Internet of Things Security Acquisition Guidance

Information Technology Sector

CISA
CYBER+INFRASTRUCTURE

INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL

INFORMATION TECHNOLOGY GOVERNMENT COORDINATING COUNCIL

Table of Contents

Foreword

As the Sector-Specific Agency for the Information Technology Sector, the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) prepared this document with a working group composed of members of the Information Technology Government Coordinating Council (GCC) and the Information Technology Sector Coordinating Council (SCC) to help stakeholders incorporate security considerations when acquiring Internet of Things devices[1], systems, and services. The working group serves under the auspices of the Critical Infrastructure Partnership Advisory Council established by the Secretary of Homeland Security under the authority provided by 6 U.S.C. § 451.

This document highlights areas of elevated risk resulting from the software-enabled and connected aspects of Internet of Things technologies and their role in the physical world. It provides information on certain vulnerabilities and weaknesses, suggests solutions for common challenges, and identifies factors to consider before purchasing or using Internet of Things devices, systems, and services.

The recommendations in this document are designed to improve the effectiveness of supply chain, vendor[2], and technology evaluations prior to the purchase of Internet of Things devices, systems, and services. Adoption of these recommendations by all organizations will help strengthen the Nation's cyber resilience[3] by ensuring the cybersecurity of Internet of Things technologies is addressed throughout the acquisition lifecycle.

Ms. Helen Jackson
Chair
Information Technology Government Coordinating Council
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Mr. John Miller
Chair
Information Technology Sector Coordinating Council
Critical Infrastructure Partnership Advisory Committee

[1] See Appendix A – Glossary for definition.
[2] See Appendix A – Glossary for definition.
[3] See Appendix A – Glossary for definition.

Preface

This document provides recommendations to the acquisition function[4] of an organization about how to apply cybersecurity and supply chain risk management (C-SCRM) principles and practices throughout the acquisition lifecycle when purchasing, deploying, operating, and maintaining Internet of Things (IoT)[5] devices, systems, and services. As an informative document, there are no specific requirements or "normative language", but the information herein can be used to assist in determining requirements based on organizational needs and applicable constraints.

This document is the first in a series of C-SCRM documents to be published by DHS, serving in its role as the IT Sector Specific Agency, and the Sector Coordinating Councils. Subject Matter Experts (SMEs) selected from across the Federal Government and the Information Technology (IT) industry through the public-private partnership contributed to the collaborative development process to create this document.[6]

Acquisition teams face a significant challenge in addressing cybersecurity in the acquisition process because of the rapid, continuous, sometimes inconsistent evolution of features of technology, and the resulting absence of complete information about changes in the configuration (i.e. software upgrades) of IoT technologies. The dynamic role which software[7] and connectedness play in IoT devices, systems, and services provides important functional benefits, but may also carry risks to security, safety, privacy reliability, and resiliency. It is very important during the acquisition of IoT technologies to ensure the acquisition team includes (or minimally, consults with) network security professionals and other technical experts to account for these inherent security concerns and other risks.

Cybersecurity is one of several priorities in an acquisition. At times, policies or priorities guiding acquisition activities may have conflicting directions; however, the importance to national and economic security, in addition to ensuring an organization's information or assets are safeguarded, compels organizations to address C-SCRM as a high priority consideration for enterprise risk management and as a core requirement in acquisitions that present cyber risks.

The rapid increase of IoT devices, systems, and services used by organizations allow new opportunities for efficiently conducting business operations but may also introduce additional challenges. When deployed, many IoT technologies connect to enterprise networks, for the

[4] Hereafter, all acquisition functions of an organization will be referred to as "acquisition team".
[5] For the purpose of this guide, the working group used "IoT" as defined in DHS' *Strategic Principles for Securing the Internet of Things (IoT)*: *"*The connection of systems and devices with primarily physical purposes (e.g., sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems." Available at https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf. Hereinafter, for ease of reading, the phrase "IoT devices, systems, and services" is used interchangeably with the terms "IoT," "IoT technologies," or "IoT technology."
[6] Appendix B contains a list of the working group members.
[7] See Appendix A – Glossary for definition.

purpose of generating and using data which can provide insights into physical operations within the organization using them. Because the IoT technology uses a network that may be fully connected to other parts of the organization, a single exploited[8] vulnerability[9] within an IoT technology can lead to other connected IT systems and services becoming compromised.

Gaining a better understanding of the risks that IoT can present – and how to address those risks - is an area where more education and training is needed for our workforce and leadership. The types and architectures of IoT technologies are diverse and sometimes complex, making it difficult to know what security requirements should be and how best to evaluate security features and their impacts on network operations and security. There is broad recognition of the need for specialized training and education about IoT technologies for acquisition teams. Training should provide a basic understanding about the structure and complexities of IoT technologies, so acquisition teams are better equipped to consider the risks and how to coordinate with the appropriate SMEs within the organization during the planning, assessment and decision-making processes for acquisition and use of IoT technologies. Acquisition team members should make risk-informed decisions when procuring, deploying, using, and sustaining IoT devices, systems, and services. Team members need to be clear about the intended purpose and use of the IoT technology, the operating environment in which it will be deployed, and how it will be maintained. Understanding this information is essential to being able to define security requirements and controls, and the ability to assess whether the IoT technology's security features and configurations are acceptable.

By adopting the recommendations in this document, acquisition teams will send a demand signal for improved cybersecurity in IoT technologies to sellers and manufacturers of IoT technology. In turn, by adopting these recommendations, the vendors and manufacturers of IoT technologies will be able to objectively demonstrate increased value to buyers.

[8] See Appendix A – Glossary for definition.
[9] See Appendix A – Glossary for definition.

Executive Summary

Organizations of all sizes, types, and across all sectors are often highly dependent on vendors or integrators to deliver Information and Communications Technology (ICT) products and services - and increasingly Internet of Things (IoT) technologies - to support their operations and to accomplish their business objectives. While advances in technology and integration of it into every aspect of the modern world have led to significant improvements in security and economic prosperity, the same technology that has made our lives better has also introduced new security risks.

As an example, one of these new security risks arises from software vulnerabilities. As technology has evolved, software and software-enabled functions embedded in ICT and IoT technologies have become integral to virtually all mission and business capabilities. Yet, because software is intangible and complex, evaluation of software security is often given inadequate attention in the acquisition process. Yet, poorly written code, or a malicious insertion of a backdoor into the software could introduce an undiscovered risk to an enterprise. This risk provides a prime example of the importance of comprehensively evaluating the supply chains of ICT and IoT technologies before buying and deploying them.

There are a wide range of risks that can be introduced during the purchase and use of ICT and IoT technologies, and many ICT and IoT risks are similar. However, many of the risks introduced by IoT devices, systems, and services are different from those introduced by ICT, and these unique risks are not widely understood and are often not addressed by IoT buyers, vendors, or manufacturers. Therefore, this document focuses on IoT technology risk and how to adequately address it throughout the acquisition lifecycle.

Opportunities to address cybersecurity when purchasing IoT technologies begin during the planning phase and occur throughout the acquisition lifecycle. Important IoT technology security considerations include, but are not limited to, poor design (use of plaintext and hard-coded passwords[10]), coding flaws (buffer overflows and command injection[11]), and inconsistent patching[12] of software. With the proliferation of IoT devices, systems, and services connecting to enterprise ICT networks, the introduction of new potential vulnerabilities (both known and unknown) increases security risks that require attention by staff purchasing, operating, and maintaining IoT technologies. Due to the physical interactivity of IoT technologies, it is also critical to consider the potential for new threats to safety and privacy enabled by connected IoT technology.

The challenges associated with connecting IoT technologies to existing systems[13] demands comprehensive and thoughtful planning to appropriately be able to manage the new and varied risks that connected IoT technologies introduce. Acquisition teams should minimally consider: the purpose of the IoT connections; associated organizational, business and functional requirements; and the arc over time of how systems will be supported and sustained.

[10] See Appendix A – Glossary for definitions.
[11] See Appendix A – Glossary for definitions.
[12] See Appendix A – Glossary for definition.
[13] See Appendix A – Glossary for definition.

This document identifies select examples of types of IoT devices, systems, and services that can present risk to an organization's functions and leverages existing best practice information [14] to provide acquisition teams with actionable recommendations for addressing IoT technology risks at each stage of the acquisition lifecycle. Information on business risk analysis, standardization, testing, resilience factors, and design is also provided to assist with addressing these broad challenges. References to various IoT-related documents can be found in the Appendix of this document, for more in-depth research needs. The purpose of this document is to inform and provide information to organizations to better assess needs and acquisition requirements.

This document focuses on the following subject matter areas:

- Cybersecurity issues to consider when purchasing IoT technologies.
- Cybersecurity issues to consider during deployment and implementation of IoT technologies.
- Recommendations for how to address cybersecurity issues of IoT technologies in each phase of the acquisition lifecycle.
- Cybersecurity considerations specific to connecting new IoT technologies to operational, developmental, and legacy systems.
- References and links to relevant standards and other resources.

The IoT marketplace offers many innovations and opportunities to enhance and streamline government and business functions. However, it is helpful if buyers exercise due care and make well-informed decisions when purchasing IoT technologies. Applying due diligence for appropriate cybersecurity throughout the IoT technology lifecycle is paramount to mitigating the spectrum of risk its use introduces to modern society.

[14] This document recognizes that smaller businesses and enterprises may face resource limitations and business constraints in taking full advantage of the proposed guidance therein. Considerations for developing guidance that more narrowly focus on smaller businesses will be explored as an addendum to this document or as a follow-on activity of the IoT Working Group.

Section 1: Overview of IoT Cybersecurity Considerations

Background

IoT devices, services, and solutions development continues to evolve to meet consumer and business demands. Given the connected nature of IoT technologies, securing the data, software, and hardware[15] which enable its fundamental functionality remains imperative for ensuring an organization can meet its operational needs and objectives. All purchasers of IoT devices, systems, and services, face significant challenges evaluating and validating available security options and integrating them with other IoT technologies or existing ICT within the enterprise. IoT technologies offer many innovations and opportunities to enhance and streamline business functions. At the same time, IoT technologies are also ICT, and thus present some of the same risks and require similar protections as ICT. Buyers' due diligence when procuring IoT technologies and addressing the potential impact the IoT technologies proposed for use are critical for safety, privacy, reliability, resiliency, and security.

The acquisition and deployment process for IoT technologies may be described as compound and needs to be adaptive to dynamic environments. Not only is the underlying infrastructure where IoT technologies will be deployed frequently in a state of continuous change, but the acquisition process and deployment of the technologies itself is often an agent of change in the operating environment. It is important to consider the specific function or activity supported by the IoT technology and what risks the IoT technology's software-enabled and connected nature could present to the organization if that capability were to be compromised in some way.

Consequently, prior to purchasing any IoT devices, systems or services, the purchaser and contracting or acquisition staff, working with their acquisition team members from network security and risk management need to know the cybersecurity issues that staff consider important for protecting assets and data, as well as any other risks the IoT technology could introduce to the agency's mission, workforce, and user community.

General Cyber Risks

IoT devices, systems, and services are susceptible to many of the same security challenges faced by ICT systems such as vulnerabilities introduced during design, manufacturing, implementation, configuration and disposal. Some of the vulnerabilities that have been reported as affecting IoT devices, systems, and services range from those attributable to design choice (e.g., use of plaintext and hard-coded passwords), to coding flaws (e.g., buffer overflows and command injection), denial-of-service[16], and susceptibility to malware or ransomware due to missing or improper security patching. In general, many of the same vectors of attack to ICT exist within IoT technologies.

[15] See Appendix A – Glossary for definition.
[16] See Appendix A – Glossary for definition.

Interconnection with Existing ["Legacy"] Systems

Many legacy Information Technology (IT) and Operational Technology (OT) systems were not designed for operation over the Internet. When these technologies are integrated with newer IoT devices, systems, and services new security controls may need to be implemented. Legacy systems often require expansion or part replacements to integrate with IoT technology and may not be easily converted at a reasonable cost. In certain cases, updates to legacy systems may require having a technician physically work with every individual device in the system. In other instances, a legacy system cannot be updated and would need to be replaced. Systems under development and in operation can accept connection to IoT devices but gaps in security controls may not be knowable without extensive regression testing[17]. Many IT departments, especially within smaller organizations, are not adequately prepared to address these challenges. Consequently, when purchasing IoT technologies, acquisition teams should closely coordinate with the requiring office or end user to ensure appropriate risk management decisions are made throughout the process. Coordinated efforts between IT and procurement staff prior to making acquisition decisions will help ensure these issues with legacy systems are addressed during planning and requirements development and contract administration, as detailed in Section 3.

Assessing Criticality of Technology

In the world of finite resources, it is not possible to apply equal protection to all assets. When purchasing and deploying IoT technologies, acquisition teams should use a structured method of prioritizing programs, systems, and components based on their importance to the goals of the organization and the impact that their inadequate operation or loss may present to those goals. A criticality analysis helps organizations identify and better understand the systems, subsystems, components, and subcomponents that are most essential to their operations and the environment in which they operate. That understanding facilitates better decision making related to the management of an organization's information assets, including information security and privacy risk management, project management, acquisition, maintenance, and upgrade decisions.

The National Institute of Standards and Technology Internal Report (NIST) 8179[18] provides a comprehensive Criticality Analysis Process Model the acquisition teams can use to ensure criticality assessments are conducted with appropriate discipline and rigor.

IoT References

While guidance and standards for IoT are still being developed and are evolving, there are numerous available reference documents that can be leveraged and help organizations to develop risk management strategies and practices to address IoT cybersecurity risks. See reference list, provided at the end of this document.

[17] Regression testing is re-running functional and non-functional tests to ensure that previously developed and tested software still performs after a change. https://en.wikipedia.org/wiki/Regression_testing.
[18] Available at, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf.

Cybersecurity Framework (CSF)

The Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders. Organizations can use the CSF to integrate and align cybersecurity and acquisition processes. For example, offerors can leverage the CSF to develop target profiles to aid in the preparation of their responses to contract solicitations for IoT technologies. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization. Use of the CSF in the acquisition process is a nascent practice, and its utility in providing a common way to communicate cybersecurity requirements in contracts is promising.

More information about the CSF can be found at: https://www.nist.gov/cyberframework.

Using CSF in the Acquisition Lifecycle

Use of the CSF during the acquisition lifecycle can be a straightforward way for the requiring activity and contracting entity to develop cybersecurity requirements and communicate the requirements to prospective offerors. The CSF provides a common way to communicate cybersecurity activities and facilitate collaboration between requiring activities, contracting entities, and contractors when developing contract cybersecurity requirements. Section 2 of this document provides information about incorporating cybersecurity of IoT technologies into the acquisition lifecycle.

By following the security recommendations in this document, purchasers can limit the risks associated with introducing IoT technologies into the organizational environment. Risk management strategies differ between organizations, so this document does not provide a one-size-fits-all checklist of security requirements; rather, it provides suggestions for how to engage vendors and stakeholders and mitigate risks throughout the acquisition and deployment lifecycles.

The IoT technology considerations addressed in this document can help inform planning and actions taken by acquisition teams and drive interactions between contracting entities and IT security teams to ensure acquired IoT devices, systems, and services are aligned with an organization's risk management strategy.

Following are some potential key considerations for the purchase and use of IoT technologies. Section 3 of this document maps each IoT issue to the acquisition lifecycle and provides recommended actions and steps.

IoT Device Baseline Security

"Baseline" – or certain minimum – device and organizational capabilities are identified as a starting point for ensuring the security of IoT technology. Establishing a "baseline" of what is minimally acceptable with regard to security of IoT can serve as an invaluable resource to both acquirers and providers when determining whether an IoT technology will satisfy an organization's security requirements. As an example of such a baseline, NIST has published the

Draft NIST Interagency Report 8259[19] (NISTIR 8259) "Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers." Another baseline resource is the "C2 Consensus on IoT Security Baseline Capabilities," [20] developed and published by the Council to Secure the Digital Economy (CSDE). Both documents include lists of capabilities for organizations to consider.

Using IoT Device Security Baselines in the Acquisition Lifecycle

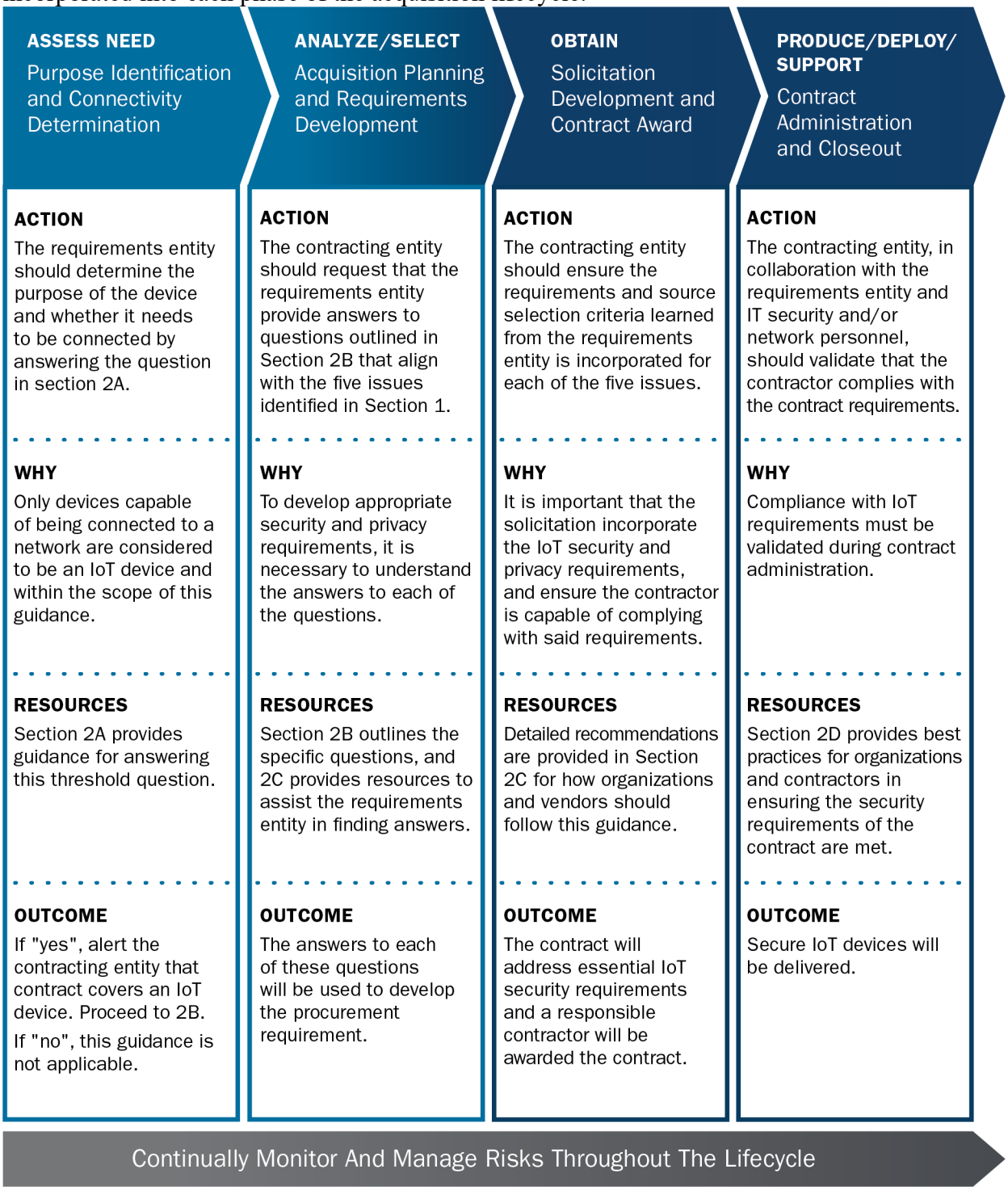
Like the CSF, a "baseline" can help the organization to develop and communicate requirements to prospective offerors and provides a starting point for building upon the baseline set of requirements as appropriate. Baselines provide a means to communicate important device specifics in common language. Information in the Baseline documents explains when and why the organization should consider a Baseline capability for a device type. To learn more about how to leverage IoT device security baselines, reference the documents mentioned above.

[19] NIST, Core Cybersecurity Feature Baseline for Securable IoT Devices, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf

[20] CSDE, The C2 Consensus on IoT Security Baseline Capabilities, https://securingdigitaleconomy.org/projects/c2-consensus/

Section 2: Acquisition Lifecycle Considerations

This section maps each IoT issue outlined in Section 1 to the acquisition lifecycle and provides recommended actions and steps. The graphic below summarizes how these issues are incorporated into each phase of the acquisition lifecycle.



2A: ASSESS NEED

Overview

- **Action:** The requirements entity should determine the purpose of the IoT technology and whether it needs to be connected to the Internet by answering the questions in Section 2A.
- **Why:** Network connectivity introduces specific cybersecurity risks and the purpose for and method of the connection informs what the applicable security controls should be.

Threshold Question			
This is a baseline question to ensure connectivity is necessary/desired for mission.			
	Question	Expected Answer	Resources/Additional Information
1	For what purpose is the device being procured?	Detailed description of device purpose and potential risk	• NIST Cybersecurity for IoT Program • The Internet of Things: An Overview on How to Acquire "Things" Securely
2	Is the device intended to be connected?	Yes or No	Connection is not limited to persistent connections over airwaves or wire (copper/fiber) but also includes routine sharing of removable media between the device and enterprise-connected systems. Exceptions might be infrequent, one-way transfers of data from networked systems to devices for the purpose of updates/upgrades of electronic components. Even this requires risk assessment and approval.
3	Is there a need to assure post-acquisition compliance with IoT-based security requirements or evaluation considerations?	Yes or No	Organizations should consider a life-cycle based approach to ensuring that IoT security controls are in place prior to installation and effective during operational use.

2B: ANALYZE/SELECT

In the tables below, key Questions are indicated with the form of the Expected Answer. Some Sample Requirements are also provided; however, note that these are not intended to be used directly. It is noted in the table that actual answers will differ based on organization needs; the intent is for these requirements to be developed by the acquisition team.

Overview

- **Action:** The contracting entity should request the requirements entity answers the questions outlined in Section 2B that align with the issues identified in Section 1.
- **Why:** In order to develop appropriate security requirements, it is necessary to understand the answers to each of the questions.

Type and Control of Connectivity			
Overview: Often for security reasons, an organization would want to turn off or limit connectivity or segment the local network. It is important that if this is the case, the device still functions or at least functions in the way necessary to fulfill the organization's operational or business need.			
	Question	Expected Answer	Sample Requirement (actual answers will differ based on organization needs)
1	Are there specific types of network assets[21] the device needs to be connected to for operation? (Public Internet, organization only network, other devices, etc.)	Type of network asset to which the device is expected to be connected	N/A
2	Does connectivity need to be able to be turned off?	Yes or No	Connectivity must be capable of being disabled.
3	Does the device need to function without connectivity?	Yes or No	Devices must be capable of functioning without connectivity.
4	Is it acceptable if the device functions differently without connectivity?	Yes or No, description of acceptable parameters of functional limitations	Device must be able to provide basic functionality without connectivity.
5	Does the device need to maintain partial functionality, through local segmentation on a network?	Yes or No	Device must maintain partial functionality even if on a segmented network.

[21] See Appendix A – Glossary for definition.

Third-Party Service and Data Management			
Overview: IoT technologies often require additional services to properly function. These services may be included in the acquisition of the ICT or may be procured separately. If sensitive or protected privacy information is intended to be collected, processed, stored, or transmitted by the technology, it is important that organizations conform to their own internal policies or applicable legal or regulatory requirements.			
	Question	Expected Answer	Sample Requirement (actual answers will differ based on organization needs)
1	Does the IoT device/service/solution require support from or use of an outside (third party or external) service to function?	Yes or No, description of third-party service	N/A
2	How does the data collected from the device need to be governed? Are different types of data involved?	Description of data governance requirements, parameters	The following types of data will be collected through this acquisition: protected privacy information and business proprietary information. This data must be governed in accordance with applicable policy, law, requirements, etc.
3	Where and how does the data need to be stored?	Description of data storage requirements, parameters	This data must be stored in accordance with applicable policy, law, requirements, recommendations, etc.
4	Who should have access to as well as ownership of collected data?	Description of data access/ownership needs, parameters	Data generated by this device will be owned by the procuring organization. Data access will be granted to the contractor and subcontractors for patching and maintenance only.
5	Will the device collect privacy protected or sensitive information?	Yes or No, description type of data to be collected and data management needs and parameters regarding that data	This device is expected to collect Personally Identifiable Information (PII), which will be managed in accordance with applicable policy, law requirements, etc.
6	If the device requires servicing by a third party, will the contractor be responsible for risks associated with that third-party?	Yes or No	The Contractor is responsible for ensuring requirements are met by any subcontractor or third-party vendor that services this device.
Patching			

Overview: The ability to patch a device to mitigate against identified vulnerabilities is important. A particularly important consideration is the length of patching service available by a vendor (or manufacturer) in comparison to the expected lifecycle of the technology. In some instances, a product may not have the capability to be patched.			
	Question	Expected Answer	Sample Requirement (actual answers will differ based on organization feedback)
1	Does the device need to be patchable or upgradable?	Yes or No. If no, justification needs to be given as to why.	The device must be patchable.
2	How long is the device expected to be in operational use (i.e., For what length of time will it need to be patched?	Date ranges for expected device lifecycle	The device must be serviced with regular security patches for a minimum of five years from the start of the contract.
3	Is the needed use of the device potentially longer than the period in which it will likely be serviced? If yes, what are the options to maintain the device?	Yes or No.	If the contractor is unable to service the device for the full five years, a subcontractor or third-party vendor must be required to service the device for the remaining time.
4	Is a specific path or technique required to receive and apply patches? Does this require direct Internet connectivity?	Description of patching path/technique required	The device must be patchable only through authenticated, over-the-air, updates.
5	What are the necessary responsibilities of the user and/or enterprise manager, and what are the necessary responsibilities of the manufacturer and/or service provider with regard to patching?	Description of required roles and responsibilities	The contractor is required to provide regular security patches over the air. Organizations should ensure proper functionality post-patch and to follow-up with the contractor to resolve any issues.
General Vendor Cybersecurity Practices			
Overview: These questions address general practices of the vendor that can help to ensure that the technology was designed securely. A secure development lifecycle typically refers to standard processes in which security is considered from design to end of life for the technology. Vulnerability disclosure programs enable a clear way for external researchers to			

make the vendor or servicer of the device aware of possible vulnerabilities, as well as a means for the vendor to self-report vulnerabilities. Fail-safe mechanisms are important backstops if a security incident occurs, as the system's design prevents or mitigates unsafe consequences of the system's failure. A supply chain risk management program is particularly important for technologies used in sensitive areas or when there will be access to sensitive data. Work is ongoing to advance these practices.			
Question		Expected Answer	Sample Requirement (actual answers will differ based on organization feedback)
1	Is evidence of a secure development lifecycle required or helpful?	Yes, to one or the other, or No. If yes, could be included as requirement or an evaluation factor.	A secure development life cycle is required and specified in acquisition-related requirements.
2	Do you require reporting of or response to vulnerability disclosures?	Yes or No. If no, could be an evaluation factor.	A vulnerability management program is required.
3	In the event of a security incident, are fail-safe mechanisms required?	Yes or No. If no, could be an evaluation factor.	The contractor is required to document and deploy fail-safe mechanisms in the case of a security incident.
4	Is a supply chain risk management program required?	Yes or No. If no, could be an evaluation factor.	A supply chain risk management program is required.
Security of Device and Communications			
Overview: Authentication (you are who you say you are) and access (you are authorized to view or do something) are important aspects of keeping technology manageable and secure. Considerations about how to address both of these need to be integrated into the user's IT infrastructure and management and operational practices. Encryption[22] is a way data is kept secure and can be applied at the device-level for data "at rest" as well as when data is being communicated over networks (data "in transit"). Depending on the risk profile of the device as well as the sensitivity of the data, encryption may be required. Keeping track of devices, to include their firmware and software types and versions, will help in being able to more rapidly and appropriately respond if and when there is a security incident.			
Question		Expected Answer	Sample Requirement (actual answers will differ based on organization feedback)
1	How does the device need to handle authentication?	Description of authentication needs	Devices must be authenticated through two-factor authentication with no hard-coded passwords.

[22] See Appendix A – Glossary for definition.

2	How does access to the device need to be managed?	Description of access management needs	Device access must be manageable in accordance with applicable policy.
3	How does the device need to be authenticated on the network?	Description of network authentication needs	Device network authentication must be managed in accordance with applicable policy.
4	Does the solution need to use encryption to protect data? Data stored on the device? Transmitted over the network?	Description of encryption needs	Data must be encrypted at rest and in transit in accordance with applicable policy.
5	What form should encryption keys take, are they securely stored, and do they need to be rotated?	Description of key needs	Encryption keys must be rotatable and should be created in accordance with applicable policy.
6	How do channels between components of the IoT solution need to be secured?	Description of secure channel needs	Communication between IoT components must be secured through applicable encryption standard.
7	Do IoT devices and the software and firmware of each device need to be tracked. If so, how?	Description of tracking needs	Software and firmware of the device must be trackable by the network manager in accordance with applicable policy.
8	How do the software components need to be logged and audited?	Description of logging and auditing needs	Device components must be loggable, and these logs must be auditable in accordance with applicable policy.
9	Does automated or continuous monitoring need to be provided, and how?	Description of monitoring needs, if applicable	Contractor must provide automated monitoring of the device in accordance with applicable policy.
Additional Considerations			
Overview: This section covers additional considerations not addressed above.			
Question		Expected Answer	Sample Requirement (actual answers will differ based on organization needs)
1	Given the risk posture of the organization, are there any other security considerations that need to be incorporated into the requirements documentation?	Additional requirements	Device must include physical security controls in accordance with applicable policy.

2C: OBTAIN

Overview

- **Action:** The contracting entity ensures the requirements and source selection criteria incorporate the information learned from the requirements entity, for each of the issues.

    - Changes to the contract requirements to comply with the standard practices of the contracting entity such as the use of boilerplate language that changes the wording of the requirements or selection criteria must be approved by the program submitting them. Even small changes in requirements descriptions can have significant unintended consequences.
    - Taxonomies and terminologies developed by industry-recognized standards bodies, particularly those associated with cybersecurity and safety, should be used exclusively.

- **Why:** It is important that the solicitation incorporates IoT security requirements and ensures the contractor understands and is capable of complying with the requirements.
- **Resources:** Section 2C provides information on how organizations and vendors can follow this recommendation.
- **Outcome:** The contract will address a core set of essential IoT security requirements and a qualified contractor will be awarded the contract.

Requirements

The answers provided in Section 2B should be used to help develop the IoT security requirements for the solicitation. Minimally, a procurement of an IoT technology should identify the requirements for the following topics:

I. Type and Control of Connectivity
II. Third-party Service and Data Management
III. Patching
IV. General Vendor Cybersecurity Practices
V. Security of Device and Communications
VI. Additional Considerations

To make the expectation clear to the vendor and to facilitate a clear and complete response back from the vendor, the requirements should be topically organized, based on these categories. If there are no requirements for a specific category, the statement of work should state clearly that there are no requirements. It is important to clarify within the requirements language whether a security practice or standard is a requirement or only a suggestion. It's also important to identify the different factors that will be considered when evaluating different offers.

Pre-award Deliverables

The solicitation should also identify whether pre-award or post-award deliverables (e.g., product specifications, documentation of offeror cybersecurity practices) must be provided. A pre-award deliverable should only be required by the contractor if such a deliverable is necessary for the contracting activity to evaluate prior to award whether an offeror can meet the minimum requirements of the solicitation.

Contractor Source Selection

For complex acquisitions, it may be helpful to evaluate offerors based on their qualifications to comply with the IoT security requirements in the solicitation. Contractors can also be evaluated on whether they provide additional protection beyond the minimum contract requirements. Evaluation of IoT security can be included as a separate evaluation factor or as part of a larger evaluation factor.

Examples of IoT evaluation factors include:

- General Vendor Cybersecurity Practices: Evaluate the contractor on how they address questions tailored to the risk and mission impact of the product or service being acquired. At a minimum, have the supplier answer the following questions:
    - Do they use a secure development lifecycle and are they able to document it in their processes or procedures?
    - Do they have a vulnerability reporting and response program?
        - Can they describe the program using metrics such as the time between a bug being reported and a fix/patch release?
        - Do they actively seek to include patches and version updates of software libraries, open source software, or copyrighted software in the public domain?
    - Can they describe their supply chain risk management program?
        - Do they have alternate sources for critical components?

What are their quality standards for their suppliers such as response to bugs and defects?

- IoT Security Plan: Require the contractor to address how they will comply with the IoT security requirements of the solicitation and whether they provide additional protection beyond the minimum requirements of the contract.

2D: PRODUCE/DEPLOY/SUPPORT

Overview

- **Action:** The contracting entity, in collaboration with the requirements entity and IT personnel, should validate that the contractor complies with the contract requirements.
- **Why**: Compliance with IoT requirements should be validated during contract performance. For government agencies, this must be in accordance with Federal Acquisition Regulation Part 42.
- **Resources:** Section 2D provides best practices for organizations and contractors in ensuring the security requirements of the contract are met.
- **Outcome:** Compliant IoT devices will be delivered.

Post-Award Contractor Deliverables

During contract administration, it is important for contractors to provide any required post-award deliverables required by the contract. The contractor should request clarification from the contracting officer if they are unsure about documentation being required.

Validating Compliance

Acquisition team members should validate that documentation, including the bill(s) of material provided by the contractor, is accurate and complies with the requirements of the contract. It is important to coordinate such validation efforts with the requirements entity to ensure the requirements entity is receiving the contracted products and services.

Deployment

When deploying the IoT technology, acquisition teams should work closely with their organization's Chief Information Officer (CIO), Chief Information Security Officer (CISO), Chief Privacy Officer (CPO) or other relevant IT security personnel to meet cybersecurity compliance needs and address emerging risks.

Section 3: Examples of IoT Technology and Associated Risks

The purpose of Section 3 is to illustrate examples of IoT devices, systems, and services, highlight associated risks, and document how some attacks manifest in the context of IoT technologies. IoT technologies have many different forms and functions, ranging from common consumer-oriented products to industrial control systems[23]. All IoT technologies gain connectivity and interoperability as part of broader ICT ecosystems and rely on software and some form of connectedness for their capabilities. Some functions inherently bring greater degrees of risk than others, such as devices that contain microphones or cameras, or systems that control critical physical functions in their environment. IoT technologies often rely upon extrinsic ICT hardware and software infrastructure to properly operate.

Examples of Security Concerns Related to IoT Devices, Systems, and Services

Note: In the examples listed below, IoT technologies exist as points of vulnerability and come under attack. It should be noted that these examples involve the technology being both the target of one attack, and a launching point for another attack. This is a common event. IoT technologies have not typically been the final points of compromise; however, an attack where the goal is to influence, control, or disrupt the functionality of the IoT technology are easy to imagine and need to be considered. Many examples of such attacks have been documented by researchers and presented in public, including attacks on medical devices, building management systems, automotive systems, and critical infrastructure elements. Attackers often use the IoT technologies to gain entry into an environment as a stepping-stone to compromise other systems. This section illustrates how an IoT technology can pose risk, even when the technology's intended function is not particularly critical. Many IoT devices, systems, and services are capable of harboring the same kinds of vulnerabilities as traditional computing assets.

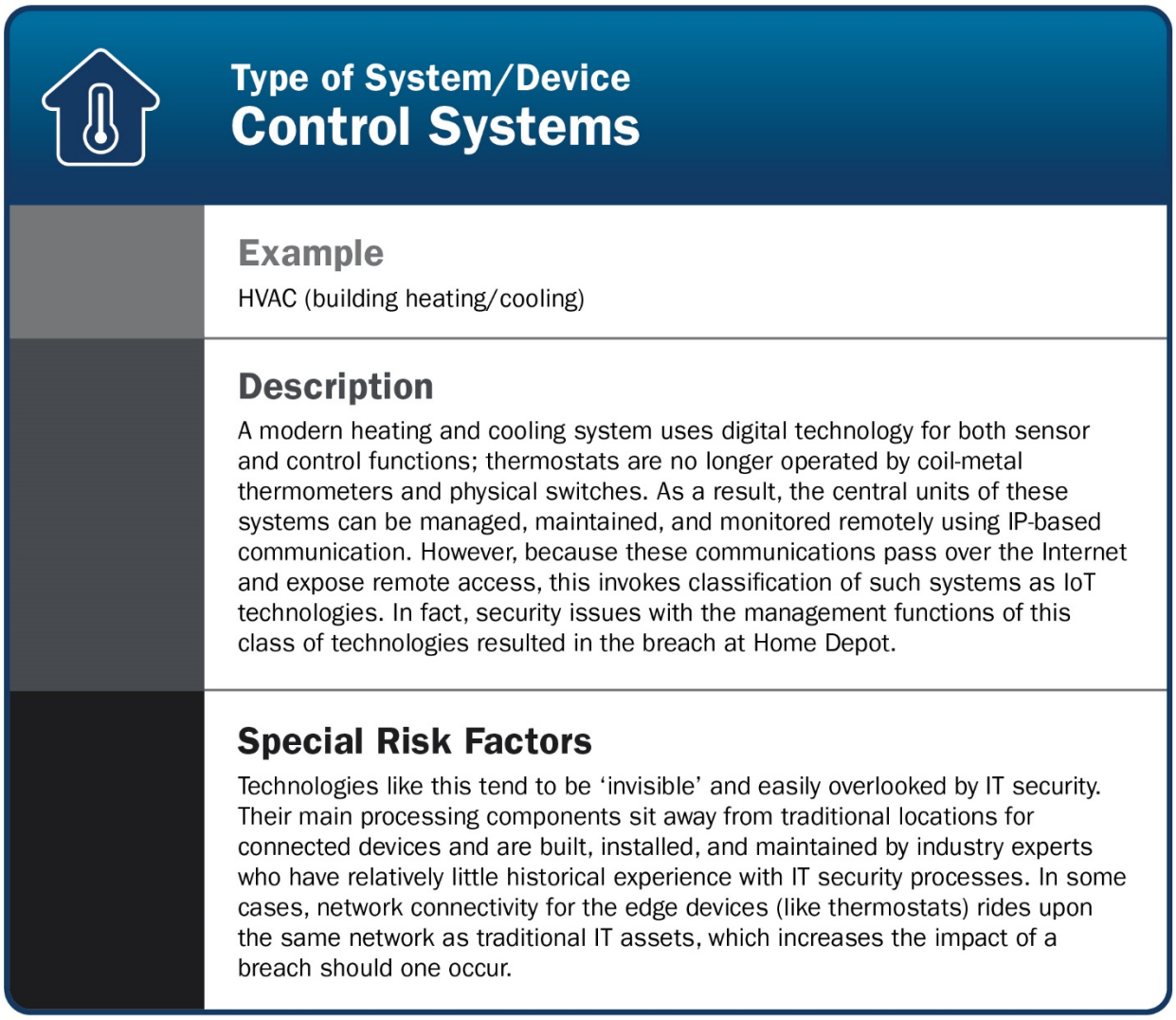
The first part of this section breaks out examples using four attributes:

- The general type of IoT technology.
- An example of such an IoT technology.
- A description of the IoT technology.
- Any special risk factors which accompany the example IoT technology.

The second part of this section describes real-world attacks in the context of IoT technologies.

[23] For the purpose of this guide, the working group considered categories for consumer, federal, and industrial IoT as outlined in the Departments of Commerce and Homeland Security paper, A Road Map Toward Resilience Against Botnets (Botnet Road Map), a follow-on to "A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats".

Examples of IoT Devices and Systems



Type of System/Device
Connected Vehicle

Example

Most vehicles for sale today fall within this category, ranging from small cars to heavy transport vehicles used for shipping. Even agricultural combines and large tractors often have external connectivity built into their design. Indications that a vehicle is "connected" include:

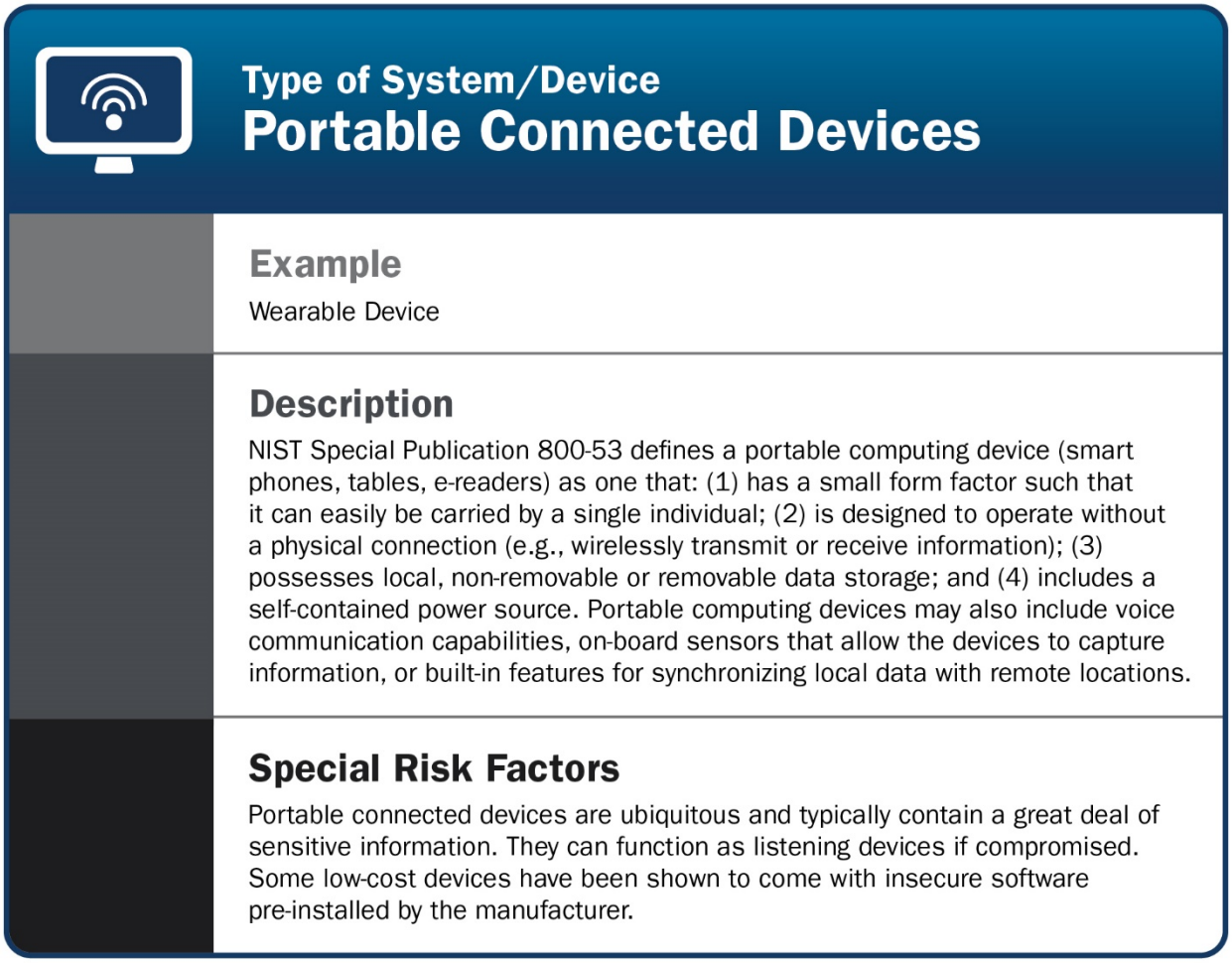
- Wi-Fi hotspot capability
- In-vehicle conveniences like OnStar, UConnect, etc.
- Accompanying smartphone apps which can lock/unlock a car or perform other similar remote functions
- In-dash navigational systems, particularly if they are able to receive real-time updates about traffic or other changing conditions
- Remote maintenance/location/fleet management functionality

Description

"Connected car" capabilities can include: (1) the ability to collect information via sensors and communicate this information back to a central organization (e.g., central fleet management organization or vehicle manufacturer) or to interact with other parts of the vehicle to trigger an action; (2) the ability of a driver and/or passenger's device to connect to and communicate with technology within the vehicle to perform a function (e.g. start vehicle, play music, call someone from user's contact list); or (3) the ability of parts of the vehicle to interact with technology and the physical environment surrounding the car.

Special Risk Factors

Research has demonstrated that connected cars are often "hackable" and alterations can be made that negatively affect how the vehicle operates. Vehicles used for high-risk purposes have typically required special modifications to remove external connectivity; but even when optional connectivity-based services are not enabled, the vehicle's telematic unit remains operational and active. Data on location, vehicle state, and other information that is uploaded to cloud-based service providers poses confidentiality risk, particularly for vehicles with sensitive mission purposes (like law enforcement or protective services).



IoT Services Description

Voice Recognition Services

Voice control services exist on many IoT technologies, ranging from phones to cars to television sets. Nearly all of these technologies depend on outside processing (e.g., a cloud computing environment) where audio is uploaded and processed by an array of servers and the interpreted commands are sent back to the device. For the most well-known services, this data transfer does not occur until the device hears and recognizes (without outside assistance) a "command phrase." The device only sends what immediately follows that instruction for processing. For some devices, most notably smart TVs, the voice command function continuously sends a stream of audio and relies upon the back-end processing for recognition that a command has been offered.

Connected Car Support Services

Nearly all cars manufactured today are "connected," which means they have a cellular data connection built into the vehicle to serve multiple purposes. This can be used for diagnostics, in-vehicle assistance and concierge services, traffic information, and vehicle software and

firmware[24] updates. A vehicle often has half a dozen or more such services that are provided by different vendors. The vendors provide a specific piece of functionality in the vehicle. The hosting and management of these services is nearly always provided by an outside vendor contracting with the automotive manufacturer.

Authentication and Identity Management Services

When an IoT technology has identity capabilities for authentication[25] purposes or as a means of storing different settings or preferences for multiple users, there is almost always an outside service involved. This also holds true for cases where a smartphone application has some degree of control over an IoT device; the identity service keeps track of which device should be controllable for any given user.

Types of Real-World Cyber Incidents Involving IoT Devices, Systems, and Services

Distributed Denial of Service

A Distributed Denial of Service (DDoS) attack occurs when an attacker is able to control a large number of devices, ranging in the tens of thousands or more. The attacker uses DDoS to generate massive amounts of network traffic aimed at disrupting a target system, creating a "botnet," The traffic comes from so many different sources that it becomes difficult for the targeted system to filter out and effectively block the attack. This also makes the investigation and source attribution of an attack extremely challenging.

As a real-world analogy, imagine if an office on a top floor of a building has a receptionist to prevent unauthorized people from entering the offices. A DDoS would be the equivalent of someone sending so many people to the office that they would clog the lobby, the elevators, the stairs, even the street outside the building. Even though the crowding might make it impossible for anyone to enter past the receptionist, it would not matter, because no one—even those with a valid reason to enter or exit the offices—would be able to enter because of the crowding. The overwhelming traffic prevents the receptionist or gatekeeper system from doing its normal job. An IoT device, system, or service that is fully connected to a network could be targeted by a DDoS attack to deny access or communication to this IoT resource.

The size of a DDoS attack depends upon the number of network-connected devices compromised by an attacker. IoT technologies, due to their ubiquity, large numbers, and lack of common security features and functions, make excellent sources for attackers to launch this kind of attack. In 2017, an attacker created the largest botnet ever comprised solely of IoT devices to deny access to a large provider of Domain Name Services (DNS) used by popular commercial multimedia companies.[26]

---

[24] See Appendix A – Glossary for definition.
[25] See Appendix A – Glossary for definition.
[26] Internet of Things and the Rise of 300 bps DDoS Attacks, https://www.akamai.com/us/en/multimedia/documents/social/q4-state-of-the-internet-security-spotlight-iot-rise-of-300-gbp-ddos-attacks.pdf

Data Manipulation and Privacy Leakage Risk

Commonly, IoT devices, systems, and services provide multiple functions for many entities within an organization. They often collect, measure, or generate data during operation. Transmission of data can become a source of risk if the IoT technology is capturing Personally Identifiable Information (PII) or other data with privacy implications. Unintended violations of a Privacy law could result because of the unforeseen integration of disparate sensitive personal data by IoT technologies. This unforeseen integration can result in the synthesis of PII into a specific "identity" and its unconsented entry into an organization's systems. Some issues and concerns are a result of connectivity; others may result from specific relationships with third-party vendors, such as cloud service providers, and can be addressed through contract provisions that govern those relationships. To the extent the issues are a result of broad connectivity, each user must be vigilant in understanding the data it shares and accumulates.

Another related risk may result when properly collected data is modified to influence the actions of the system using maliciously altered (or negligently inaccurate) information to make decisions, or for a purpose other than that which was authorized or intended.

In industrial settings, IoT technologies are being installed across wide areas to collect environmental information about temperature, moisture, wind, or other physical characteristics, as well as video and images. This information is intended to allow for analytics to assist with optimization of operations of many types; however, if data can be easily manipulated by an attacker, then the attacker can influence those operations to cause catastrophic consequences.

Third Party Access and Control

Third-party support and network connectivity of IoT technologies pose security challenges because of third-party access. This access is usually provided for remote management functions (for maintenance), software/firmware update functions, or features/functionality which leverage external services. An IoT technology may incorporate installation of a device on the user network which is, by design, controlled by a third party. For this reason, segmentation of networks hosting IoT devices is highly recommended, especially for devices which have no need to directly communicate with other ICT assets. Ease of access should not be used as a justification for allowing a connection between an IoT technology and a workstation or system on the user network without a complete understanding of the accompanying cyber risk and an acceptance of that risk by the organization. Importantly, many IoT technologies are at least partially under the control of an outside entity. Even though the device, system, or service may be "owned" by the purchasing organization, understanding its dependencies on outside vendors or third parties needs to be considered accordingly.

Section 4: Conclusion

The prevalence of IoT devices, systems, and services continues to grow in all facets of modern life. Currently, inconsistencies that exist in vendor standards throughout the design and production of IoT technologies pose a significant risk to organizations wishing to integrate and take advantage of IoT capabilities. Acquisition teams are responsible for acquiring new technologies and need the knowledge to ensure new vulnerabilities do not negatively impact the acquiring organization's mission or operations. When discussing vendor requirements and capabilities, coordination between acquisition and IT teams is an important step toward ensuring all staff have the awareness of the security and resiliency implications of introducing IoT devices, systems, and services to the organization's network.

IoT technologies are susceptible to many of the same types of vulnerabilities as traditional ICT technologies; however, many of the mitigations currently used for ICT may not be interoperable with IoT. Commonly seen attacks such as DDoS can deny the availability or accessibility of IoT devices, systems, and services. However, not only can IoT be the target of attacks, if not secured properly, it can become compromised and serve as a node in a botnet used to launch DDoS attacks on other resources either inside or outside the organization. The connected nature of IoT technologies implies a dependence on data transmissions to provide regular diagnostics and communication. Risks associated with collecting and transmitting sensitive IoT data include the loss of PII or other data requiring privacy. Since IoT devices, systems, and services can be connected to other parts of a network, ensuring appropriate user access controls are in place is just as important as controlling what the device, system, or service itself is authorized to access.

Each step of the acquisition lifecycle includes activities that are important to determine the impact and risk posture of IoT technology connected to an organization's network. This document can be used to determine requirements for deployment, operation, and maintenance of the IoT device, system, or service and how to measure IoT technology compliance with security and risk management policies within the organization.

This document is not an exhaustive resource. It provides a set of fundamental considerations an organization should take before acquiring and deploying an IoT device, system, or service. Following the recommendations in this document will empower acquisition team members to engage confidently with vendors and the appropriate members of their organization to ensure necessary information about the IoT device, system, or service is collected and evaluated before purchase or use. This document can also be used to establish an initial strategy for understanding the risks associated with IoT technologies in the context of an organization's operations.

References

The following is a list of links to reading materials and references that were used in the development of this document.

"C2 Consensus on IoT Security Baseline Capabilities", Council to Secure the Digital Economy, https://securingdigitaleconomy.org/projects/c2-consensus/

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," DOD, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

Department of Homeland Security (DHS), "Strategic Principles for Securing the Internet of Things (IoT), DHS, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

DFARS 252.239-7018, "Supply Chain Risk", DOD, https://www.law.cornell.edu/cfr/text/48/252.239-7018

"Evaluating and Choosing an IoT Platform", O'Reilly Media, 2016, https://www.oreilly.com/learning/evaluating-choosing-iot-platform

"Evaluation of IoT Backend Providers", Crisp Vendor Universe, https://d1.awsstatic.com/analyst-reports/CVU_Evaluation-of-IoT-Backend-Providers_shortversion_AWS_LogoNew.pdf

FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems", National Institute of Standards and Technology (NIST), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems", NIST, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

FIPS PUB 140-2, "Security Requirements for Cryptographic Modules", NIST, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

"IoT Privacy by Design", GSMA, 2015, https://www.gsma.com/iot/iot-knowledgebase/iot-privacy-design-decision-tree/

NIST Special Publication (SP) 800-18 Revision (Rev). 1, "Document for Developing Security Plans for Federal Information Systems", NIST, https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

NIST SP 800-30 Rev. 1, "Risk Management Document for Information Technology Security Risk Assessment Procedures for Information Technology Systems", NIST, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

NIST SP 800-34 Rev.1, “Contingency Planning Document for Information Technology Systems”, NIST, https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

NIST SP 800-37, Rev. 1, “Document for the Security Certification and Accreditation of Federal Information Systems”, NIST, https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final

NIST SP 800-47, “Security Document for Interconnecting Information Technology Systems”, NIST, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf

NIST SP 800-53 Revision 3, “Recommended Security Controls for Federal Information Systems”, NIST, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-53r3.pdf

NIST SP 800-53A, “Document for Assessing the Security Controls in Federal Information Systems”, NIST, https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final

NIST SP 800-171 Rev. 1, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations”, NIST, https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

NIST SP 800-82 Rev. 2, “Document to Industrial Control Systems (ICS) Security”, NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

NIST Interagency Report (NISTIR) 8200, “Interagency Report on Status of International Cybersecurity Standardization for IoT”, NIST, https://csrc.nist.gov/publications/detail/nistir/8200/final

NIST Interagency Report (NISTIR) 8259 (draft), “Core Cybersecurity Feature Baseline for Securable IoT Devices”, NIST, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf

“Security for the Internet of Things”, Harbor Research, http://harborresearch.com/download-security-for-the-internet-of-things-report

Appendix A – Glossary

As defined on the NIST Computer Security Resource Center website: https://csrc.nist.gov/glossary, unless otherwise noted. Definitions marked with an asterisk were defined by the working group for the purposes of this document.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Buffer Overflow: A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Attackers exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Command Injection: An attack method that alters dynamically generated content on a webpage by entering HTML code into an input mechanism. When users visit an affected webpage, their browsers interpret the code, which may cause malicious commands to execute in the users' computers and across their networks.[27]

Connectivity: The ability for a device to access the Internet or other networked device or asset.*

Cyber Resilience: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources

Cyber Supply Chain Risk Management: The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products), or services at any point during the life cycle.

Denial-of-Service: The prevention of authorized access to a system resource or the delaying of system operations and functions.

Device: A combination of components that function together to serve a specific purpose; in automated assessment, a type of assessment object that is either an IP addressable (or equivalent) component of a network or a removable component that is of security significance.

Encryption: Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

Exploited: When a specific vulnerability is used by an attacker to attain control of a network

[27] https://searchsoftwarequality.techtarget.com/definition/command-injection

device or resource.*

Firmware: Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

Hard-Coded Passwords: A term used to describe the process of including passwords in plaintext within the firmware or other software code for the IoT device, which bypasses the need for an external input to authenticate the device itself or its function while on the network.*

Hardware: The physical components of a system.

IoT Products, Services, and/or Solutions: A phrase used to describe the collection of hardware and software needed to install and operate an IoT device or set of devices.*

Legacy Systems: A term used to reference outdated or unsupported methods, software, hardware, or devices that are operating within an enterprise and cannot take advantage of the latest advancements in technology.*

Network Asset: A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Patching: A “repair job” for a piece of programming; also known as a “fix.” A patch is the immediate solution that is provided to users; it can sometimes be downloaded from the software maker’s website. The patch is not necessarily the best solution for the problem, and product developers often find a better solution to provide when they package the product for its next release. A patch is usually developed and distributed as a replacement for or an insertion in compiled code (that is, in a binary file or object module).

Plaintext: Intelligible data that has meaning and can be read or acted upon without the application of decryption. Also known as cleartext.

Software: Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Third-Party Service: An outside entity (not the purchaser or vendor) which provides a resource necessary for some or all functionality of a device.*

Vendor: A commercial supplier of software or hardware.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix B – Acknowledgements

This document was a collaborative effort based on the input and analysis from individuals in both the IT Government Coordinating Council and IT Sector Coordinating Council who participated in the IoT Security Working Group. The objective of the working group for the purposes of this document was to provide actionable recommendations to assist organizations involved in the acquisition lifecycle in making risk-informed acquisitions decisions and drive demand for secure IoT products and services. This effort was co-chaired by Mr. Emile Monette, Cybersecurity and Infrastructure Security Agency, DHS *(former)*, and Mr. David Durcsak, General Dynamics Information Technology.

Additionally, the following organizations participated in developing this document:

Government Organizations

- The U.S. Department of Homeland Security (DHS)
- The U.S. General Services Administration (GSA)
- The National Telecommunications and Information Administration (NTIA)

Industry Organizations

- CISCO Systems
- Consumer Technology Association (CTA)
- CyberRx
- General Dynamics Information Technology
- Honeywell
- Information Technology Industry Council (ITI)
- Intel
- Samsung

Specifically, this document was written and informed by the following participants.

Michael Aisenberg, The MITRE Corporation
Peter Allor, Honeywell
Mike Bergman, CTIA
Nadine Burris, GSA
David Durcsak, General Dynamics Information Technology
Kevin Funk, GSA
Karen Goertzel, Booz Allen Hamilton
Phil Grant, Booz Allen Hamilton
Russell Gyurek, CISCO
Travis Hall, NTIA
Keith Hill, The MITRE Corporation
Julian Humble, DHS
Helen Jackson, DHS
Robert Martin, The MITRE Corporation
Emile Monette, DHS *(former)*
Mary Rossell, Intel
Ola Sage, CyberRx
Ryan Sheehy, Booz Allen Hamilton
Rob Shein, PricewaterhouseCoopers
Angela Smith, GSA
Eric Tamarkin, Samsung
Scott Tousley, DHS Science and Technology *(former)*
Pamela Walker, ITI
Eric Wenger, CISCO