NISTIR 8379

Summary Report for the Virtual Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance

Katerina N. Megas
Michael Fagan
David Lemire

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8379

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8379

Summary Report for the Virtual Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance

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

David Lemire
Huntington Ingalls Industries
Annapolis Junction, MD

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8379

September 2021

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

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8379
27 pages (September 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8379

Comments on this publication may be submitted to:

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

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 (IT). 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.

Abstract

This report summarizes the feedback received on the work of the NIST Cybersecurity for IoT program on device cybersecurity at a virtual workshop conducted April 22, 2021. NIST conducted the "*Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance*" to discuss and gather community input on the December 2020 public drafts of NISTIR 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*, and SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. This publication provides a summary of the workshop.

Keywords

Cybersecurity baseline; Internet of Things (IoT); securable computing devices; security requirements; Risk Management Framework; federal profile.

Acknowledgments

The authors wish to thank all contributors to this publication, including the participants in workshops and other interactive sessions; the individuals and organizations from the public and private sectors, including manufacturers from various sectors as well as several manufacturer trade organizations, who provided feedback on the preliminary public content and colleagues at NIST who offered invaluable inputs and feedback.

Audience

The main audiences for this publication are IoT device manufacturers and federal agencies procuring IoT devices. This publication may also help IoT device customers or integrators, particularly those that work in or with the federal government.

Table of Contents

1 Introduction

On April 22, 2021, the National Institute of Standards and Technology (NIST) conducted a virtual workshop entitled *Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance*. The event included stakeholders from across industry, academia, and government. The goal was to discuss feedback NIST had received on two draft documents:

- NIST Special Publication (SP) 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* [SP800-213]
- NIST Interagency Report (NISTIR) 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* [NISTIR 8259D]

Both drafts were published in December 2020, with a public comment period extending through February 26, 2021. Over 230 people participated from the U.S. and nine other countries, representing a broad mix of industry, academia, and government..

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 [3] is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools developed in collaboration with stakeholders across government, industry, international bodies, and academia[1]. The NIST 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.

1.2 Background

In December 2020 NIST published public drafts of four IoT cybersecurity documents:

- NIST SP 800-213, *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*
- NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline* [NISTIR8259B]
- NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline* [NISTIR8259C]
- NISTIR 8259D, *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*

These documents build on the previously published NISTIR 8259, *Recommendations for IoT Device Manufacturers: Foundational Activities* [NISTIR8259], and NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* [NISTIR 8259A], to define a federal profile for IoT device cybersecurity that encompasses both technical abilities and non-technical supporting

[1] "NIST Cybersecurity for IoT Program" website available at https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

capabilities required from IoT devices and their manufacturers, respectively, as well as associated documentation to round out the guidance provided by the program. The documents are complemented by an online catalog [CATALOG] of detailed technical capabilities and supporting non-technical capabilities, updates that were published in March of 2021.

The Internet of Things Cybersecurity Improvement Act of 2020[2] became law in December 2020. The law directs NIST to publish "standards and guidelines for the Federal Government on the appropriate use and management by agencies of Internet of Things devices owned or controlled by an agency and connected to information systems owned or controlled by an agency, including minimum information security requirements for managing cybersecurity risks associated with such devices." The NISTIR 8259 series and SP 800-213 represent a significant portion of NIST's activities to address the requirements of the Act.

After the draft documents were published, NIST began a series of stakeholder engagement activities. The April 2021 workshop was an open event to engage stakeholders in focused discussions on two of the draft documents: NIST SP 800-213 and NISTIR 8259D, which are the core documents defining federal requirements and processes for IoT device cybersecurity.

1.3 About the Workshop Addressing Public Comment on NIST Cybersecurity for IoT Guidance

The free, publicly available virtual workshop consisted of a mixture of plenary and breakout sessions[3]. The agenda is provided in Table 1. The workshop included a keynote presentation from the U.S. Government Accountability Office (GAO) describing their survey of federal use of IoT technology and an overview from the NIST Cybersecurity for IoT Program's technical lead on potential responses to the comments NIST has received. These sessions were followed by breakout discussions on various aspects of NIST's proposed approach to revising the documents. The plenary sessions resumed with an overview of NIST's Online Informative References (OLIR) Program, followed by a summation of the breakout sessions provided by their facilitators and closing remarks from the NIST program manager.

This workshop focused on discussing themes raised in the comments submitted on the two subject documents, some of which will have implications across the entire set of documents. The goal of the workshop was to improve the documents to reflect federal government needs and stakeholder concerns. NIST sought to get additional input from stakeholders through the facilitated breakout discussions, bringing together different points of view around key topics that involved audience participation and questions.

[2] https://www.congress.gov/bill/116th-congress/house-bill/1668/text

[3] Recordings of the plenary sessions can be accessed at: https://www.nist.gov/news-events/events/2021/04/workshop-addressing-public-comment-nist-cybersecurity-iot-guidance

NIST sought attendance from those involved in federal IoT cybersecurity, the manufacturers of IoT devices, researchers in related fields, and other stakeholders. NIST encouraged participants to become familiar with the draft documents prior to the workshop.

The workshop drew approximately 230 participants, panelists, speakers, and moderators. This included representatives from:

- A mixture of industry, academia, and government, as well as independent researchers;
- Seventeen federal government organizations including civil government, defense, and intelligence; and
- Nine countries.

Table 1 – Agenda for the IoT Federal Profile Virtual Workshop

Time	Activity and Presenters
10:00 am	Welcome and introduction: Kat Megas, Program Manager, NIST Cybersecurity for IoT Program
10:15 am	Keynote: "Federal Use of IoT: Insights into a Government-wide survey and Case Studies" – Eric Hudson and Steve Rabinowitz, GAO
10:45 am	Overview of comment themes and paths forward for the documents – Michael Fagan, NIST
11:30 am	Breakout 1: Risk-Based Approach: Assessing IoT Device Risk and Mitigation Approaches
1:00 pm	Breakout 2: No One Size Fits All: Accounting for Device Architecture in applying the Federal Profile
2:00 pm	Breakout 3: Ecosystem View: Mitigating Risks and Reducing Fragmentation Through Ecosystem Cybersecurity
3:00 pm	NIST Online Informative Reference (OLIR) Program and Call for Informative References (Kevin Brady, NIST)
3:30 pm	Facilitator panel and discussion
3:50 pm	Conclusion (Kat Megas)

Videos of the workshop plenary sessions are available on the event web page.[4] 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.

[4] https://www.nist.gov/news-events/events/2021/04/workshop-addressing-public-comment-nist-cybersecurity-iot-guidance

2 Event Summary and Key Takeaways

The summary below highlights significant points from the plenary presentations and identifies the discussion topics and NIST's takeaways and observations from the three breakout sessions.

2.1 Plenary Sessions

This section provides an overview of the presentations and discussions during the workshop plenary sessions.

2.1.1 Introduction: NIST Cybersecurity for IoT Program Manager

Katerina Megas, the program manager for the NIST Cybersecurity for the IoT Program, gave a brief introductory presentation. She thanked participants for attending, provided a summary of the agenda, and presented information on the NIST Cybersecurity for IoT Program. Ms. Megas reviewed the goals of the program and five principles that guide its execution. She emphasized the importance of risk management in NIST's approach to IoT cybersecurity guidance, describing the view of the risk management hierarchy from enterprise down to systems, and then extending on to IoT devices that are components of federal information systems. Ms. Megas also pointed out that NIST guidance needn't have "IoT" in the title to be applicable to IoT cybersecurity, noting that the NIST security controls contained in SP 800-53, and other guidance documents that address zero-trust architecture and supply chain security, among other topics, are also relevant and useful. She concluded by reminding participants that the workshop discussions were focused on cybersecurity for federal information systems, which guided the selection of topics in the agenda.

2.1.2 Keynote: GAO Survey of Federal IoT Use

The keynote presentation was made by Eric Hudson and Steve Rabinowitz of the GAO, based on a GAO report titled *Internet of Things: Information on Use by Federal Agencies* [GAO20-577]. Mr. Hudson is a senior analyst with GAO's physical infrastructure team. Mr. Rabinowitz is also a senior analyst at GAO and has participated in a number of infrastructure-related studies. Their presentation had three components:

- Mr. Hudson presented background information on the GAO and conduct of the study that was the basis for the report;
- Mr. Rabinowitz reviewed the survey results from the study; and
- Mr. Hudson described several interesting use cases that were explored in greater depth.

Mr. Hudson described the GAO's role as a non-partisan agency of Congress that does most of its study work on behalf of Congressional committees. He noted that the study they were presenting was performed at the request of four Senators. He described the focus of the study as being to identify the nature of federal agency use of IoT technology, review the benefits and challenges that agencies had experienced with the technology, and understand government-wide policies and agency-specific policies and guidance that inform their use of IoT and associated decision making. Mr. Hudson said the GAO combined a survey with four case studies to gain deeper insights, selecting the case studies based on a combination of agency information technology

budgets, agency missions, and the specific use cases available. The use cases selected came from the Departments of Commerce (DOC) and Homeland Security (DHS), the Environmental Protection Agency (EPA), and the National Aeronautics and Space Administration (NASA). He said the GAO met with department-level and sub-agency staff and program management staff. The GAO also reached out to other agencies based on the survey results. He noted that the GAO used a specific definition of IoT to clarify the scope of their study with the agencies surveyed:

> The Internet of Things (IoT) generally refers to the technologies and devices that allow for the network connection and interaction of a wide array of devices, or "things", throughout such places as buildings, vehicles, transportation infrastructure or homes. [GAO20-77]

Mr. Rabinowitz then presented the results of the survey, which he described as a "shallow look" at how the federal government is using IoT technology, while providing a useful look at the extent of IoT use and the high-level benefits and challenges. He noted that the study excluded common IT products as well as smart devices that weren't connected to an agency network, and he indicated that the types of IoT addressed by the survey included control or monitoring devices such as smart heating, ventilation and air conditioning (HVAC) and sensors that collect environmental data, fire suppression systems with IoT sensors, and network-connected telemetry devices (e.g., cameras). He explained that the survey was targeted to subcomponents of agencies and was sent to 115 federal entities that had been identified through their membership in the Federal Chief Information Officer (CIO) Council, with the survey addressed to the component's CIO or senior IT executive.

Regarding the extent of use and plans for use of IoT, the survey results were that:

- 56 of 90 agencies were using IoT, especially to control or monitor systems, control access to facilities, and track physical assets (vehicles, property).
- 25 agencies were currently using IoT and planned to expand their use.
- 13 agencies were neither using nor planning to use IoT, based on lack of return on investment, internal administrative hurdles, or the lack of a business case.

GAO's survey results about the nature of IoT technology use indicated that 50 agencies were using commercial off-the-shelf products, while 17 were using more specialized, "home-grown" devices. An example of the latter was NASA's use of custom IoT for monitoring space suits.

The benefits that agencies reported from their use of IoT included improved data collection, improved efficiency, increased productivity, and overall automation. Mr. Rabinowitz provided some examples:

- Improved data collection: The EPA deployed IoT sensors at a factory fire in New Jersey to monitor the dispersal of chlorine gas, gaining a "real-time picture" that helped in coordinating the response effort.
- Improved efficiency: The National Oceanic and Atmospheric Administration (NOAA) used IoT to deploy unmanned systems (aircraft, watercraft, buoys) that wouldn't

otherwise have been deployed without manning, enabling them to gather significant additional oceanographic and atmospheric data to support research.
- Improved productivity: DHS Customs and Border Patrol (CBP) used IoT to process vehicles faster at ports of entry, improving their ability to identify threats and take action.

The two most common challenges identified by agencies using IoT were cybersecurity and interoperability with legacy systems. Many off-the-shelf IoT solutions of potential interest to federal agencies weren't created with a federal or enterprise customer in mind. Such products, oriented toward the consumer or industrial markets, often lack the security capabilities needed in the federal environment. Interoperability with legacy systems was also cited as a challenge, particularly at some organizations with a significant installed base of older systems.

Another dimension of the survey was policy guidance for the use of IoT. Over half of the agencies surveyed used general information technology (IT) policies, finding them sufficient to guide IoT acquisition and use. A mixture of government-wide and agency-specific IT policies were used. A smaller percentage of agencies (slightly more than 25 %) developed IoT-specific policies, and survey respondents were about equally divided on whether current IT security policy guidance needs to be supplemented with IoT-specific guidance.

Mr. Hudson presented several IoT use cases that GAO found particularly interesting:

- The EPA used environmental buoys to monitor water quality in Boston's Charles River, measuring pH, temperature, and other variables. This provides a very efficient means to collect the data, and the real-time information enables quick reaction if some incident (e.g., a chemical spill) were detected.
- The St. Lawrence Seaway Development Corporation deployed a hands-free mooring system for two locks they operate along the seaway, working with a Canadian partner that manages other locks. The pads use a vacuum system to moor the ship, providing a very efficient and safe means to move ships through the locks faster than using manual mooring methods.
- The DHS has developed customer IoT automated surveillance towers to monitor the southwest borders of the U.S. The towers provide data that can be analyzed to detect border incursions and trigger the deployment of agents if needed. This provides greater efficiency in use of human resources.
- NASA has developed specialized IoT for monitoring rockets and astronauts in space suits. This gives NASA access to data that are not otherwise observable during launches.

Mr. Hudson identified two of the NIST program principles — no one-size-fits-all and risk-based understanding — that resonated with the GAO survey results. The mission and associated data for various IoT applications aligned closely with the cybersecurity concerns. Relevant examples here are the environmental data collected by EPA compared with more sensitive personal data collected by CBP at border crossings. Agencies that developed their own IoT had greater control over the cybersecurity characteristics compared to when off-the-shelf technology was used.

2.1.3 Groundwork: Overview of Comment Themes and Paths Forward for the Documents

Michael Fagan, the technical lead of the NIST Cybersecurity for IoT Program, provided an overview of themes NIST identified in the comments received on the December 2020 draft documents. He also presented concepts for how to address some of those themes in future versions, with the intent of setting the stage for the breakout session discussions. He began by briefly reviewing the documents the program has published to-date, describing NISTIRs 8259 and 8259A as defining fundamental security for IoT devices, phrased at a high level and defining outcomes broadly applicable to a wide range of use cases. He stated that one of the goals of the workshop and subsequent work was to explore the range of applications of that foundational guidance. He briefly reviewed the set of documents published in December 2020, and he highlighted the workshop's focus on the federal government customer-oriented documents (draft NISTIR 8259D and SP 800-213) and the online catalogs of detailed capabilities.

Mr. Fagan briefly reviewed how IoT devices as system elements (i.e., components) support the broader system security requirements and expectations of the owning organizations, where a device provides technical and non-technical cybersecurity capabilities that support the larger system security requirements. He then summarized the use of the Risk Management Framework (RMF) Low Impact baseline as the basis for defining the security capabilities identified for IoT devices in the federal profile, and he noted that NIST viewed the profile as a starting point that federal agencies could tailor if needed to address unique requirements.

Mr. Fagan then summarized the feedback NIST has received through formal comments and discussions with stakeholders. Key points were:

- A need for greater clarity on the positioning of NISTIR 8259D and NIST SP 800-213, how they interrelate and how they relate to other NIST work and associated industry standards.
- Concerns that the requirements in NISTIR 8259D cannot be supported by many IoT devices, especially technically constrained IoT devices.
- Concerns regarding the potential for fragmented requirements and policies based on the documents.
- A need to distinguish different classes or types of IoT devices to guide the tailoring of requirements and reduce the potential for fragmentation.

Mr. Fagan explained that the federal profile was a starting point and was based on a number of assumptions regarding the IoT devices it covered. In particular, the devices were assumed to be general purpose (e.g., low criticality) IoT devices that are fully-connected, fully-featured devices. He noted that this assumption of connectivity would not apply to all devices, such as those that connect to a hub for their interface to the larger network. Mr. Fagan described variations of capabilities that could be provided by IoT devices based on their inherent hardware limitations and reviewed other areas of variability that might apply to particular devices. He stated that the profile would be tailored by federal agencies based on risk, with NIST intending to provide guidance regarding tailoring.

Mr. Fagan then presented the RMF perspective positioning an IoT device as a system element in a federal information system and described the need to take a system view to fully grasp an IoT device's potential impact on system risk. He explained that introducing an IoT device or adding an Internet connection to support a device's operations may bring new mission or safety risks that in turn require additional security controls (e.g., if an IoT device is deployed in place of an operational technology [OT] device that wasn't Internet-connected). He highlighted various aspects of IoT device implementation (e.g., processing capability, power limitations, connectivity patterns) that can influence the device's impact on the system's security risks. He then walked through the steps of a risk assessment, as defined in the RMF, and some associated IoT device considerations that can apply at each step of the process.

Mr. Fagan continued by introducing the notion of "risk descriptors" that can be used to relate IoT device risk considerations to how an IoT device is designed and used. The risk descriptors he presented were broken into three groups:

- "Device Use" descriptors related to the context in which an IoT device is used; he noted that the NISTIR 8259D profile assumed a "non-critical" device.
- "Device Architecture" descriptors related to the architecture of the IoT device, based on Internet Engineering Task Force (IETF) RFC 7228; the NISTIR 8259D profile assumes a microcomputer-based device.
- "System Relationship" descriptors related the IoT device's relationship with the remainder of the system; he noted that the NISTIR 8259D profile assumed a "peer" relationship.

The full definitions of the risk descriptors presented during the workshop can be found in Appendix A, Descriptor Definitions.

Mr. Fagan presented a diagram to illustrate the "IoT Device – System Relationship" descriptors, highlighting how descriptors would be applied to devices in a notional deployment scenario. He then briefly introduced three example use cases to be used to focus discussion during the workshop's breakout sessions:

- Smart Door Lock: Federal organizations may utilize connected door locks that can scan PIV cards and manage access to and within facilities.
- Unmanned Aircraft System (UAS): Federal organizations could use UAS to inspect facilities as part of monitoring and maintenance of the facility.
- Water Sensors: Some federal organizations may use connected IoT environment sensors to monitor various aspects of facilities.

Mr. Fagan concluded by briefly reviewing updates to the online IoT device cybersecurity capabilities catalog and encouraging workshop participants to provide input and feedback on the catalog's contents and utility.

2.1.4 Online Informative Reference Program

After the breakout sessions, Mr. Kevin Brady of the NIST Cybersecurity for IoT Program team provided an overview of the NIST Online Informative References (OLIR) program [OLIR]. He described OLIR's purpose as providing a centralized location to find, display, and update linkages between a NIST document and those from external sources. OLIR assists subject matter experts (SMEs) in defining and capturing linkages and allows efficient reviewing and updating of the linkages. He explained that NIST introduced informative references (IRs) in the Cybersecurity Framework (CSF) [CSF].

The OLIR database provides a centralized location for capturing and describing IRs that can be accessed by anyone. OLIR is public, providing transparency, and defines a consistent manner for describing relationships, which assists with harmonizing the references between documents and improving clarity and consistency. The OLIR approach also provides the opportunity to apply automation for ingesting and utilizing IRs.

Mr. Brady explained that OLIR applies set theory concepts for defining relationships as a mechanism to reduce subjectivity and retains the identity of the SME that defined each relationship. The program, defined in NISTIRs 8278 [NISTIR8278] and 8278A [NISTIR8278A], has a standardized process for submitting OLIRs to be added to the database. He noted that documentation of an IR in OLIR does not demonstrate certification or compliance to the NIST document in question.

Mr. Brady explained the terminology OLIR uses to describe documents. In OLIR, a "focal document" is a NIST document (e.g., an SP or NISTIR) that is the basis for the document comparison; and the "reference document" is an external document being compared to the focal document. The comparisons are formulated between "document elements" (e.g., discretely identifiable pieces of content) and the "reference documents" here could also be products, services or training materials.

Mr. Brady listed the five possible relationship types that OLIR recognizes, which are subset, intersection, equal, superset, and not related, and provided an illustrative diagram. He also listed the possible relationship rationales – syntactic, semantic, and functional – and provided examples from NISTIR 8278. He noted that an IR should be described with the most specific rationale option.

Mr. Brady explained the concept of reference data and described what data are kept in OLIR versus what data can be inferred. Tier 1 mapping data are stored in OLIR and may be submitted by the reference document owner or by some other party. Tier 2 mappings are derived based on relationships to focal documents from multiple reference documents, enabling a form of indirect mapping.

Finally, Mr. Brady explained the life-cycle of an OLIR submission. For OLIR, an initial IR submission is posted in a draft state, screened by NIST, and then published for a 30-day public review period. During the review period, anyone can submit feedback, and the submitter can respond to that feedback and update the mapping. After 30 days, the submission's status is

changed to final; however, maintenance is allowed to keep the IRs up-to-date. The IR will be archived when it is no longer relevant (e.g., because a document is withdrawn or deprecated). He noted the availability of a focal document template on the OLIR site as well as the template for submission of a reference document.

Links to the relevant NISTIRs and the OLIR program website are provided in the references.

2.1.5 Facilitator Panel Discussion & Wrap-Up

Ms. Megas moderated a panel discussion with the four breakout room facilitators to provide an initial summary of the information collected in each of the three breakout sessions. Those breakout sessions are summarized in Section 2.2 of this report, but the facilitator panel content is not summarized here since it would duplicate the material presented about the breakout sessions in Section 2.2.

Finally, Ms. Megas provided a brief wrap-up focused on next steps for the NIST Cybersecurity for IoT Program. She thanked the facilitators, participants, and NIST conference services for their contributions to the event. Ms. Megas stated the team would process the feedback received from the workshop, the public comment period, and stakeholder conversations held since the comment period ended. She pointed to a workshop poll result suggesting that GitHub could be a useful tool for asynchronous interactions between the NIST program and the stakeholder community. She stated that the program intended to publish another round of documentation, likely second public drafts, of the new material by late summer. Ms. Megas also announced the plan for a set of roundtables to discuss NISTIR 8259B in June 2021. She said the program had heard feedback about linking the program's NISTIR 8259A guidance to other NIST projects and was evaluating how the guidance could be connected, perhaps via a mapping, to projects in the NCCoE. She also mentioned that a NISTIR summarizing the October 2020 workshop on Cybersecurity Risks in Consumer IoT [NISTIR 8333] had been published. She announced the impending publication of a paper on potential confidence mechanisms for IoT cybersecurity and requested feedback on that paper.

2.2 Summary and Takeaways from Breakout Session Discussions

These takeaways discussed below are ideas that NIST heard from participants and that received significant, but not necessarily unanimous, support from attendees and/or panelists. While this document seeks to be thorough in reflecting the workshop discussions, a summary document cannot capture all the thoughts, opinions, and suggestions provided during the sessions. The topics, takeaways, and observations in this report do not represent specific NIST recommendations or guidance but are intended to capture and summarize discussions from the workshop and viewpoints expressed by panelists and participants. These takeaways provide important feedback to the program and a basis for future conversations with the community.

There were four concurrent breakout "rooms" during each of the breakout sessions. The takeaways reflect thoughts in multiple but not necessarily all rooms during a particular session. The takeaways are not separated by room.

2.2.1 Breakout 1: Risk Descriptors

The first breakout session was titled "Risk-Based Approach: Assessing IoT Device Risk and Mitigation Approaches" and focused on discussion of the "device use risk" descriptors presented during Mr. Fagan's presentation (See Appendix A for the definitions).

The stated objective for this breakout session was to obtain feedback on the utility of the proposed risk descriptors for:

- Selection of additional needed system controls and IoT capabilities (Note that additional controls/capabilities may be non-technical)
- Adding or deleting requirements from NISTIR 8259D to support needed additional controls (Note that this uses the NIST SP 800-213 process and the capabilities catalogs)

A goal for the descriptors is to support better understanding between manufacturers and customers about federal organizations' expectations and requirements.

> Takeaway 1: IoT device use risk cannot be independently described without the context of device deployment and system architecture.

Participants saw value in the risk descriptors but didn't believe they could be usefully applied in a context-free manner. There was strong agreement that, for example, whether a device introduced "mission/operation" risk could not be determined without understanding how the device was deployed and being utilized. An illustration was that the risk potentially associated with the smart lock would depend greatly on what it was protecting: an innocuous location versus one with major mission significance. As one facilitator summarized the discussion: "context is everything." A related reaction was that the descriptors as presented were not as independent and mutually exclusive as NIST had intended, and that in many cases multiple descriptors might apply to a particular IoT device deployment.

> Takeaway 2: Unintended uses can create unanticipated risks.

Related to the first takeaway, participants felt that the ability of manufacturers to define the use risk of their products with the descriptors was limited by the potential for customers to deploy the products in unexpected circumstances. By definition the manufacturer cannot know all relevant information about the deployment environment, so the manufacturer's assessment of use risk could be significantly misaligned with the actual risk introduced by unanticipated use. One example presented was the use of a "baby monitor" for monitoring an elderly person; the differences in potential outcomes notably change the "device use" risk.

Takeaway 3: The descriptors could be useful as a communications tool.

Breakout participants expressed support for the potential value of the descriptors as a tool for communications about risk between manufacturer and customer, albeit with some reservations. There were strong expressions regarding the need for common language, and the potential utility for that language being used by customers to express their needs and by manufacturers to describe the capabilities of their products. One facilitator summarized the discussion, saying it is "critically important to have a common list of descriptors being used for that dialog: expression of needs, expression of capabilities". However, there were also reservations regarding how beneficial such descriptors might be for consumer-oriented products and markets, compared to enterprise or government customers.

Other Noteworthy Discussion Points.

- NIST should consider utilizing the Cybersecurity Framework (CSF) when describing risk associated with IoT devices.
- Enterprises, especially larger enterprises, are more familiar with making conscious risk-based assessments; risk evaluation may be implicit in consumer decision making, but risk language may not capture key concerns of consumers.
- For consumers, consider focusing on the privacy implications of IoT devices which could be more useful for consumers.
- A pilot effort applying the descriptors could be very useful in helping to refine them.
- The viewpoint of the party doing the risk assessment may have a significant influence on their view of the risk of a product (e.g., assessment in a laboratory vs. an operational context)

2.2.2 Breakout 2: System and Architecture Descriptors

The second breakout session was titled "No One Size Fits All: Accounting for Device Architecture in applying the Federal Profile", and it focused on discussion of the "device architecture" and "device-system relationship" descriptors presented during Michael Fagan's presentation (See Appendix A for the definitions).

The stated objective for this breakout session to obtain feedback on the utility of the proposed device and system architecture descriptors for:

- Selecting additional needed (or potentially deletion of) controls (Note that the additional controls may be non-technical)
- Adding or deleting requirements from the profile in NISTIR 8259D to support needed additional controls for devices (Note that this uses the NIST SP 800-213 process and the capabilities catalogs)

- Identifying mismatches between manufacturer expectations about usage scenarios from federal organization expectations
- Supporting allocation of requirements within the system addressing the constraints of device and system architecture

As with the descriptors discussed in Breakout 1, a goal for these descriptors is to support better understanding between manufacturers and customers about federal organizations' expectations and requirements.

Takeaway 1: The "device architecture" descriptor definitions have insufficient precision.

Breakout participants generally felt that the device architecture descriptors were not adequately defined and potentially were in conflict with industry usage. An example of this was the association of memory volumes with device types; participants from manufacturers indicated that current microcontrollers have notably more memory. This also highlighted the need for the descriptor specifics to evolve over time with expanding hardware capabilities. There were also suggestions that the microcontroller definition could be improved by citing hardware characteristics such as lack of memory management or virtualization.

Takeaway 2: More "device architecture" descriptors are needed for sufficient granularity.

Both the "constrained microcomputer" and "microcontroller" descriptors generated considerable feedback, suggesting that multiple levels of capability fit under each of those definitions and need to be separated. There was also concern raised that the descriptor definitions needed to explicitly address a broader range of the hardware characteristics of the different device types, and that how those characteristics could affect the risks potentially introduced by different device types needed to be considered. An example of this was devices that incorporate native cellular communications capability, which gives them the potential to bypass the organization's own networks (and network security controls) and communicate directly to outside elements (e.g., "the cloud").

Takeaway 3: The "system relationship" descriptors aren't mutually exclusive.

Breakout participants generally saw value in the device-system relationship descriptors but felt that while they were presented with the intent of being mutually exclusive, they actually would not be so in practice. For example, it was suggested that a device could be both "gated" and a "peer" depending on other elements considered in the relationship. The example of devices with cellular capabilities also aligns with this takeaway. Such devices also potentially reduce the control their owners have over them; for example, the alternative communication paths could be used to push device updates without either the knowledge or the permission of the owners.

2.2.3 Breakout 3: IoT Ecosystem

The third breakout session was titled "Ecosystem View: Mitigating Risks and Reducing Fragmentation Through Ecosystem Cybersecurity" and focused on the role of other elements of IoT devices' ecosystems in identifying and managing risk. IoT device customers must consider the ecosystem where an IoT device (an ecosystem element) is used:

- Network and other technical components
- Physical components
- Administrative and other non-technical considerations and actions
- Other ecosystem elements

The stated objective for this breakout session was to gather feedback regarding IoT device customers' ecosystem risk considerations, and discussion was focused around how the associated risks can be mitigated:

- What are the technical, administrative, and physical risks?
- What do IoT device customers need from manufacturers to support risk mitigation?
- Why is supply-chain/vendor/manufacturer ecosystem transparency needed?
- Why is IoT platform/cloud ecosystem transparency needed?
- Do international standards, confidence mechanisms, and trustworthiness play a role in risk mitigation, or device purchasing decisions? In what ways?

Takeaway 1: A single set of ideally international requirements, standards, and associated confidence mechanisms is needed to address market fragmentation.

Breakout participants expressed support for standards and guidelines to drive security requirements. This includes both support for NIST's work on IoT cybersecurity and a desire for alignment with international standards that span markets. The potential for standards to drive both technical and non-technical aspects of IoT cybersecurity (e.g., establishing a norm for manufacturers to create and provide documentation) was identified as a desirable step forward. Concern was expressed over the current diversity of implementation approaches and the difficulty for manufacturers to select among them. Suitable international standards could help create transparency and encourage trust, and they could also serve to establish a common language for communications between manufacturers and customers.

Takeaway 2: Standards need to encourage cybersecurity by default.

The concern was expressed that a lack of usable standards would lead to "security by proxy as a default," which could introduce potential for expanded risks. Participants indicated that standards for IoT security could compensate for a lack of customer demand, creating an incentive for IoT device security features and corresponding manufacturer support. There were suggestions to review the work of other agencies, such as the Food and Drug Administration (FDA), for effective examples of educating a community about a technology. The Manufacturer Disclosure

Statement for Medical Device Security (MDS[2]) was cited as a good example of a standardized documentation requirement that has proven very effective[5]. There were also suggestions that a scale of "enterprise readiness" would be very helpful for large enterprises making purchasing decisions regarding IoT devices.

Takeaway 3: Supply chain security and transparency are important but very complex.

A number of challenges were identified regarding developing transparency and trust in IoT device supply chains. Participants noted the role of cloud systems in IoT devices as part of the supply chain, and that the constantly evolving nature of cloud implementations and business models could leave customers with no insight into any changes in the cloud that could alter what was an acceptable level of security at time of purchase. The provision of a software bill of materials (SBOM)[6] can help with visibility into an IoT device's implementation, but there are challenges both with the complexity of creating complete, accurate SBOMs and with trust that either the SBOM or the device has not been altered so that they no longer match. Participants largely seemed to agree that many manufacturers currently have poor visibility into and management control over the supply chains for their products.

[5] See https://www.nema.org/standards/view/manufacturer-disclosure-statement-for-medical-device-security

[6] See https://www.ntia.gov/sbom for information about SBOMs

3 Next Steps

The NIST Cybersecurity for IoT Program has identified next steps based on the workshop:

1. Continue to focus on incorporating risk into the NIST cybersecurity for IoT guidance. This includes strengthening the connections to the NIST Risk Management Framework and Cybersecurity Framework. Cybersecurity for IoT is one aspect of addressing cybersecurity broadly within an enterprise, and strengthening the connections to demonstrate the overall unity of the guidance is helpful.

2. Incorporate the feedback received from comments and stakeholder interactions into the NIST Cybersecurity for IoT guidance. Stakeholder interaction has been fruitful and helpful in strengthening the guidance.

3. Develop an updated round of documents with publication targeted for late summer 2021. Guidance is needed, and, to continue to build on the work with the stakeholder community, updates to the cybersecurity for IoT guidance documents need to be finalized.

References

[CATALOG] National Institute of Standards and Technology (2021) *NIST's IoT Cybersecurity Capabilities Catalog*. Available at https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/

[CSF] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[GAO20-77] United States Government Accountability Office (2020) Internet of Things: Information on Use by Federal Agencies. (GAO, Washington, DC), GAO-20-577, August 13, 2020. Available at https://www.gao.gov/products/gao-20-577

[NISTIR8259] Fagan M, 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

[NISTIR8259A] Fagan M, 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

[NISTIR8259B] Fagan M, Marron J, Brady KG, Jr., Cuthill BB, Megas KN, Herold R (2021) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. https://doi.org/10.6028/NIST.IR.8259B

[NISTIR8259C] Fagan M, Marron J, Brady KG, Jr., Cuthill BB, Megas KN, Herold R (2020) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8259C. https://doi.org/10.6028/NIST.IR.8259C-draft

[NISTIR8259D] Fagan M, Marron J, Brady KG, Jr., Cuthill BB, Megas KN, Herold R (2020) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or

Internal Report (IR) 8259D. https://doi.org/10.6028/NIST.IR.8259D-draft

[NISTIR8278] Keller N, Quinn SD, Scarfone KA, Smith MC, Johnson V (2020) National Online Informative References (OLIR) Program: Program Overview and OLIR Uses. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8278. https://doi.org/10.6028/NIST.IR.8278

[NISTIR8278A] Barrett MP, Keller N., Quinn SD, Smith MC, Scarfone KA (2020) National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8278A. https://doi.org/10.6028/NIST.IR.8278A

[NISTIR8333] Megas KN, Fagan M, Cuthill BB, Raguso M, Wiltberger J (2021) Workshop Summary Report for "Cybersecurity Risks in Consumer Home Internet of Things (IoT) Products" Virtual Workshop. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8333. https://doi.org/10.6028/NIST.IR.8333

[OLIR] National Institute of Standards and Technology (2021) *National Online Informative References Program*. Available at https://csrc.nist.gov/projects/olir

[SP800-213] Fagan M, Marron J, Brady KG, Jr., Cuthill BB, Megas KN, Herold R (2020) IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-213. https://doi.org/10.6028/NIST.SP.800-213-draft

Appendix A: Descriptor Definitions

IoT Device Use Risk Descriptors:

- *Non-Critical:* Devices the customer may regularly use but does not rely upon. Loss of functionality for short periods has minimal impact on the customer organization's operations. The device does not collect any sensitive data. These devices do not introduce significant risk to systems and/or data beyond being a connected product.
- *Environment:* Devices that can have an impact on the physical environment in which the equipment is used but do not pose physical safety risks. These devices are not relied upon for accomplishing core mission functions. The impact on the physical environment introduces additional risk for customer organizations.
- *Mission/Operation:* Devices that the customer relies on for their operations and interference with function or unauthorized data disclosure can introduce significant risk for the customer organization.
- *Safety:* Devices that can impact safety, which can introduce significant risk for the customer organization.

IoT Device Architecture Descriptors:

- *Microcomputer:* Has a traditional architecture that supports flexible software packages, including an operating system, etc. These support all conventional IT cybersecurity needs and goals with some adaptations for divergent use cases and form factors for IoT devices. (Equivalent to IETF RFC 7228, Class 2 Constrained Nodes)
- *Constrained Microcomputer:* These devices can support many customer cybersecurity needs and goals but may do so differently from conventional IT equipment. Their more limited functionality may reduce risks to networks, but these devices should not be assumed to have a reduced risk profile. (Equivalent to IETF RFC 7228, Class 1 Constrained Nodes)
- *Microcontroller:* These devices will likely need an intermediary (e.g., hub/gateway) to help support customers' needs and goals. Their severe technical constraint also makes it possible that these devices may pose less inherent risk and need less to support customer's cybersecurity needs and goals. Gated or Segmented system relationships can help make these devices securable. (Equivalent to IETF RFC 7228, Class 0 Constrained Nodes)

IoT Device-System Relationship Descriptors:

- *Peer:* IoT component is fully integrated into the system. An IoT device/component that is connected to a network/system as a peer may need to provide all capabilities required to support all the controls of the customer network.
- *Peripheral:* IoT component is not fully integrated into the network (e.g., it may be separated via some kind of hub or gateway from the broader system) but can systematically access data or operations of other components through its connection. Like a "peer", programmatic data and component access can be leveraged by an attacker in the

event of a cybersecurity event. Mitigations and/or capabilities needed for support could change if a hub or other device provides the connection.

- *Gated:* IoT component is not integrated on its own into the network and its data streams at all, but it is linked via an intermediary gateway and may communicate with the system only through this gateway. Peripheral and Gated relationships differ in the level of separation provided by the gateway between IoT device and the broader system. A Gated relationship will ensure that the IoT device has no possible direct access to other system components.
- *Segmented:* The IoT component is logically or physically detached from the broader network and cannot communicate with the broader system at all. This relationship fundamentally alters the risk an IoT device would present to a customer system. Its ability to taint the broader system's operations is zero, but this does not mean this IoT device will have no customer cybersecurity needs and goals.

Appendix B: Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

CIO	Chief Information Officer
CBP	Customs and Border Patrol
CSF	Cybersecurity Framework
DHS	Department of Homeland Security
DOC	Department of Commerce
EPA	Environmental Protection Agency
FDA	Food and Drug Administration
GAO	Government Accountability Office
HVAC	Heating, Ventilation, and Air Conditioning
IETF	Internet Engineering Task Force
IoT	Internet of Things
IR	Informative Reference
IT	Information Technology
ITL	Information Technology Laboratory
MDS2	Manufacturer Disclosure Statement for Medical Device Security
NASA	National Aeronautics and Space Administration
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal / Interagency Report
NOAA	National Oceanic and Atmospheric Administration
OLIR	Online Informative References
OT	Operational Technology

PIV	Personal Identity Verification
RFC	Request For Comments
RMF	Risk Management Framework
SBOM	Software Bill of Materials
SME	Subject Matter Expert
SP	Special Publication
UAS	Unmanned Aircraft System