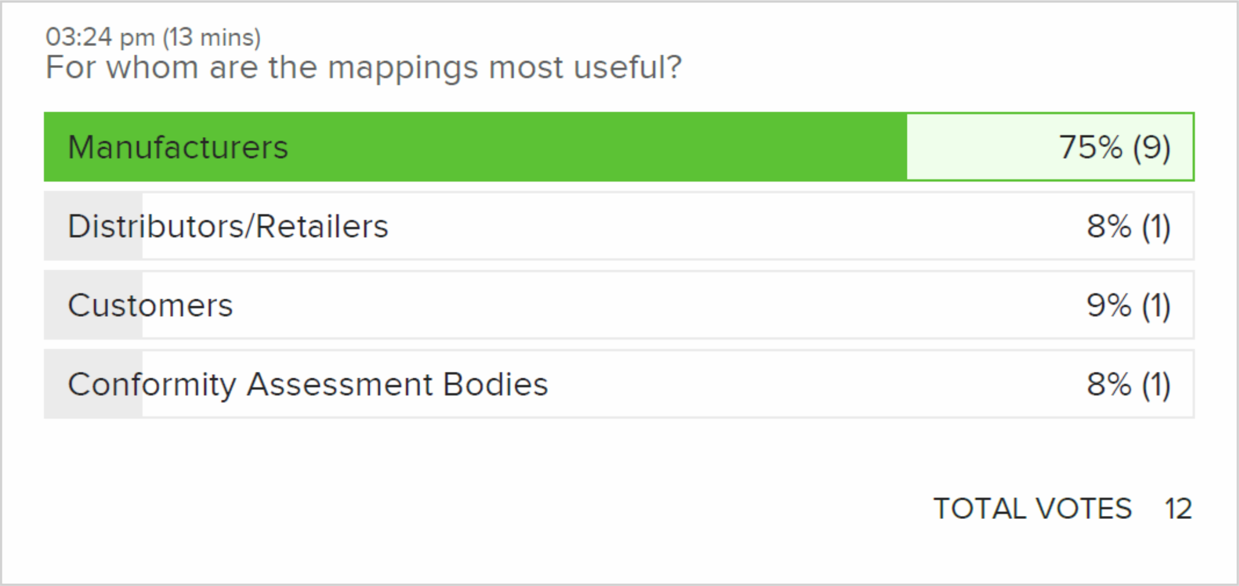


02:58 pm (26 mins)
How valuable is it to publish mappings to NIST IoT guidance?

Very valuable	82% (14)
Somewhat valuable	18% (3)
Not valuable	0% (0)

TOTAL VOTES 17

A.6. Greatest Benefit From Mappings

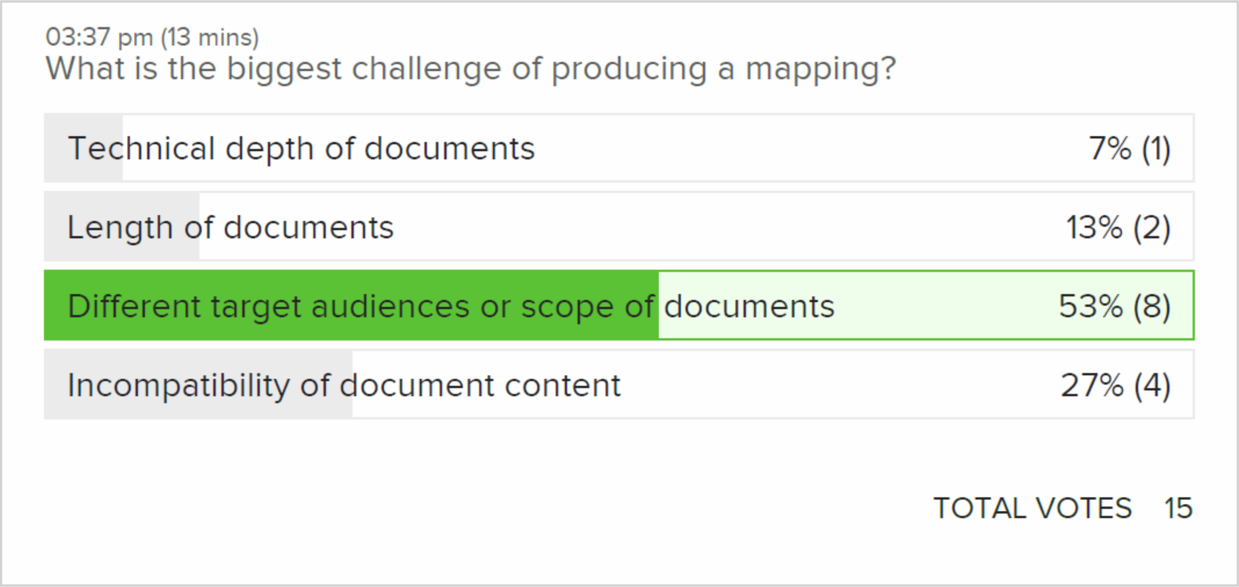


03:24 pm (13 mins)
For whom are the mappings most useful?

Manufacturers	75% (9)
Distributors/Retailers	8% (1)
Customers	9% (1)
Conformity Assessment Bodies	8% (1)

TOTAL VOTES 12

A.7. Biggest Challenge In Producing Mapping



03:37 pm (13 mins)
What is the biggest challenge of producing a mapping?

Technical depth of documents	7% (1)
Length of documents	13% (2)
Different target audiences or scope of documents	53% (8)
Incompatibility of document content	27% (4)

TOTAL VOTES 15

Appendix B. List of Symbols, Abbreviations, and Acronyms

AI
Artificial Intelligence

ALM/PLM
Application Life cycle Management / Product Lifecycle Management

CISO
Chief Information Security Officer

CPSO
Chief Product Security Officer

EO
Executive Order

ETSI
European Telecommunications Standards Institute

IoT
Internet of Things

ISO
International Organization for Standardization

NIST IR
NIST Interagency or Internal Report

OEM
Original Equipment Manufacturer

OLIR
On-Line Informative Reference

OWASP
Open Web Application Security Project

R&D
Research & Development

SAMM
Software Assurance Maturity Model

SBOM
Software Bill of Material

SDLC
System Development Life Cycle

SLA
Service Level Agreement

SMOS
Service Model Operating System