NISTIR 8322

Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop

Katerina N. Megas
Michael Fagan
David Lemire

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8322

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

NISTIR 8322

Workshop Summary Report for "Building the Federal Profile for IoT Device Cybersecurity" Virtual Workshop

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.8322

January 2021

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8322
30 pages (January 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8322

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. 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 in July 2020. NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device Manufacturers* and NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline* provide general guidance on how manufacturers can understand and approach their role in supporting customers' cybersecurity needs and goals. As discussed in those documents, specific sectors and use cases may require more specific guidance than what is included in NISTIR 8259A's core baseline for IoT devices. NIST conducted the virtual workshop "Building the Federal Profile for IoT Device Cybersecurity" to discuss and gather community input on the creation of a federal profile of the core baseline for use by federal agencies. This publication provides a summary of the workshop. The baseline will be published in NISTIR 8259D, *Profile of the IoT Core Baseline for the Federal Government*.

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 and those considering how profiling the core baseline will further IoT device cybersecurity for their sector.

Table of Contents

List of Appendices

1 Introduction

On July 22-23, 2020, the National Institute of Standards and Technology (NIST) conducted a virtual workshop entitled *Building the Federal Profile For IoT Device Cybersecurity: Next Steps for Securing Federal Systems*. The event included stakeholders from across government, industry, international bodies, and academia. The goal was to identify gaps in the Internet of Things (IoT) cybersecurity ecosystem that need to be addressed in a federal profile for IoT device cybersecurity. Over 500 people participated from the U.S. and 25 other countries, representing a broad mix of government, industry, and academia.

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 [PRGM] is to cultivate trust in the IoT and foster an environment that enables innovation on a global scale through standards, guidance, and related tools. The Cybersecurity for IoT program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

1.2 Background For The Federal Profile

NIST leveraged the Core Baseline established in NIST Internal Report (NISTIR) 8259A, *IoT Device Cybersecurity Capability Core Baseline* [NISTIR8259A], and analyzed the security controls found in NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* [SP800-53], to develop a catalog of key IoT device cybersecurity capabilities and non-technical supporting capabilities and associated IoT device customer controls. As was discussed in NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* [NISTIR8228], IoT devices routinely lack critical cybersecurity capabilities that are commonly found in IT devices. Additionally, IoT manufacturers often do not provide sufficient information for IoT device customers to integrate their devices in secure ways in order to mitigate the risks created within the associated systems and to comply with compliance requirements. The catalog under development is a critical building block for establishing a federal profile of the Core Baseline ("federal profile") to help federal agencies and manufacturers bridge these gaps. Identifying critically needed capabilities will help federal agencies acquire IoT devices that they can securely incorporate into their systems and meet security requirements for federal information and systems. The future federal profile also aims to help manufacturers looking at federal customers and use cases to go beyond identifying the types of cybersecurity device capabilities listed in NISTIR 8259A to considering specific capabilities requirements of federal agencies. Manufacturers can engineer the technical capabilities and provide non-technical supporting capabilities to IoT device customers to help ensure that customers' systems meet an established level of management, operational, and technical security control requirements.

1.3 About the IoT Federal Profile Virtual Workshop

The free, publicly available virtual workshop consisted of a pair of two-hour long sessions, one per day[1]. The agenda is provided in Table 1. It included panel discussions on key topics related to cybersecurity challenges for federal IoT devices. These topics include the need for support for IoT device cybersecurity capabilities and additional supporting capabilities from the manufacturers and mechanisms giving federal agencies, as well as non-federal users of IoT devices, confidence that such devices will satisfy defined cybersecurity requirements.

Table 1 – Agenda for the IoT Federal Profile Virtual Workshop

Day	Time	Activity and Presenters
22 July	10:00 am	**Welcome and introduction: Kevin Stine**, Chief, Applied Cybersecurity Division, NIST
	10:15 am	**Keynote: Grant Schneider**, Senior Director for Cybersecurity Policy at National Security Council, The White House and Federal Chief Information Security Officer
	10:45 am	**Panel Discussion: Stoves, Drones, and Automobiles!: Federal Government IoT Use-Cases and Technical Cybersecurity Considerations** (1 hour, 15 minutes) • **Moderator: Michael Fagan**, Technical Lead, NIST Cybersecurity for IoT Program • **Bo Berlas**, Chief Information Security Officer, U.S. General Services Administration • **Katherine Gronberg**, Vice President for Government Affairs, Forescout Technologies • **Nedim Goren**, Federal Information Security Management Act (FISMA) Implementation Project, Computer Security Division, NIST • **Scott Rose**, Computer Scientist, Advanced Network Technologies Division, NIST • **Trevor H. Rudolph**, Vice President, Global Digital Policy, Schneider Electric • **McKay R. Tolboe**, Chief of the Cybersecurity Policy and Implementation Division, Department of Defense (DoD)
23 July	10:00 am	**Panel Discussion: Who are you going to call?: Federal Government IoT Non-Technical Cybersecurity Needs** • **Moderator: Barbara Cuthill**, Deputy Program Manager, NIST Cybersecurity for IoT Program • **Dr. Amit Elazari Bar On**, Director, Global Cybersecurity Policy, Intel Corporation • **Nedim Goren**, Federal Information Security Management Act (FISMA) Implementation Project, Computer Security Division, NIST • **Deral Heiland**, Principal Security Researcher (IoT), Rapid 7 • **Rebecca Herold**, CEO, Rebecca Herold & Associates, LLC • **David Kleidermacher**, Vice President, Android Security & Privacy, Google • **Ari Schwartz**, Managing Director of Cybersecurity Services, Venable LLP

[1] Recordings of the event can be accessed at: https://www.nist.gov/news-events/events/2020/07/building-federal-profile-iot-device-cybersecurity-next-steps-securing

Day	Time	Activity and Presenters
23 July	10:55	**Panel Discussion: Close Encounters of the Confidence Mechanism Kind** • **Moderator: Amy Mahn**, International Policy Specialist, NIST Cybersecurity for IoT Program • **Mike Bergman**, Vice President, Technology & Standards, Consumer Technology Association • **Rob Cantu**, Director, Cybersecurity, CTIA • **Gordon Gillerman**, Director, Standards Coordination Office at NIST • **Apostolos Malatras**, Network and Information Security Expert, European Union Agency for Cybersecurity (ENISA) • **Rob Morgus**, Director, Research & Analysis, U.S. Cyberspace Solarium Commission • **Peter Stephens**, Head of Secure by Design, Cyber Security for the Internet of Things, Department of Digital, Culture, Media, and Sport (UK)
23 July	11:55 AM	**Concluding Remarks: Kat Megas**, Program Manager, NIST Cybersecurity for IoT Program

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 key IoT device cybersecurity capabilities and supporting non-technical manufacturer capabilities and associated IoT device customer controls previously developed by NIST and available for review and feedback via GitHub[2].

The workshop drew approximately 500 participants, panelists, speakers, and moderators. This included representatives from:

- A mixture of government, industry, and academia, as well as researchers and the press
- A broad range of federal government organizations including civil government, defense, and intelligence
- 26 countries, including 5 foreign governments
- At least 39 U.S. states, including 8 state governments

In addition to the ability for participants to submit individual questions (which could be "up-voted" by other participants), the workshop included a series of 12 polls as a mechanism to gather participant feedback and influence the focus of panel discussions. The poll questions and poll results are presented in Appendix A. Since workshop attendees created a by-definition self-selected survey group 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. 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] The catalog of technical cybersecurity capabilities and non-technical supporting capabilities can be viewed on GitHub at https://pages.nist.gov/FederalProfile-8259A/; feedback can be submitted by submitting issues to the repository at https://github.com/usnistgov/FederalProfile-8259A.

2 Event Summary and Key Takeaways

The summary below highlights significant points from the keynote presentation, and identifies discussion topics, and NIST's takeaways and observations from the three panel sessions.

2.1 Keynote: Federal Chief Information Security Officer

The keynote presentation was made by Grant Schneider, the Federal Chief Information Security Officer (CISO), setting the stage for the panel discussions that followed. Mr. Schneider also participated in a question and answer session at the conclusion of his keynote. Mr. Schneider's presentation and responses to questions highlighted a number of important considerations for the use of IoT technology in federal information systems:

- In his opinion, IoT security has not received enough attention, in both consumer and organizational contexts. He noted that the increasing interconnection of systems of all types increases attack surfaces and expands the threat profile.
- He identified three core activities that the Office of Management and Budget (OMB) performs that are particularly relevant to federal information system security:
    - Overseeing the implementation of Federal Information Security Management Act (FISMA) for non-National Security Systems; he noted that in doing this OMB works closely with the Department of Defense (DoD) and the Director of National Intelligence (DNI) to present consistent guidance across the federal space including the DoD and the intelligence community (IC).
    - Overseeing the implementation of cybersecurity policies and standards. He noted that OMB has been taking a more active oversight role and seeking to assist federal organizations in meeting their FISMA responsibilities.
    - Ensuring agencies comply with government-wide cybersecurity guidance and legislation, including Binding Operational Directives and Emergency Directives from the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA).
- He stated that the scope of "Federal Information systems includes IoT devices", adding "I don't think we've had enough conversation on that." He expressed concern that IoT devices are seen as less impactful or less risky, and cited an example of a networked traffic sign being used as an entry point for a cyber-attack as a "wake-up call" to the range of concerns that IoT raises.
- He emphasized that OMB's work in cybersecurity is guided by a risk management philosophy. He described a "high-value asset" program intended to assist agencies in identifying and protecting their high-value information system and data, and share solutions across agencies.
- He said the Federal government is seeking to lead by example, as captured in the National Cyber Strategy published in September 2018 [CYBSTRAT]. Concerns he identified included the difficulty of determining the security provided by IoT products, and the limitations of government buying power to "move the economy", meaning that other incentives such as government mandates or regulation might need to be considered.

- He indicated that IoT devices were a component of broader concerns about supply chain security and risk management, which is a major focus of both the executive and legislative branches of government. Poorly designed and configured devices are a notable part of that supply chain concern.
- He described the creation of the Federal Acquisition Security Council (FASC) by the Secure Technologies Act of 2018 [SECTECH], and identified several FASC focus areas:
    - The creation of an information sharing environment for supply chain risk management information.
    - The potential establishment of shared services for supply chain risk management, to allow federal organizations of all sizes to perform due diligence regarding supply chain risk.
    - Recommending removal orders or exclusion orders to DHS, DoD, and the IC to ban covered items, and encouraging individual agencies to develop their own such orders where appropriate.
- He clarified that IoT devices that connect via cloud or mobile (e.g., 5G) technologies are part of federal information systems even if they don't directly touch a federal network, saying that current policies cover IoT and similar devices in the definition of a federal information system, although he recognized there may be need for amplifying guidance.
- He stated that he saw value in third-party certifications for IoT cybersecurity, although he noted that it could be unclear what is actually being certified, and suggested that it may be more meaningful to certify the manufacturer's development methodology rather than specific IoT products.
- He discussed the value of an international trusted marketplace for IoT, and the importance of international standards and working with international partners to achieve that.

2.2 Summary and Takeaways from Panel Sessions

These takeaways are ideas that NIST heard from participants and that received significant support from attendees and/or panelists. This workshop was not a forum for developing consensus, so these takeaways represent themes repeatedly heard not a formal position of attendees or participants. 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.

Takeaway 1: IoT is both extremely diverse and becoming pervasive in federal information systems and beyond. This will only grow over time as network-connected products of all types become the norm in the market.

Numerous panelists noted that consumers are widely adopting IoT devices and that IoT use within federal agencies is growing rapidly. The General Services Administration (GSA) has identified over 75 makes and 210 distinct models of IoT devices deployed in facilities they manage, spanning a broad range of IoT related services. IoT devices support many kinds of services that include network-connected surveillance equipment, irrigation control systems, physical access control systems, lighting control systems, and various types of environmental measuring systems, among others.

Manufacturers have entered the IoT market with enthusiasm leading to a great deal of innovation and a diversity of product offerings. However, this market is still quite immature and dynamic where price and features have dominated manufacturer priorities and cybersecurity has not been given adequate attention. Many small- and medium-size manufacturers moving into the IoT market do not have the cybersecurity background of more established information technology (IT) product manufacturers. Many of the lessons learned in the world of security for IT have not yet been applied to IoT devices, or haven't been adapted to those devices' unique characteristics, such as limited power and computing capabilities. The market is also quite diverse, with some vertical sectors (e.g., medical devices) having more clearly defined requirements than others (e.g., consumer-oriented IoT).

Use of IoT is expected to grow widely. The addition of network connectivity to products of varying types is a near-universal theme. Manufacturers are incorporating this feature into nearly every new product, creating a situation where the introduction of network-connected IoT devices into an environment is nearly unavoidable. Katherine Gronberg of Fourscout noted it is "going to be increasingly hard for agencies to have appliances … that don't have a network connection."

Takeaway 2: The NIST IoT cybersecurity project's characterization of IoT has found general acceptance in the cybersecurity community as a working definition.

While IoT devices are becoming nearly ubiquitous in many environments, defining and categorizing such devices remains an on-going challenge.[3] IoT covers a broad spectrum, from building monitoring systems to connected automobiles to smart appliances and even toys. This lack of consensus was discussed at the October 2017 NIST *IoT Cybersecurity Colloquium*. Since that event, the NIST IoT Cybersecurity program published a description of IoT device capabilities in NISTIR 8228, and created a working definition of IoT devices as the scope for

[3] NIST SP 1900-202, *Cyber-Physical Systems and Internet of Things*, focuses on the meanings of the phrases "cyber-physical systems" (CPS) and "Internet of Things" (IoT), and on the relationship between them. This document examines 31 definitions for CPS and 30 definitions for IoT.

NISTIR 8259. Panelists in the July 2020 workshop, including representatives from two vendor participants, described the NISTIR 8259 characterization of IoT devices as having "at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface … for interfacing with the digital world" as "more or less becom[ing] a *de* facto definition … [that] will probably be used by regulatory bodies in the U.S. and the federal government and abroad moving forward."[4]

Takeaway 3: IoT customers, especially in the consumer space, tend not to prioritize IoT device security and are often unaware that it should be a consideration in their selection and use of IoT devices.

Overwhelmingly, workshop participants agreed that customers lack an awareness that cybersecurity capabilities can vary among devices when they make purchasing decisions about IoT. This appears to be true regardless of whether the customers are individual consumers or those responsible for procurement in organizational environments. In the consumer space the buyer's assumption generally is that if a product is on the market, its safety and security can be assumed. A UK study found that consumers focus on IoT device features and costs as the most important discriminators, with cybersecurity either not on the list of customer priorities or at best lagging far behind as a decision criterion. Mike Bergman of the Consumer Technology Association (CTA) stated that "we have been doing this research for years and years and the answers never changed. Cybersecurity is not on this list. So while it might be a good idea to try to get it on the list … it is going to be a very long and expensive education process."

Where meaningful cybersecurity information about a product is available, a further challenge is educating customers about how to understand the information available and interpret its implications when using the product in their environments. In organizational procurement environments, the staff responsible for procurement contracts typically lack subject matter expertise regarding cybersecurity and need education and training in leveraging contractual language to mandate security for procurements. Peter Stephens said "whenever I speak to procurement organizations, whether they are retailers or housing, manufacturing, builders or other organizations who use smart devices in some format, the person responsible for procuring the devices quite often is not an expert at all." The availability of sample procurement language can be of great benefit in improving the security of products procured by organizations.

[4] The NIST description was also used in H.R.1668 - *IoT Cybersecurity Improvement Act of 2020*, which referenced the NISTIR 8259 definition, stating that IoT devices "(A) have at least one transducer (sensor or actuator) for interacting directly with the physical world, have at least one network interface, and are not conventional Information Technology devices, such as smartphones and laptops, for which the identification and implementation of cybersecurity features is already well understood; and (B) can function on their own and are not only able to function when acting as a component of another device, such as a processor."

Takeaway 4: The community recognizes a need for an "international trusted marketplace" for IoT, but market forces alone are unlikely to provide sufficient incentive to bring that into being.

Most workshop participants agreed that manufacturers of IoT devices currently lack market incentives to prioritize cybersecurity as a concern when designing, marketing, and supporting their products. Some counterexamples were presented in which informed customers do recognize the advantages of enhanced security. This suggests that enhanced cybersecurity could demonstrably be a market advantage if it is emphasized. Workshop poll results showed strong support (71 %) for government mandates as a mechanism for enhancing IoT cybersecurity (poll #4), and general agreement (55 %) that developers of IoT devices currently lack appropriate incentives to secure their products (poll #2). Participants supported a mixture of regulatory guidance, customer education, supply chain pressures, and other considerations to create the economic incentives to shift the overall IoT device market toward enhanced cybersecurity.

A lack of customer understanding today often translates into a lack of demand for needed device cybersecurity capabilities, leading to manufacturers prioritizing other aspects when defining their markets and developing products. The lack of incentives to address cybersecurity is a significant problem in the current IoT ecosystem. This lack is particularly problematic with new developers of IoT devices, who are focused on features and fail to recognize their responsibilities for cybersecurity, and with smaller developers who lack the resources, and often the awareness of the need for cybersecurity, to engineer cybersecurity capabilities within their IoT devices. The introduction of third-party certification or labeling authorities into the ecosystem could also provide incentives for IoT device developers and help level the playing field by encouraging all developers to address cybersecurity requirements.

The requirement for government purchasers to meet mandatory security requirements provides some degree of incentive but the government market, including both civil government and DoD, is neither large enough nor diverse enough to have sufficient leverage to truly drive the broader IoT market. Panel members also mentioned a variety of proposals for incentives to improve IoT device cybersecurity: legislative solutions, third-party certifications, and non-profit labeling authorities. All of these approaches were recognized as ways to encourage manufacturer attention to cybersecurity. A primary objective for all of these incentives is to encourage the development of a trusted, international marketplace for IoT devices where the customers can confidently procure IoT devices and manufacturers recognize that cybersecurity as a feature has meaningful market value.

Takeaway 5: Governments are moving ahead with providing guidance, and consensus is building around international standards.

Workshop participants were broadly supportive of the development and application of formal guidance as a mechanism to improve the cybersecurity of IoT devices. This guidance is developing in the form of international standards, national and state government legislation and regulations, and other mechanisms. Several examples of such guidance were discussed. The

NIST IoT cybersecurity program in the U.S. is developing guidance that can be applied by federal agencies, as well as other sectors that choose to adopt them. Individual U.S. states have begun developing IoT security regulations, mandating specific security features in state laws. The United Kingdom is legislating IoT cybersecurity requirements.

In addition to governmental cybersecurity standardization and regulation efforts within the U.S. at the national and state level, international standards bodies are working to establish IoT cybersecurity guidance, such as the development of International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27402, *Cybersecurity — IoT security and privacy — Device baseline requirements*. The development of consensus international standards could provide a baseline of cybersecurity guidance for manufacturers and assist in the development of a trusted international marketplace.

Takeaway 6: Manufacturers are concerned that fragmented guidance from multiple sources could force corresponding fragmentation of product offerings.

Manufacturing representatives expressed concern about the potential with the proliferation of guidance from multiple sources for creating conflicting requirements, creating the potential that manufacturers will be forced to respond to fragmented and incompatible or contradictory guidance from different jurisdictions. In that situation manufacturers are faced with the challenge of deciding which markets to address and which regulations apply within those markets. Manufacturers want regulatory consistency and are challenged if conflicting requirements from diverse sources necessitate costly measures (e.g., multiple manufacturing lines) in order to deliver products that address the relevant guidance. Trevor Rudolph said "from the manufacturer's standpoint really what we want is regulatory certainty and guidance from the federal government." The ability to focus resources on improving cybersecurity overall by creating fewer products suitable for a broader set of markets is diminished if fragmented regulatory guidance enforces a need to provide different versions of products that each satisfy a different guidance regime. Gordan Gillerman stated "In my experience, manufacturers are adept at building products that meet supersets of requirements and having them be globally able. What is challenging for manufacturers is when all of a sudden [they] need two production lines for the same product because somebody has exclusive requirements from what everyone else agreed on." Specific security measures that do not adapt to the evolving technology of IoT devices create additional potential for market fragmentation.

Takeaway 7: Security for IoT is a shared responsibility between manufacturers and customers. The goal of a shared responsibility is: Manufacturers provide securable products and guidance on secure configuration and use. Customers then apply the manufacturer's guidance to employ the technology securely.

Security for IoT devices cannot be achieved through technology alone. Eighty-two percent of responses to one poll question agreed that the responsibility for securing IoT devices is shared between manufacturer and customer (poll #9). On the manufacturer side, devices should

incorporate appropriate technical cybersecurity capabilities so that secure deployment and operation are feasible, and those technical capabilities should be complemented with non-technical supporting capabilities such as documentation explaining secure configurations, software updates to address discovered vulnerabilities, and publication of security best practices for their products. Customers, then, are responsible for implementing IoT devices in accordance with manufacturer guidance, ensuring devices have connectivity to receive updates, and monitoring devices to ensure continued security. Customers also follow their own established policies to appropriately mitigate the risks that IoT devices bring within their system(s). The support procedures will typically use the manufacturer's guidance. Bo Berlas suggested that a solution similar to FedRAMP would be appropriate: "in cloud with FedRAMP there is this notion of customer responsibility such that what the vendor does together with what the customer does effectively results in a secure profile and I think that logic can generally align here too."

Takeaway 8: Manufacturer support for IoT device security is essential for the shared responsibility model to succeed.

Manufacturer support comprises a number of activities, especially documentation and software updates. An on-going challenge for customers and users in assessing and improving IoT device cybersecurity is inadequate documentation of device characteristics. Lack of documentation hinders both security assessments and the ability to select compensating security controls to address IoT device cybersecurity shortcomings. While some manufacturers do provide substantive documentation, many provide very little, leaving customer organizations starved for information on which to base risk assessments. Both the development of security solutions and the assessment of those solutions require information about, for example, the network communications patterns expected for IoT devices.

Manufacturer communications regarding IoT device cybersecurity need to address a range of audiences with diverse levels of sophistication and understanding of the cybersecurity challenge. This includes communication both at the consumer level and with organizational procurement activities. Vendors need to convey information about product operation and about using device cybersecurity features, as well as more general communications regarding manufacturer procedures and commitments for vulnerability disclosure, software update frequency and mechanisms, and duration of support commitments for IoT products. Derail Heiland explained "we need to be able to get detailed information around those specific security topics on how do we reduce risk by properly implementing. How do we deploy into our organization? How do we get the detailed information to help us make those security risks evaluations for better deploying the technology? Often we are not seeing that information."

An essential element of manufacturer communications is clear explanation of customer responsibilities for IoT device cybersecurity. Consumers, for example, primarily need basic installation and configuration guidance, whereas organizational customers need more extensive documentation to address device configurability, deployment of devices at scale, and information enabling the organization to ensure it is able to satisfy its legal obligations. All customers need clarity regarding available manufacturer communications channels, frequency of software updates, and end-of-life dates beyond which specific IoT devices will no longer be supported.

Takeaway 9: Security for IoT should be addressed using a risk management approach in concert with that used for traditional information technology, although different technical solutions may be needed for each.

Workshop panelists agreed that IoT devices introduce varying amounts of risk into their environments. For example, IoT devices regulating physical access or supporting warning systems may represent much greater risk than so-called "smart" appliances; however, attacks using apparently low-risk devices (e.g., an aquarium thermometer, a network-connected traffic sign) as paths into owner information systems have had serious consequences. Detection and identification of the IoT devices present in an environment also presents a significant challenge. Information about individual devices can be difficult to obtain, although there are efforts to crowdsource such information to ease the challenge of device identification.

The introduction of IoT devices may require a shift of mindset when applying the NIST Risk Management Framework (RMF). As stated by Grant Schneider: "Risk management: that's really what this boils down to." System owners and assessors need to clearly understand guidance that federal information systems include IoT devices, which must be viewed as part of the enterprise information system and treated as components of the system(s) being assessed. Katherine Gronberg observed that a goal of federal programs "is ultimately to assess and then mitigate risk on the networks which include IoT and OT presence." Agencies must ensure that IoT devices are included within the scope of their risk management approach, whether assessing enterprise IT, specific IT systems, or operational technology (OT) systems where IoT devices have been introduced. Security controls from the SP 800-53 catalog must be considered in the assessment of IoT devices within agency systems.

No single security solution is appropriate for all devices across this spectrum. As IoT devices are integrated into federal information systems, potential issues arise regarding the ability to both understand and modify device configurations in order to bring them into alignment with security controls imposed by the RMF process (e.g., implementing a mandatory warning banner in the user interface of an IoT device).

The introduction of IoT devices creates significant challenges for security assessment of federal information systems. Cybersecurity must be assessed both at the component level (i.e., individual IoT devices) and the system level (i.e., the integration of a set of IoT devices with traditional IT in a specific operating environment). An additional challenge is security testing of systems with IoT devices, especially when evaluating the impacts of updates to those devices. For example, if automatic security updates of IoT devices are enabled, when and by whom are tests of those updates to be performed?

Software updates for IoT devices are a crucial aspect of cybersecurity. Automation of updating is generally one of the strongest mechanisms for minimizing device vulnerability and opportunities for attack, especially in the consumer space. Workshop participants favored automated update mechanisms that still offer device owners a measure of control over when updates are applied (poll #7). In the context of a federal information system, a complicating factor is the need to test updates prior to application due to their potential to affect a system's security posture. In some

cases, updates can significantly alter the capabilities of an IoT device (e.g., by activating hardware capabilities that have been latent), with correspondingly significant implications for the information system's risk posture. Federal information system owners need to establish a process to assign responsibility for and establish an environment to enable testing of updates.

Takeaway 10: Securely integrating IoT devices into modern networks will require moving beyond legacy network security solutions.

Network segmentation, traffic shaping with firewalls, and other legacy network security solutions are severely challenged by the introduction of IoT devices. IoT devices as elements of federal information systems may present very different security characteristics from traditional IT system elements, yet all must support the overall security goals and objectives for the complete information system. Bo Berlas observed "Traditionally we've been dependent on VLANS and firewalls and things of that nature, I think we need to go through and advance that understanding to start to look at for example with network access control tools, … looking at device profiling, … looking at newer concepts like zero trust."

The threat environment associated with IoT devices can be more dynamic than that associated with other products, including traditional IT products. For example, not all IoT devices support software updates to remove vulnerabilities. When software updates are possible, updates to deployed IoT devices can change their operational and cybersecurity characteristics. Such changes can, in turn, change the risk characteristics of the systems in which the devices are deployed. In parallel, attackers seek new avenues for exploitation of IoT devices as their characteristics evolve. The dynamic nature of IoT devices mitigates against the use of traditional product assessment and certification models for IoT devices; a one-time certification becomes meaningless as the device changes over time.

Another challenge is dealing with security incidents involving devices performing critical functions. It may be unacceptable, for example, to completely quarantine a device that performs a mission critical function dependent on Internet connectivity. A related consideration is the loss of manufacturer support when Internet connectivity is withdrawn, both in terms of direct actions like software updates, and considerations of whether manufacturers honor product warranties.

When combined with edge computing concepts enabled by new technologies such as 5G, this creates difficulty in defining the boundaries of a federal information system by introducing system topologies that vary greatly from traditional models. This technology enables the expanded use of edge computing deployed outside the traditional boundaries that define federal information systems, as well as other "smart" solutions, both of which could create situations where 5G-enabled IoT devices may be capturing and processing federal data while being physically and/or logically outside the bounds of any particular federal information system.

Takeaway 11: Automation protocols provide promise for deploying, on-boarding, and securely using IoT devices at scale in the enterprise.

Device discovery and on-boarding is a known major challenge with IoT devices. Katherine Gronberg stated that IoT devices are "actually very difficult to detect. It is actually hard, we find agencies don't know how much is actually on their networks." Scott Rose observed "in order for IoT to succeed you cannot rely on individuals to set up and administer every individual IoT device. You will have to have this kind of autonomic network configuration." Manufacturers and standards organizations have begun developing approaches to address some of these concerns:

- The Internet Engineering Task Force (IETF) has a group developing the Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol, intended to provide a solution for secure zero-touch (automated) bootstrap of new (unconfigured) devices. [ID-BRSKI]
- The IETF's Manufacturer Usage Description (MUD) is a protocol for IoT devices that provides a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. The MUD protocol is documented in [RFC8520].

Takeaway 12: The supply chain[5] for IoT devices is both a source of security risk and a potential opportunity to encourage improvements.

The supply chain represents both challenge and opportunity for IoT device cybersecurity. Grant Schneider stated that "supply chain risk management … [is of] significant interest both on the part of Congress and on the part of the executive branch." The complexity and opacity of current IoT supply chains raises concerns about opportunities for bad actors to negatively impact device cybersecurity and a general inability for purchasers to have confidence in the characteristics of any particular product emerging from that supply chain. Apostolos Malatras noted that the European Union Agency for Cybersecurity (ENISA) has observed that, compared to other manufacturing sectors, "the relationship between suppliers and providers, between the peers in the supply chain are not mature at all. And they change very frequently." However, there are also opportunities to share information gathered about the supply chain, and some organizations are focusing on the supply chain as a more effective place to focus cybersecurity efforts: rather than working to raise customer awareness they instead place pressure on manufacturers to configure their supply chains to produce more secure products. There is also potential for other mechanisms, such as third-party assessment and certifications and regulations requiring recall procedures, to have a positive impact on IoT device cybersecurity through the supply chain.

[5] As described in NIST SP 800-161, the supply chain infrastructure is the integrated set of components (hardware, software, and processes) within the organizational boundary that composes the environment in which a system is developed or manufactured, tested, deployed, maintained, and retired/decommissioned. A supply chain consists of multiple layers of system integrators, external service providers, and suppliers.

Grant Schneider stated that the U.S. Federal Acquisition Security Council (FASC) within the Office of Management and Budget (OMB) has been tasked to look at the potential for shared services for federal agencies in the area of supply chain risk management. The goal is to enable the sharing of supply chain information across federal agencies and with the private sector. This would enable organizations with different levels of capability to implement consistent amounts of due diligence when evaluating supply chain risk.

Takeaway 13: Conformance assessments and third party certifications can assist customers with selection of IoT security products with suitable security.

Consumers are familiar with a variety of common product labeling regimes, such as for nutritional information and product safety (e.g., Underwriters Labs [UL]). A proposed approach to providing confidence measures around IoT device cybersecurity is the development of a roughly equivalent form of review and labeling. However, creating such a testing and labeling regime would likely be a slow and expensive process.

A related idea is the concept of a labeling authority, a non-profit, non-governmental organization that would serve as a project manager for centralized certification and labeling efforts in the United States. The authority would accredit other organizations to take on specific IoT technology verticals, such as medical devices or connected automobiles. Mike Bergman noted that "The IoT ecosystem is enormous. It needs more than a single type of baseline and more than one type of confidence mechanism. In that broad landscape there is room for third-party assessment and supplier declaration of conformity for certification and labeling and so on." Rob Morgus called participants' attention to the U.S. Cyberspace Solarium Commission's "recommendation for creation of a national cybersecurity certification and labeling authority. … It would be a nonprofit, nongovernmental organization to serve as a project manager for centralized certification and labeling efforts in the United States, empowered to accredit other organizations to sort of take on specific verticals of technology, like certain IoT verticals."

3 Next Steps

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

1. *Complete the Federal Profile*. The program needs to complete its work to create the federal profile, gather public feedback, and finalize the profile. This work is underway and the results will be published as NISTIR *8259D*, *Profile of the IoT Core Baseline for the Federal Government*.

2. *Provide Guidance for Developing Profiles*. Other groups have expressed interest in developing profiles of the core baseline for use within their own sectors of interest (e.g., vertical market sector, regulatory scope). The program is documenting the process that has been worked out while developing the federal profile. That process will be published as NISTIR 8259C, *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*.

3. *Evaluate Approaches for Establishing Confidence in IoT Device Cybersecurity*. Workshop participants indicated a desire for greater specificity regarding the use of conformance assessments and other confidence mechanisms such as labels and self-certification. These confidence mechanisms can be an important component of the IoT cybersecurity solution space. The program will begin exploring, in concert with interested government and industry organizations, approaches for gaining confidence in the cybersecurity capabilities of IoT devices that address the needs of both IoT device users and manufacturers.

References

[CYBSTRAT] The White House (2018) National Cyber Strategy of the United States of America. (The White House, Washington, D.C.). Available at https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[ID-BRSKI] Pritikin M, Richardson M, Eckert TTE, Behringer MH, Watsen KW (2020) Bootstrapping Remote Secure Key Infrastructures (BRSKI). (Internet Engineering Task Force, Anima Working Group). Internet Draft. Available at https://tools.ietf.org/html/draft-richardson-anima-brski-renamed-00

[NISTIR8228] Boeckl KR, Fagan MJ, Fisher WM, Lefkovitz NB, Megas KN, Nadeau EM, Piccarreta BM, Gabel O'Rourke D, Scarfone KA (2019) Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8228. https://doi.org/10.6028/NIST.IR.8228

[NISTIR8259A] Fagan MJ, Megas KN, Scarfone KA, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. https://doi.org/10.6028/NIST.IR.8259A

[PRGM] National Institute of Standards and Technology (2021) *NIST Cybersecurity for IoT program*. Available at https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[RFC8520] Lear E, Droms R, Romascanu D (2019) Manufacturer Usage Description Specification. (Internet Engineering Task Force), IETF RFC 8520. https://doi.org/10.17487/RFC8520

[SECTECH] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. 115-390, 132 Stat. 5173. https://www.govinfo.gov/app/details/PLAW-115publ390

[SP800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

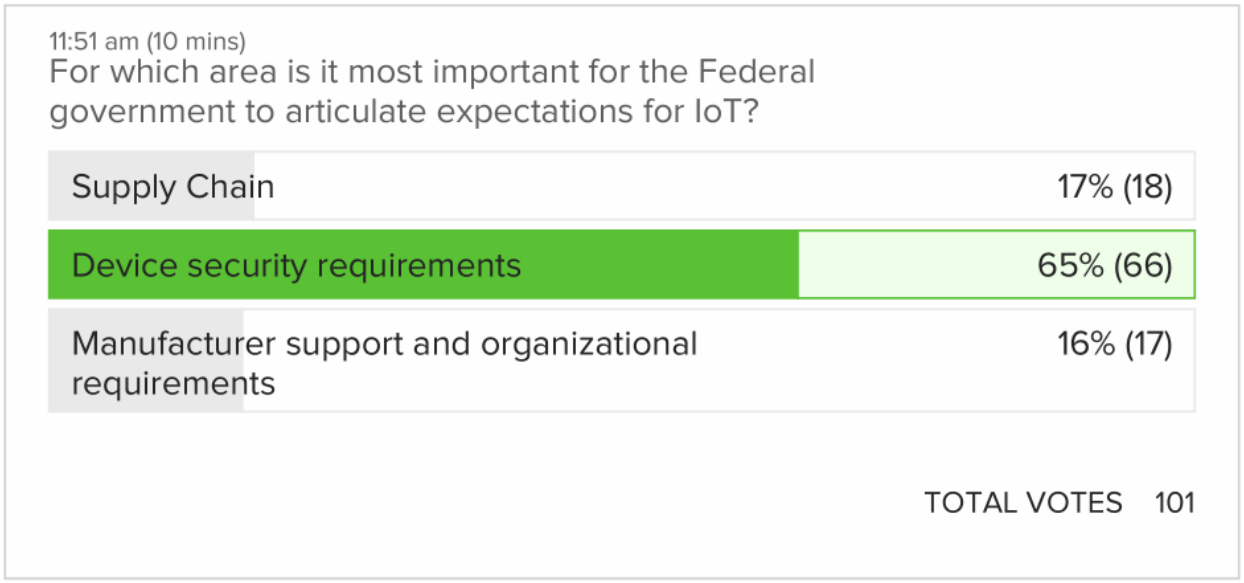
[Workshop] National Institute of Standards and Technology (2020) *Building the Federal Profile For IoT Device Cybersecurity: Next Steps for Securing Federal Systems*. Available at https://www.nist.gov/news-

events/events/2020/07/building-federal-profile-iot-device-cybersecurity-next-steps-securing

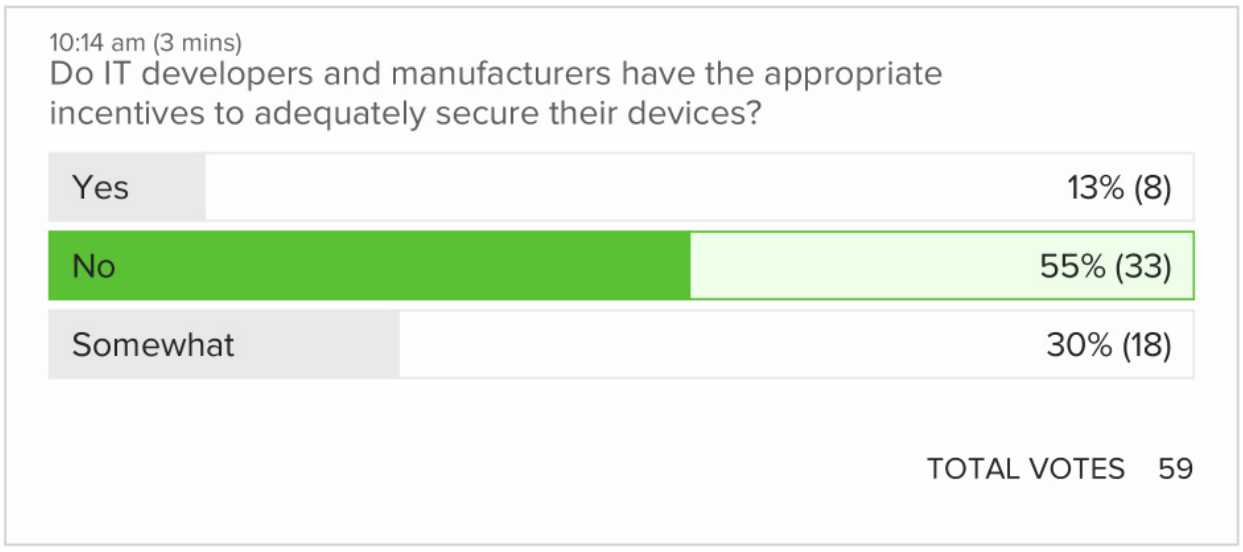
Appendix A: Poll Results

Twelve online polls were conducted during the workshop, divided equally between the two days. 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.

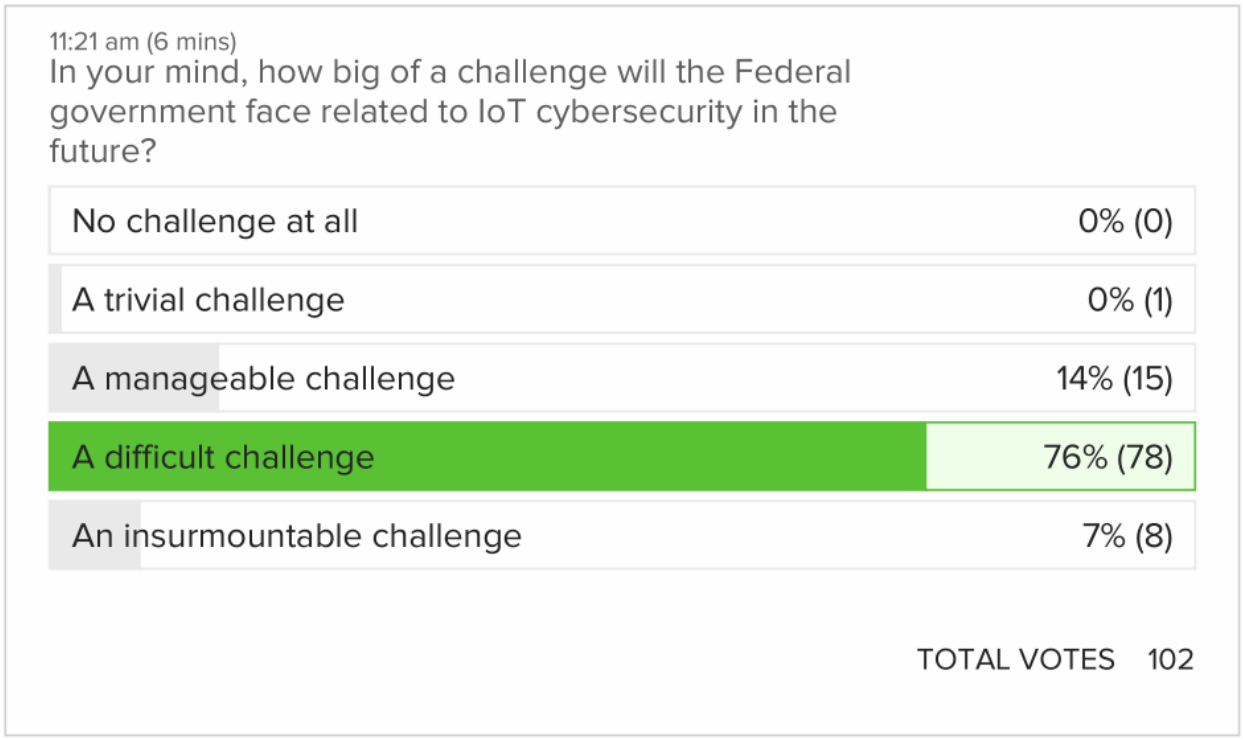
A.1 Most Important Area to Articulate Federal Expectations



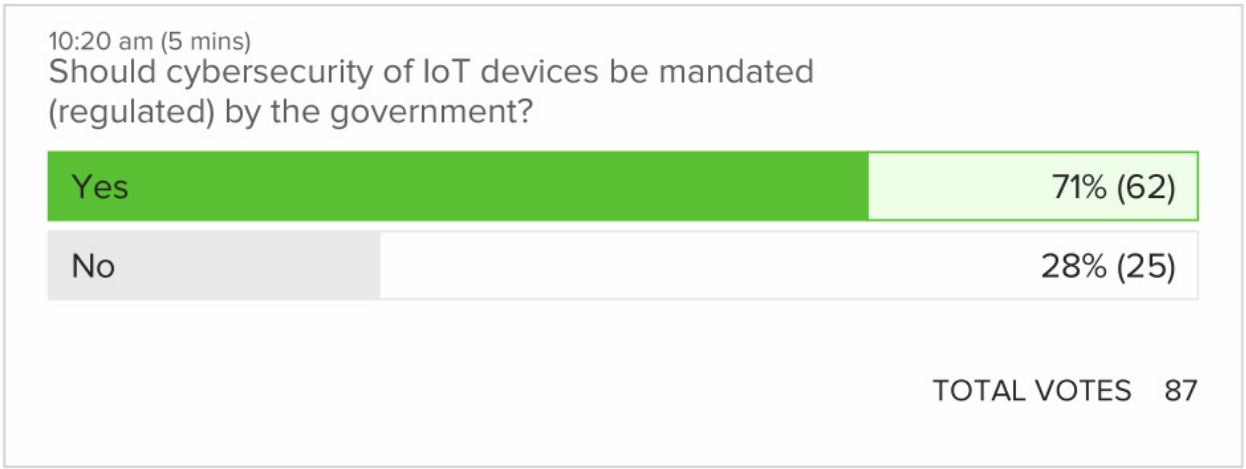
A.2 Appropriate Manufacturer Incentives for Adequate Security



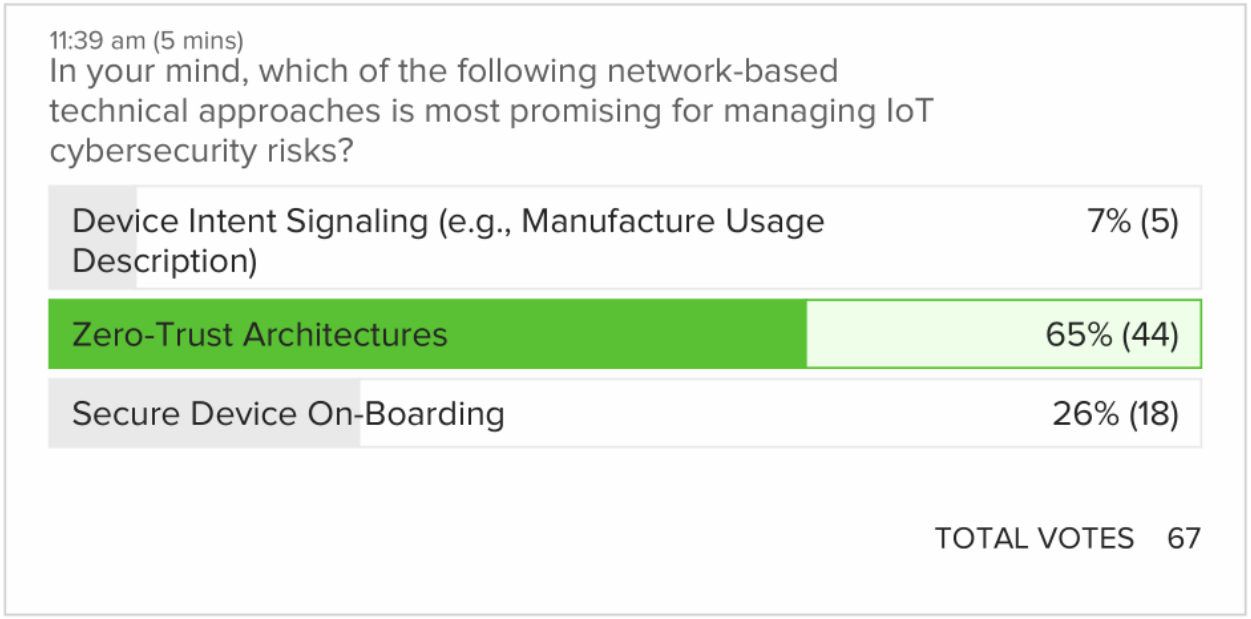
A.3 Level of Federal Challenge for IoT Cybersecurity



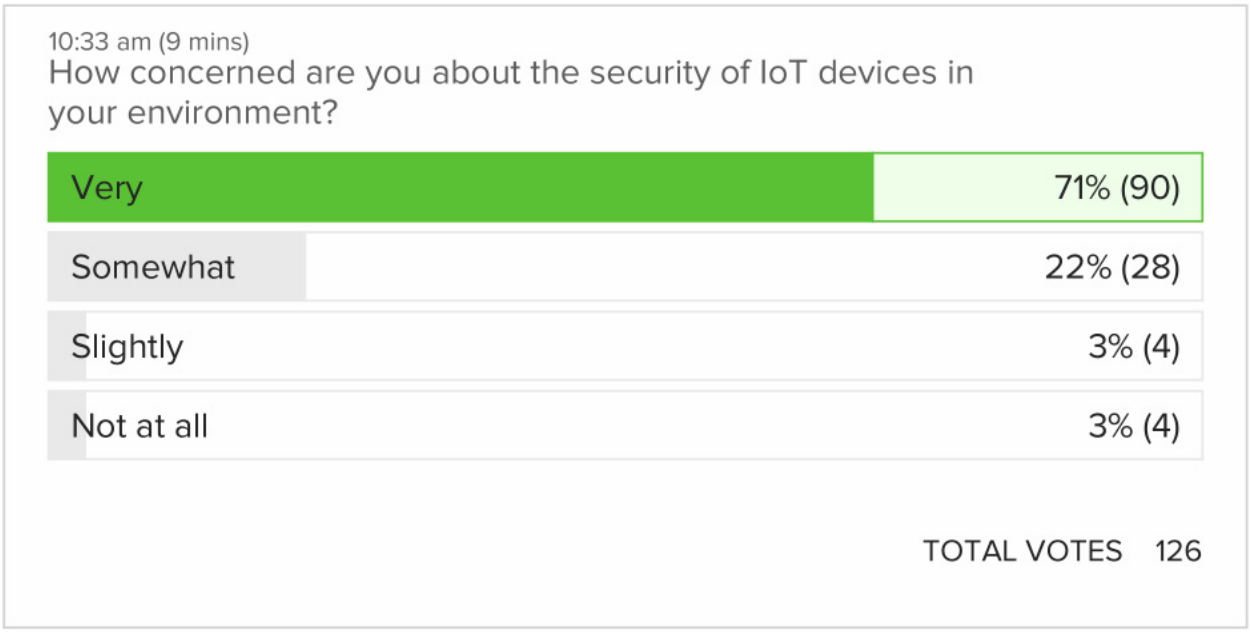
A.4 Should Government Mandate IoT Device Cybersecurity



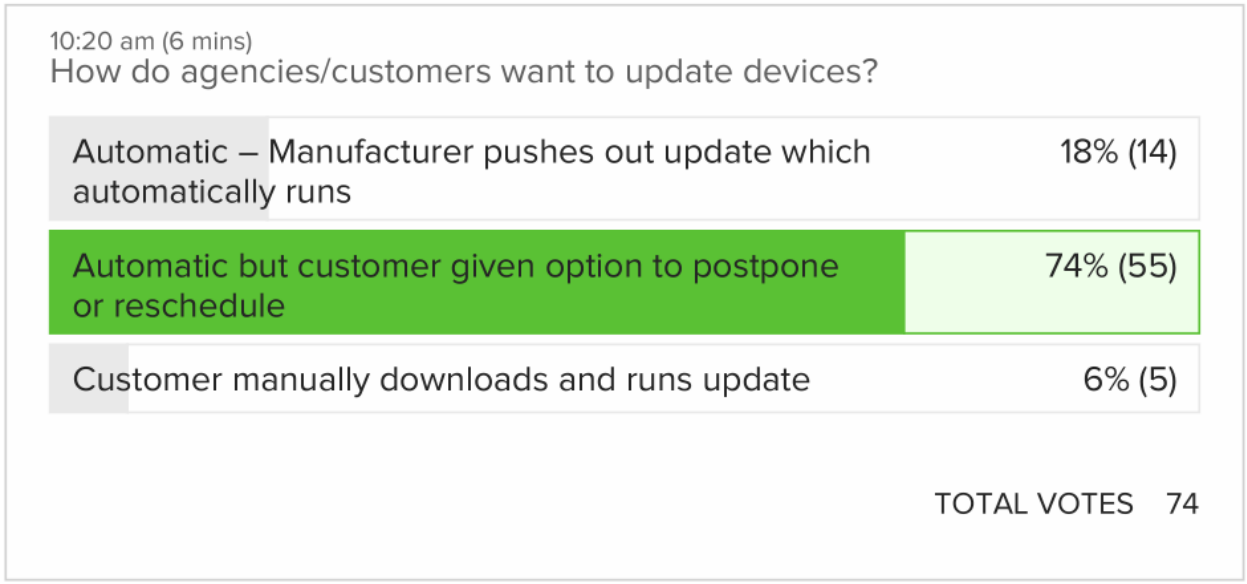
A.5 Most Promising Technical Approaches for Managing IoT Cybersecurity Risks



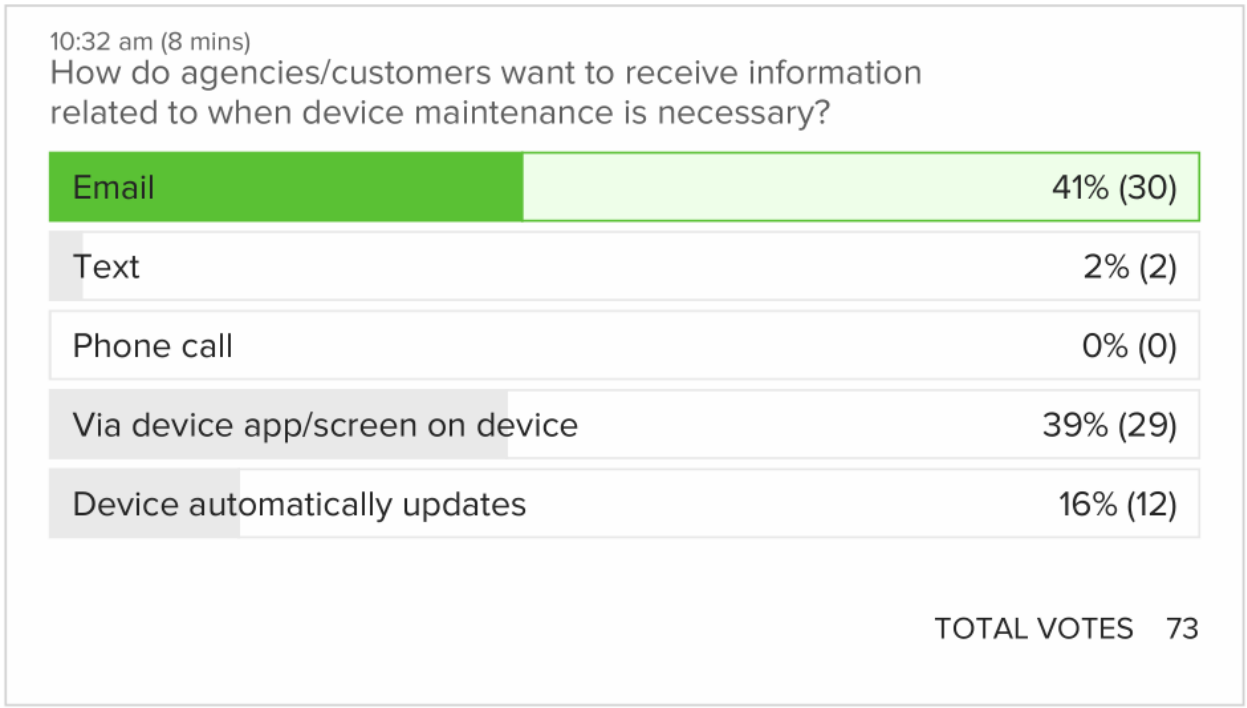
A.6 Level of Concern Regarding Security of IoT Devices



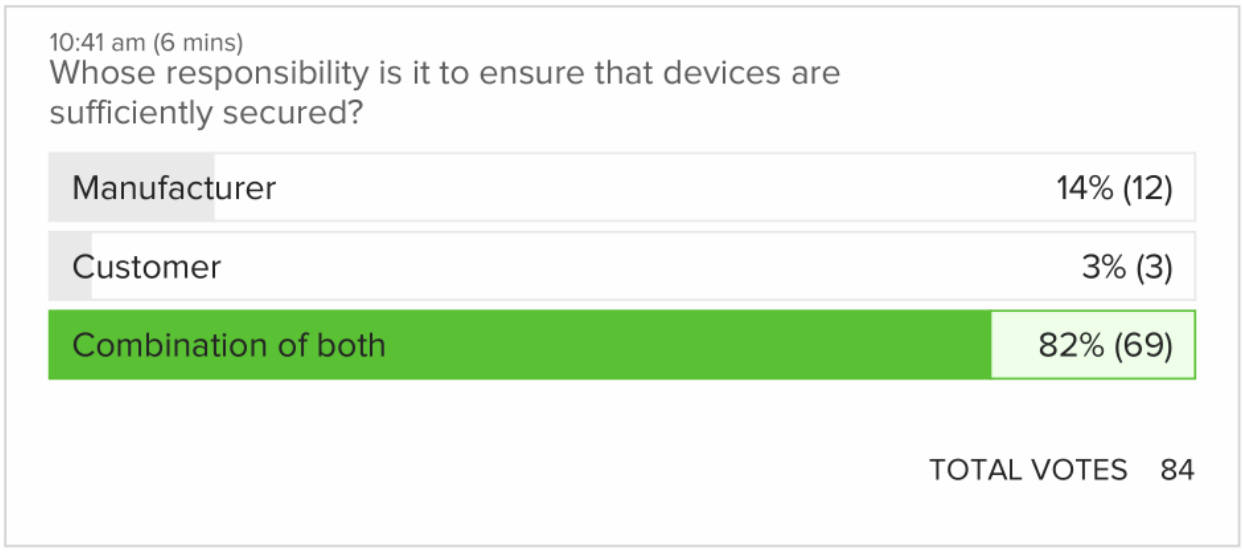
A.7 Preferred Management of Device Updates



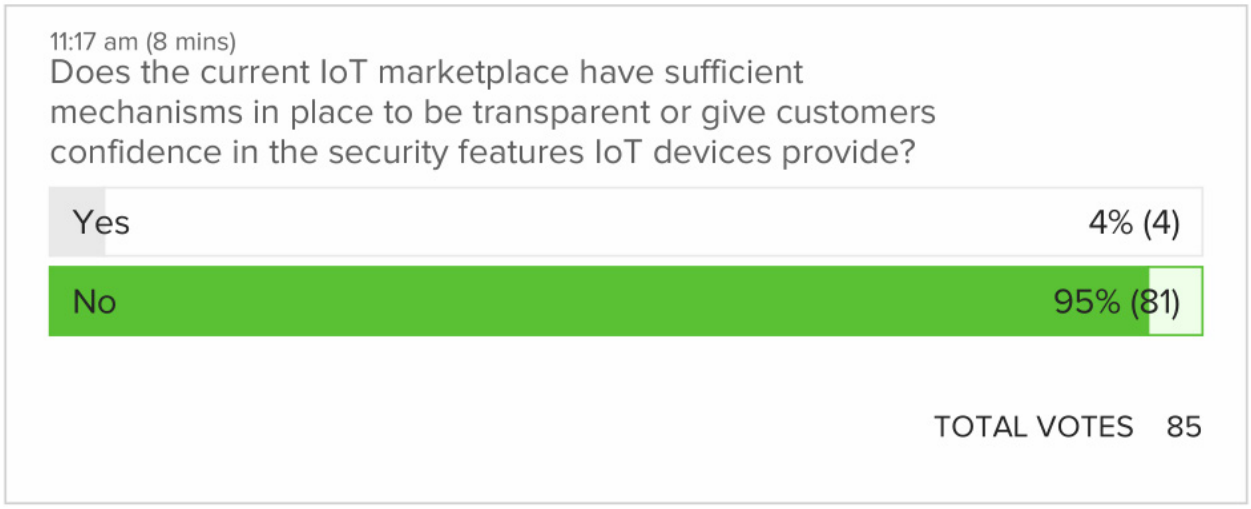
A.8 Receiving Information Regarding Device Maintenance Needed



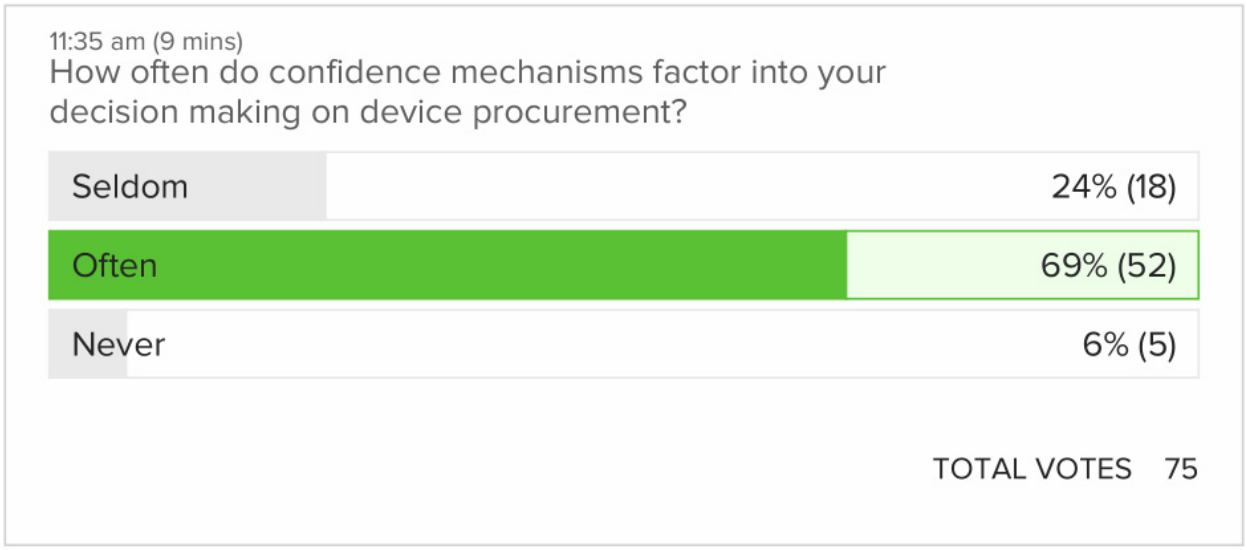
A.9 Responsibility for Device Security



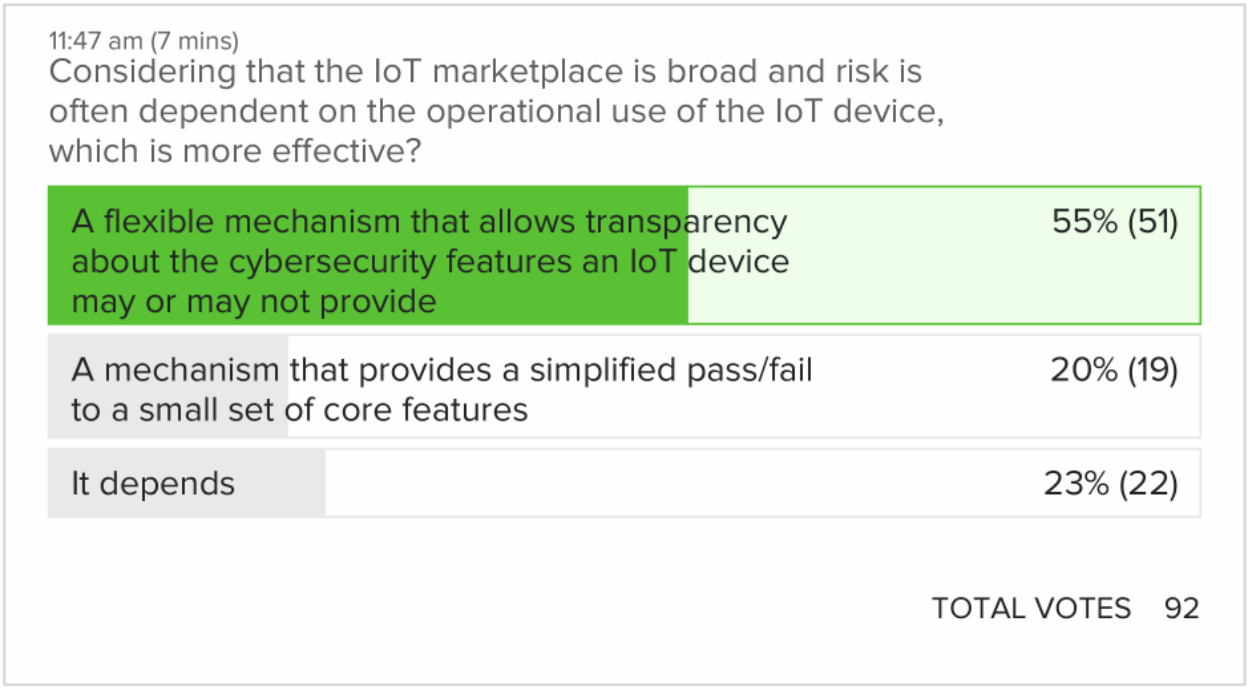
A.10 Customer View of Marketplace Transparency / Confidence



A.11 Importance of Confidence Mechanisms for Procurements



A.12 Most Effective Approach to Manage Risk



Appendix B: Acronyms

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

5G	Fifth generation technology standard for broadband cellular networks
BRSKI	Bootstrapping Remote Security Key Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CTA	Consumer Technology Association
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
ENISA	European Union Agency for Cybersecurity
FASC	Federal Acquisition Security Council
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
GSA	General Services Administration
IC	Intelligence Community
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
NISTIR	NIST Interagency or Internal Report
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
MUD	Manufacturer Usage Description

NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OT	Operational Technology
RFC	Request For Comments
RMF	Risk Management Framework
UK	United Kingdom
UL	Underwriter's Laboratories