NIST Internal Report
NIST IR 8425A

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffrey Marron
Barbara Cuthill
David Lemire
Brad Hoehn
Chris Evans

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425A

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

NIST Internal Report
NIST IR 8425A

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffrey Marron
Barbara Cuthill
Applied Cybersecurity Division
Information Technology Lab

David Lemire
Brad Hoehn
Chris Evans
HII

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8425A

September 2024

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

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

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

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

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

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-08-30

How to Cite this NIST Technical Series Publication:
Fagan M, Megas K, Watrobski P, Marron J, Cuthill B, Lemire D, Hoehn B, Evans C (2024) Recommended Cybersecurity Requirements for Consumer-Grade Router Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425A. https://doi.org/10.6028/NIST.IR.8425A

Author ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Katerina N. Megas: 0000-0002-2815-5448
Paul Watrobski: 0000-0002-6449-3030
Jeffrey Marron: 0000-0002-7871-683X
Barbara B. Cuthill: 0000-0002-2588-6165

Contact Information
iotsecurity@nist.gov

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

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8425/a/final including related content, potential updates, and document history.

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

Abstract

Ensuring the security of routers is crucial for safeguarding not only individuals' data but also the integrity and availability of entire networks. With the increasing prevalence of smart home Internet of Things (IoT) devices and remote work setups, the significance of consumer-grade router cybersecurity has expanded, as these devices and applications often rely on routers in the home to connect to the Internet. This report presents the *consumer-grade router profile*, which includes cybersecurity outcomes for consumer-grade router products and associated requirements from router standards.

Keywords

cybersecurity; consumer-grade routers; network security; Internet of Things

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 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.

Audience

The intended audience for this report consists of manufacturers of consumer-grade router products (especially product security officers), internet service providers, retailers, and testing and certification bodies interested in establishing minimum cybersecurity requirements for consumer-grade routers.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication

Table of Contents

List of Tables

List of Figures

Executive Summary

This document builds on the *Profile of the IoT Core Baseline for Consumer IoT Products*, NISTIR 8425 [IR8425]. This document specializes that consumer product baseline for routers intended for residential use that can be installed by the customer, which are referred to as *consumer-grade routers*.

Similar to NISTIR 8425, these recommendations are stated as technical and non-technical cybersecurity outcomes for consumer-grade routers, their manufacturers, and other supporting entities that may exist within the ecosystem. Cybersecurity outcomes are broad, flexible guidelines for digital products that describe hardware and software capabilities or organizational capabilities that can support cybersecurity when the product is deployed in a customer's environment. Technical outcomes are those achieved by the product itself, using hardware and software implementations. Non-technical outcomes are those achieved by the product manufacturer and other entities that support the product, usually through the dedication of resources to implement and maintain policies and procedures. To provide additional context and definition, the cybersecurity outcomes for consumer-grade routers are mapped to more detailed requirements in related standards.

In the analysis of the standards and their requirements, NIST found that no single standard addressed all the outcomes fully and found no conflicts in the requirements or how they related to the cybersecurity outcomes. Therefore, NIST recommends the use of multiple standards to fully address consumer-grade router cybersecurity.

1. Introduction

Router cybersecurity is of paramount importance in today's interconnected world, where digital communication plays a central role in both personal and professional spheres. Routers serve as the gatekeepers of our networks, managing the flow of data between devices in the home or office and the internet. A compromised router opens the door to a host of potential exploited vulnerabilities and impacts, ranging from unauthorized access and sensitive information dissemination to the possibility of malicious attacks on connected devices. Ensuring the security of routers is crucial for safeguarding not only individual privacy and safety but also the integrity and availability of entire networks. With the increasing prevalence of smart home IoT products and remote work from home offices, the significance of consumer-grade router cybersecurity has expanded. A secure consumer-grade router not only protects U.S. citizens against data theft and other cyberattacks but also contributes to the overall resilience of the global digital infrastructure. A "consumer-grade router" is a router intended for residential use and can be installed by the customer. Routers forward data packets, most commonly Internet Protocol (IP) packets, between networked systems. Throughout this document, the term "router" is used as a shorthand for "consumer-grade router." As technology advances, the need for robust router cybersecurity becomes ever more critical to maintain a safe and trustworthy digital environment.

This report presents a *profile*, which recommends cybersecurity outcomes for these products and identifies associated requirements from standards. This profile was developed starting from the outcomes defined for consumer IoT products in *Profile of the IoT Core Baseline for Consumer IoT Products*, NISTIR 8425 [IR8425]. Though developed for consumer IoT products, the NISTIR 8425 outcomes are important cybersecurity guidance for any digital product. Outcomes can be technical (i.e., implemented through hardware and/or software) or non-technical (i.e., implemented as procedures and processes by organizations or individuals). Consistent with the usage of the term "outcome" in NIST IR 8425, outcomes are broad, flexible guidelines that can apply to different use cases, contexts, technologies, etc., while requirements are targeted specifications that can define meeting an outcome for a specific use case, context, technology, etc. The guidance in this document has been developed uniquely for consumer-grade routers using cybersecurity considerations and standards specific to that product type. **NIST recommends the use of the following standards and guidance for the cybersecurity of consumer-grade router products:**

1. Broadband Forum (BBF) TR-124 Issue 8 – *Functional Requirements for Broadband Residential Gateway Devices* [BBF]
2. CableLabs (CL) Security *Gateway Device Security Best Common Practices* [CableLabs]
3. Federal Office for Information Security (BSI) TR-03148: *Secure Broadband Router – Requirements for secure Broadband Routers* [BSI]
4. Infocomm Media Development Authority (IMDA) *Technical Specification Security Requirements for Residential Gateways* [IMDA]
5. *Platform Firmware Resiliency Guidelines*, SP 800-193 [SP800-193]

6. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161 Rev. 1 [SP800-161r1]
7. *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, SP 800-218 [SSDF]
8. *Information technology — Security techniques — Vulnerability disclosure processes*, ISO/IEC 29147 [ISO29147]
9. *Information technology — Security techniques — Vulnerability handling*, ISO/IEC 30111 [ISO30111]
10. *Risk management — Guidelines*, ISO 31000 [ISO31000]
11. *Systems and software engineering — Design and development of information for users*, ISO/IEC/IEEE 26514 [ISO26514]

NIST recommends the use of four existing router standards[1] (i.e., items 1 through 4 in the list above). Requirements from these standards focus primarily on the router device, discussing many cybersecurity capabilities appropriate for this equipment. **Fig.** 1 notionally[2] depicts that requirements of the four router standards were mostly unique and had minimal overlap. Few requirements from the different standards repeat, and **each standard's requirements offer useful details about how cybersecurity outcomes can be met and important cybersecurity features to include in consumer-grade router devices**. Additional technical requirements for firmware are introduced by SP 800-193 (i.e., item 5). Appendix A provides a crosswalk between technical cybersecurity outcomes for these products and the technical requirements from these five standards.

[1] These standards primarily focused on technical capabilities for router devices. The Broadband Forum (BBF) TR-124 Issue 8 standard includes requirements outside of the purview of cybersecurity, while the other three standards focused exclusively on cybersecurity requirements. All cybersecurity requirements were examined to create the consumer-grade router profile. Non-cybersecurity requirements from the BBF standard were not analyzed as part of the profiling process.

[2] The overlap between standards in the graphic is not necessarily equal or proportional to the true overlap (i.e., the number of requirements between each standard that are the same or otherwise redundant).

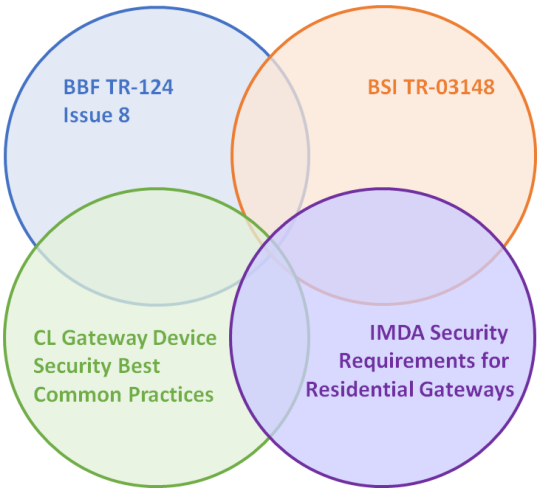

Fig. 1. Most requirements from the four consumer-grade router standards do not repeat.

The identified requirements from the four router standards address technical cybersecurity for consumer-grade router devices; however, they contain few non-technical cybersecurity requirements and no requirements for cybersecurity for product components other than the router device (e.g., backend[3], mobile application). Therefore, additional guidance found in Appendix B items 6 through 11 is recommended to help fill some of those gaps, particularly for non-technical outcomes.

These recommended publications contain a wealth of valuable guidance that, when used by manufacturers, can help improve the cybersecurity and securability of these products. **This list is intended as a minimum starting point** and may not address all the cybersecurity considerations for every consumer-grade router product. **To ensure cybersecurity consideration of all router product components, the *Product Development Cybersecurity Handbook* [CSWP33] is recommended** in addition to the standards and guidance indicated above. If a router product has additional product components, such as a smart phone application, additional technical product cybersecurity capability requirements would also be necessary to meet the outcomes for the complete product. These considerations are discussed generally for digital products in the handbook. As elaborated on in Section 2 of this profile, **full support of all outcomes in this profile by all product components is expected. Fig.** 2 shows how the standards and guidance listed above relate to cybersecurity outcomes (i.e., the technical vs. non-technical outcomes) and product components (i.e., router device vs. other product components).

[3] Backends provide remote services, management and monitoring typically hosted on cloud-based servers.

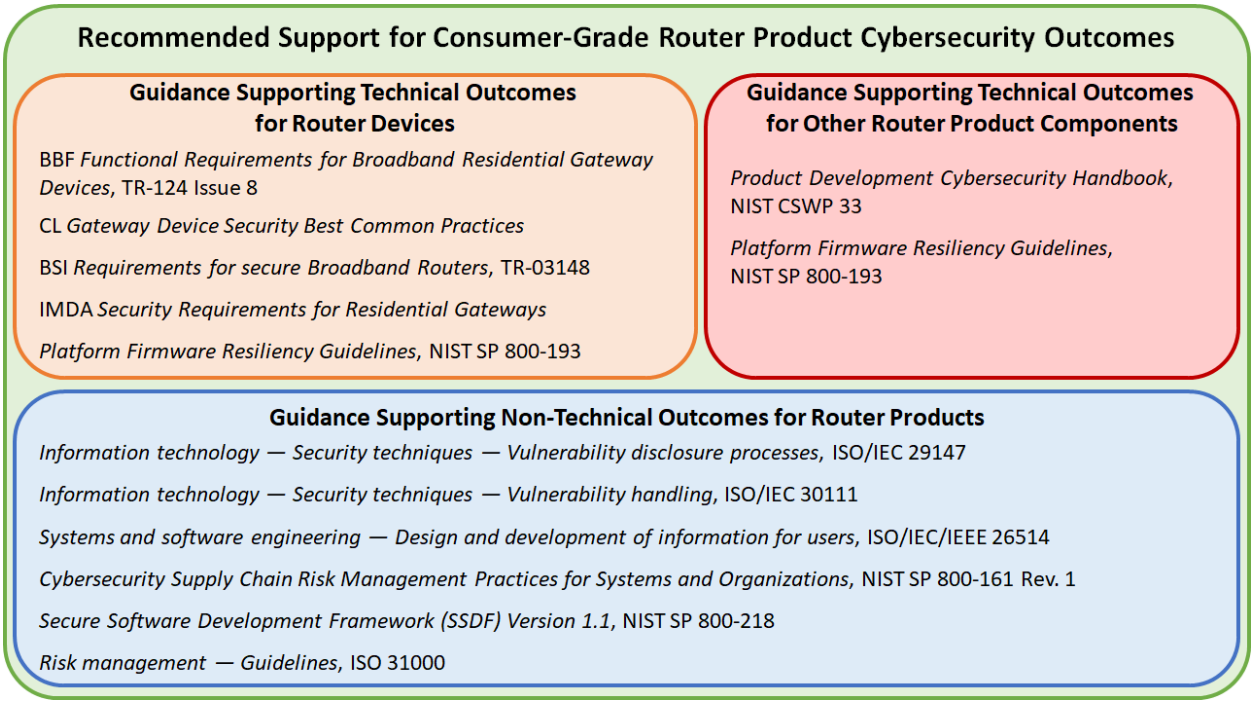

Fig. 2. Recommended guidance documents and standards support cybersecurity outcomes for all parts of consumer-grade router products throughout their development lifecycle.

Additionally, manufacturers should look beyond minimal technical requirements for cybersecurity features and consider more robust cybersecurity controls or support when applicable. Section 2.1 of this document provides examples that can improve cybersecurity related to these products.

2. Scope of Consumer-Grade Routers

This profile identifies minimum cybersecurity for consumer-grade routers. Routers forward data packets, most commonly Internet Protocol (IP) packets, between networked systems. **The profile makes no distinction in its cybersecurity recommendations with regards to whether the product is owned by the customer or leased from an internet service provider.**

> The cybersecurity outcomes defined in this profile are valuable to manufacturers of consumer-grade routers regardless of how their products end up in a customer's home. Routers leased from an internet service provider may be managed in part by both the customer and provider. Even in this scenario, the recommended requirements in this profile would be useful to both customers and providers in securing routers. Additional discussion related to this scope can be found in Appendix C.

Cybersecurity outcomes and requirements for products should be scoped to include all product components (e.g., smartphone applications) developed to be used with the router device. **Fig.** 3 below shows an example consumer-grade router product, where the router device is supported by both backend remote services and smartphone application. Third-party applications are not generally considered in the product's scope, unless designated by the product manufacturer as such. However, the product scope does include any interfaces that create risk for the router product, such as an application programming interface (API) accessible to third-party applications.

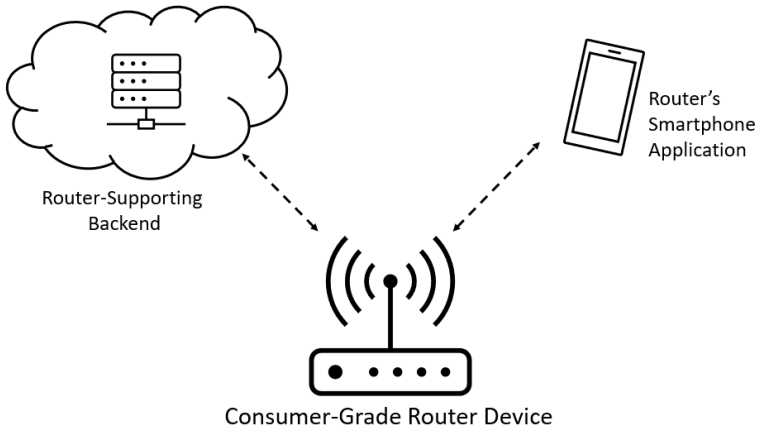

Fig. 3. An example consumer-grade router product that includes a smartphone application and backend server in addition to the router device.

Firmware is a critical foundation of many digital products, including consumer-grade routers and other router product components. Given the central role routers play in home networks, firmware vulnerabilities pose significant cybersecurity concerns. Other software that can access router data and manage the product (e.g., mobile applications or remote backends) also create attack vectors for home consumers if not appropriately mitigated in software and through the software development process.

2.1. Cybersecurity Utilizing the Full Product

The standards referenced in Section 1, particularly the four that are specific to consumer-grade routers, reflect general, minimal cybersecurity for this equipment. Router product manufacturers should look beyond these technical requirements for additional security features. The following concepts[4] are examples of emerging techniques that may help improve the cybersecurity provided by consumer-grade routers and of the products themselves:

- **Machine-readable asset identification support.** Consumer-grade routers serve as a central connection point for networks. Many types of devices will gain access to the local network and usually the internet. Consumer grade routers can be more proactive in managing the cybersecurity of the network when machine-readable asset identifiers are available. While home users could utilize machine-readable asset identification, it is more likely to be useful to small businesses or for routers leased from internet service providers (ISPs). Identification can also go beyond simple inventorying to include device type and firmware version, be extended by concepts like device intent signaling (e.g., the "manufacturer usage description" [MUD]) or be used more directly for the management of router devices' firmware updates. Machine-readable asset identifiers must be developed and used in ways that are privacy preserving.
- **Interface and functionality minimization for consumer-grade router devices.** "Secure-by-design" principles [SecureByDesign] applied to consumer-grade routers should guide manufacturers to minimize the number of interfaces, both logical and physical and general functionality provided by the router device. The primary functionality of the home router is to provide access to the Internet for devices within the home. Extraneous functions should not be included in this component. For example, configuration may be better managed by another product component (e.g., mobile application). This is not to suggest a product composed of only a router device is necessarily less secure than those that can offload functions to other components..
- **Robust network onboarding support from consumer-grade router products.** Cybersecurity when provisioning new devices to the network connected to a consumer-grade router can go beyond a single password. When a router product is composed of components such as mobile applications or backends, those components can be used as part of a more robust onboarding mechanism. For example, when a device is attempting to connect to the router device with (or without) the password, the mobile application can notify the owner and ask for explicit approval for the device to onboard. Though reliability needs to be considered to ensure individuals can always access and use their routers, onboarding mechanisms for consumer-grade routers that give individuals more access control over their networks is generally beneficial. For additional recommendations on consumer IoT onboarding and device credentialing see *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network* [SP1800-36].

[4] . These are provided at the outcome level, that is, as high-level informative statements rather than as normative text.

- **Multiple signatures for software update packages when possible.** At a minimum, all software update packages should be signed by the source of the update (e.g., manufacturer). When applicable (e.g., when routers are leased from internet service providers (ISPs) other entities, such as the owning ISP, may also cryptographically sign updates, adding another layer of security. Routers would only apply a software update if the cryptographic signatures from both the manufacturer and ISP are verified. Co-signing by the ISP also gives the ISP a mechanism to manage the acceptance of software updates.
- **Robust security for protecting logs of captured cybersecurity state information.** Cybersecurity State Awareness, documented in Appendix A, is essential for detecting compromised routers. Because logs can be a valuable tool for security researchers and others performing forensic analysis of cybersecurity incidents, this data needs to be stored securely. Protections that can enhance router log security include encrypting and password protecting logs to ensure that access is limited to authorized personnel only, use of non-volatile memory storage for logs, off-device storage for logged data, and restricting log deletion.

Several of these examples highlight ways consumer-grade router products can use multiple techniques to deliver cybersecurity capabilities. Manufacturers should consider these and other techniques to continually improve router cybersecurity as risks shift and new mitigations become available.

3. Conclusion

This consumer-grade router profile can help manufacturers determine appropriate cybersecurity to incorporate as they develop their products. These recommendations draw from current effective practices and promote the adoption of accepted and vetted cybersecurity features for router products. The outcomes, requirements, and standards referenced here should not be viewed as precluding the use of additional forward-looking requirements such as those discussed in Section 2.1.

As with any NIST report, as the standards and effective practices referenced change over time, NIST may revisit this document and revise it. NIST welcomes ongoing feedback and recommendations from the community regarding standards, effective practices, and solutions for consumer-grade routers. That said, NIST encourages readers to identify if the standards referenced here have been updated asynchronously from this report. NIST reiterates the importance of a product-wide perspective to develop a comprehensive approach to providing cybersecurity for consumer-grade router products.

References

[WHAnnouncement] White House (2023) Biden-Harris Administration Announces Cybersecurity Labeling Program for Smart Devices to Protect American Consumers. (White House, Washington, DC). https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/

[IR8425] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425. https://doi.org/10.6028/NIST.IR.8425

[BBF] Walls, J, Editor (2022) Functional Requirements for Broadband Residential Gateway Devices. (Broadband Forum, Fremont, CA), Technical Report (TR) 124, Issue 8. https://www.broadband-forum.org/pdfs/tr-124-8-0-0.pdf

[CableLabs] CableLabs Security (2021) Gateway Device Security Best Common Practices. (CableLabs, Louisville, CO), CL-GL-GDS-BCP-V01-211007. https://community.cablelabs.com/wiki/plugins/servlet/cablelabs/alfresco/download?id=1209eea3-bd81-40cb-9a18-21bd6cfcd80d

[BSI] Federal Office for Information Security (2023) Secure Broadband Router: Requirements for Secure Broadband Routers. (Federal Office for Information Security, Bonn, Germany), BSI Technical Report (TR) 03148. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03148/tr-03148.html

[IMDA] Info-communications Media Development Authority of Singapore (2020) Security Requirements for Residential Gateways. (Info-communications Media Development Authority, Singapore), IMDA Technical Specification (TS) RG-SEC. https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf

[SP800-193] Regenscheid, AR (2018) Platform Firmware Resiliency Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-193. https://doi.org/10.6028/NIST.SP.800-193

[SP800-161r1] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-161r1. https://doi.org/10.6028/NIST.SP.800-161r1

[SSDF] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-218. https://doi.org/10.6028/NIST.SP.800-218

[ISO29147] International Organization for Standardization (2018) Information technology — Security techniques — Vulnerability disclosure. (ISO Standard No. 29147:2018). https://www.iso.org/standard/72311.html

[ISO30111] International Organization for Standardization (2019) Information technology — Security techniques — Vulnerability handling processes. (ISO Standard No. 30111:2019). https://www.iso.org/standard/69725.html

[ISO31000] International Organization for Standardization (2018) Risk management — Guidelines. (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

[ISO26514] International Organization for Standardization (2022) Systems and software engineering — Design and development of information for users. (ISO Standard No. 26514:2022). https://www.iso.org/standard/77451.html

[CSWP33] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B, Lemire D, Hoehn B (2024). Product Development Cybersecurity Handbook: Concepts and Considerations for IoT Product Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Cybersecurity White Paper (CSWP) 33. https://doi.org/10.6028/NIST.CSWP.33.ipd

[SecureByDesign] Cybersecurity and Infrastructure Security Agency (2023). Secure-by-Design Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. (Cybersecurity and Infrastructure Security, Washington, DC). https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf

[MUD] Lear E, Droms R, Romascano D (2019) Manufacturer Usage Description Specification. (Internet Engineering Taskforce), IETF Request for Comments (RFC) 8520. https://datatracker.ietf.org/doc/html/rfc8520

[SP1800-36] Fagan, M., Marron, J., Watrobski, P., Souppaya, M., *et al.* (2023) Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (NIST SP) 1800-36.

[SP800-40r4] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4. https://doi.org/10.6028/NIST.SP.800-40r4

[RFC6092] Woodyatt, J, Editor (2011) Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service. (Internet Engineering Task Force), IETF Request for Comment (RFC) 6092. https://datatracker.ietf.org/doc/html/rfc6092

[IR8320] Bartock MJ, Souppaya MP, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra A, Banks D, Jordan M, Pendarakis D, Rao JR, Romness P, Scarfone KA (2022) Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8320. https://doi.org/10.6028/NIST.IR.8320

[SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[RFC6092] Woodyatt J, Ed. (2011) Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service. (Internet

Engineering Taskforce), IETF Request for Comments (RFC) 6029. https://datatracker.ietf.org/doc/rfc6092/

[ParksRouterResearch] Parks Associates (2022) Parks Associates: 52% of Consumers Acquired Their Routers From Their ISP. (PRNewswire, Dallas, TX). https://www.prnewswire.com/news-releases/parks-associates-52-of-consumers-acquired-their-routers-from-their-isp-301593338.html

Appendix A. Crosswalk between Technical Outcomes and Consumer-Grade Router Cybersecurity and Firmware Requirements

This Appendix provides additional information about how the requirements from the four router standards relate to the consumer-grade router profile outcomes. Organizations can use this informative crosswalk to understand how the technical standards relate to cybersecurity concepts identified in higher-level technical cybersecurity outcomes for router products. This is not normative guidance. As an informative crosswalk, the profile is at the level of outcomes not detailed requirements. Further detailed requirements can be found in the referenced standards. Additionally, the technical outcomes can serve as a guide for manufacturers as they consider cybersecurity for a full product as described in Section 2.

Sections A.1 to A.7 below show which requirements from the four standards relate to the technical outcomes. Each subsection from A.1 to A.7 states the high-level outcome along with each sub-outcome that defines the high-level outcome. The language for the cybersecurity outcomes was developed by modifying the outcomes from NISTIR 8425. Two new sub-outcomes were also added based on review of the standards. These are noted with a †.

For each sub-outcome, a set of related requirements from the four standards is also included. The abbreviations used for the standards are:

BBF's *TR-124 Issue 8* [BBF]

CL's *Security Gateway Device Security Best Common Practices* [CableLabs]

BSI's *Secure Broadband Routers* [BSI]

IMDA's *Security Requirements for Residential Gateways* [IMDA]

NIST recommends using Special Publication 800-193 [SP800-193] to develop firmware for router products and their components. Section 4 of that document details technical cybersecurity capabilities to help mitigate firmware vulnerabilities. These capabilities support the outcomes for consumer-grade router products defined in this document. Thus, in addition to the four standards, requirements from Section 4 of SP 800-193 are also included in the following sub-sections when applicable.

Finally, for some outcomes and sub-outcomes, commentary is also included indicating example cybersecurity enhancements of consumer-grade router products that may go beyond what is reflected in the current standards or may not be applicable to all router products but should be considered by router product manufacturers.

A.1. Asset Identification

The consumer-grade router product is uniquely identifiable and inventories all of the consumer-grade router product's components.

A.1.1. Asset Identification 1

The consumer-grade router product can be uniquely identified by the customer and other authorized entities via means including but not limited to: host name, service set identifier (SSID), and serial number.

Related Standards Requirements:

BBF GEN.DESIGN.12, GEN.DESIGN.13, MGMT.LOCAL.20, IF.LAN.WIRELESS.AP.20

CL OOB-011, KEY-006, OOB-007

BSI (3.1.2.1)

IMDA *None*

A.1.2. Asset Identification 2

The consumer-grade router product uniquely identifies each product component (e.g., router device, mobile app) and maintains an up-to-date inventory of connected product components.

No requirements from the standards were mapped to this outcome. Products composed of only a router device would meet this outcome by default. When a product is composed of other components (e.g., mobile application, backend), those components may need to support this outcome.

The asset identification outcome is focused on the ability to identify the router and the router's management of its product components, but routers may also assist customers in managing their connected devices. Machine-readable asset identifiers for all connected products could enable routers to use these identifiers for the purpose of asset management in support of customers' cybersecurity.

A.2. Product Configuration

The configuration of the consumer-grade router product is changeable, there is the ability to restore a secure default setting, and any and all changes can only be performed by authorized individuals, services, and other product components.

Configuration control of networking equipment, including router products is critical to network cybersecurity. If possible, configuration may be better managed by another product component (e.g., mobile application) to minimize interfaces (and, thus, attack surface) of the router device specifically.

A.2.3. Product Configuration 1

Utilizing strong authentication mechanisms (e.g., multi-factor authentication), authenticated and authorized individuals (e.g., customer, ISP), services, and other product components can access the consumer-grade router product's configuration interfaces (e.g., administration page) and change the configuration settings.

Related Standards Requirements:

BBF MGMT.LOCAL.2

CL OOB-007, DE-007, MI-002, MI-010, MI-011

BSI (3.1.2) (4), (4.1.1), (4.1.2), (4.2), (4.3), (4.4), (4.5), (4.8), (4.9), (4.10)

IMDA 4.2, 4.2.3, 4.4

A.2.4. Product Configuration 2

Authorized individuals (i.e., customer), services, and other consumer-grade router product components have the ability to restore (i.e., factory reset) the router product to a secure default (i.e., uninitialized) configuration. In restoring the product to a secure default, all settings and data must be deleted.

Related Standards Requirements:

BBF MGMT.LOCAL.10

CL OOB-009, DE-003, DE-004, DE-006

BSI (4.6)

IMDA 4.1.1, 4.2.1, 4.2.3

SP 800-193 4.2.4(5), 4.4.2(5)

A.2.5. Product Configuration 3

The consumer-grade router product applies configuration settings to applicable router product components.

No requirements from the consumer-grade router standards were mapped to this outcome. Consumer-grade router products composed of only a router device would natively meet this outcome via configuration on the device itself. When a router product is composed of other components (e.g., mobile application, backend), those components may need to support this outcome.

A.3. Data Protection

The consumer-grade router product protects data stored across all router product components and transmitted both between product components and outside the router product from unauthorized access, disclosure, and modification using strong encryption (e.g., FIPS-approved algorithms).

A.3.6. Data Protection 1

Each consumer-grade router product component protects data it stores via secure means, such as strong encryption (e.g., FIPS-approved algorithms). All stored data, including data used for authentication (e.g., salting and hashing stored passwords or passphrases) must be protected. Critical data (including firmware images) can be securely backed up and recovered.

Related Standards Requirements:

BBF SEC.FIRMWARE.2

CL DRP-001, KEY-001, KEY-002, KEY-003, HR-003, HR-004, SB-005, OOB-002

BSI (4.1.1)

IMDA 4.5

SP 800-193 4.1.1(1-4, 7), 4.1.4(1-2), 4.2.2, 4.2.3(1-2), 4.2.4(5), 4.4.1 (1, 2a, 7, 12), 4.4.2(1-2, 4, 6-8, 10)

A.3.7. Data Protection 2

The consumer-grade router product has the ability to delete or render inaccessible stored data that are either collected from or about the customer, home, family,, connected devices, or traffic transmitted to and from the local network. Strong protections (e.g., FIPS-approved algorithms) are used for data at rest.

Related Standards Requirements:

BBF *None*

CL OOB-009

BSI (4.6)

IMDA 4.2.3

A.3.8. Data Protection 3

When data are sent between consumer-grade router product components or outside the product, strong protections (e.g., FIPS-approved algorithms) are used for the data transmission. For data related to managing the product, this includes using hypertext transfer protocol (HTTP) over transport layer security (TLS) for external communications via the consumer-grade router product and for using device management interfaces or web portals.

Related Standards Requirements:

BBF MGMT.REMOTE.WEB.6, SEC.USERINTERFACE.1, SEC.FIRMWARE.1, SEC.FIRMWARE.2

CL OOB-003, DE-002, DE-004, DE-005, MI-001, NETS-001, NETS-003, SBOM-006

BSI (3.1.2.2), (4.1.1), (4.1.2), (4.4), (4.10)

IMDA 4.2.2, 4.2.5

A.4. Interface Access Control 1

Each consumer-grade router product component controls access to and from all interfaces[5] in order to limit access to only authorized entities.

A.4.9. Interface Access Control 1a

Permit access only to interfaces necessary for the consumer-grade router product's operation. All other channels and access to channels are removed or secured. For example, disable by default remote access to the router, especially via the wide area network (WAN) interface. Management access should be confined to local area network (LAN) interfaces.

Related Standards Requirements:

BBF MGMT.LOCAL.1, MGMT.REMOTE.WEB.1, MGMT.REMOTE.WEB.5, MGMT.REMOTE.WEB.12, MGMT.REMOTE.WEB.13, SEC.GEN.5, SEC.GEN.6, SEC.GEN.10, SEC.GEN.11, SEC.USERINTERFACE.8

CL HR-001, HR-002, OOB-005, MI-003, NETS-004, NETS-005, MI-011

BSI (3), (3.1), (3.1.2), (3.2), (4.1.1)

IMDA 4.2, 4.2.1

SP 800-193 4.2.1.2

Interfaces should be minimized for the product overall, but particularly attention should be given to minimizing the interfaces included on the router devices. Extraneous interfaces unnecessary to the core features of the router device should be implemented via other product components, be turned off by default, or be removed entirely. Note that there may be extra functionality that improves the security of the device and network. In those situations, including the functionality would be beneficial.

A.4.10. Interface Access Control 1b

For all interfaces necessary for the consumer-grade router product's use, access control measures are in place.[6] At a minimum this includes:

1. Assigning consumer-grade router products unique initial passwords that are required to be changed to a strong password or passphrase upon installation. Support for multifactor authentication is recommended.

[5] Interfaces are a boundary between the IoT device and entities where interactions take place. This includes digital or network interfaces, as well as local interfaces, such as graphical user interfaces.
[6] IETF RFC6092 Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service [RFC6092] is a relevant source for more specific guidance related to IPv6 interface cybersecurity.

2. Placing a timeout limit on account sessions.
3. Limiting each user to only one active login session at a time.
4. Protecting against authentication brute force attacks (e.g., limiting failed log-in attempts).
5. Making physical developer interface ports (e.g., JTAG) inaccessible from the outside of a component.
6. Ensuring unused OSI Layer 4 ports are not revealed during scans.
7. Prohibiting the reply to requests over a port for an API or Protocol that doesn't use that port.

Related Standards Requirements[7]*:*

BBF GEN.DESIGN.14, GEN.OPS.21, MGMT.LOCAL.1, MGMT.LOCAL.5, MGMT.LOCAL.11, MGMT.REMOTE.WEB.2, MGMT.REMOTE.WEB.9, IF.LAN.WIRELESS.AP.20, SEC.GEN.1, SEC.GEN.8, SEC.USERINTERFACE.2, SEC.USERINTERFACE.3, SEC.USERINTERFACE.4, SEC.USERINTERFACE.5, SEC.USERINTERFACE.6, SEC.USERINTERFACE.7, SEC.USERINTERFACE.9

CL OOB-001, OOB-004, OOB-006, OOB-008, OOB-010, OOB-012, MI-004, MI-007, MI-008, MI-009, MI-010, MI-013, DIAG-002, NETS-007, NETS-008, NETA-001, NETA-002, NETA-003, MI-002

BSI (3.1), (3.1.2.1), (3.2), (4.1.1), (4.4)

IMDA 4.1.1, 4.1.2, 4.2, 4.2.1

SP 800-193 4.1.1(5), 4.2.4(3-4)

Control of access to the consumer-grade router's network is critical to the cybersecurity it provides to customers. Generally, on-boarding to the router's network uses a single factor, password-based authentication method (e.g., WPA key). This on-boarding process can incorporate explicit network owner approval or some other additional factor to reduce unauthorized access to the network.

A.4.11. Interface Access Control 1c

For all interfaces, access and modification privileges are limited. For example, access to the administration page and changes to the configuration should be limited to authenticated users authorized to make such changes.

Related Standards Requirements:

BBF MGMT.REMOTE.WEB.3, MGMT.REMOTE.WEB.4, SEC.GEN.7

CL MI-006

[7] IMDA 4.1.2 discusses password requirements, as does BSI (4.1.1). IMDA's requirement is more stringent than BSIs (i.e., minimum password character length of 10 versus 8) and is recommended by the BSI requirement.

BSI (3.1), (3.1.2), (3.2)

IMDA 4.2

SP 800-193 4.2.3(3), 4.2.4(1)

A.5. Interface Access Control 2

Some, but not necessarily all, consumer-grade router product components have the means to protect and maintain interface access control.

A.5.12. Interface Access Control 2a

Validate data received by the consumer-grade router product and validate that data shared among router product components match specified definitions of format and content.

Related Standards Requirements:

BBF *None*

CL MI-012, NETS-006

BSI *None*

IMDA 4.6

SP 800-193 4.1.1(6, 8), 4.2.4(2)

A.5.13. Interface Access Control 2b

Prevent unauthorized transmissions or access to other product components.

Related Standards Requirements:

BBF WAN.DoS.1, WAN.DoS.2, WAN.DoS.3, WAN.DoS.4, WAN.DoS.5

CL MI-005, NETS-006

BSI (3.1.2), (4.3), (4.7), (4.9)

IMDA 4.2.1

A.5.14. Interface Access Control 2c

Maintain appropriate access control during initial connection (i.e., onboarding) and when reestablishing connectivity after disconnection or outage.

Related Standards Requirements:

BBF *None*

CL *None*

BSI (3.1.2.3), (3.2)

IMDA 4.1.1, 4.2, 4.2.1

A.6. Software Update

The software (including firmware) of all consumer-grade router product components can be updated by authenticated and authorized individuals, services, and other router product components only by using a secure and configurable mechanism, as appropriate for each router product component.

A.6.15. Software Update 1

Each consumer-grade router product component can receive, verify, and apply verified software updates that are signed and firmware updates that are signed and may be encrypted.

Related Standards Requirements:

BBF GEN.OPS.22, GEN.OPS.23

CL KEY-004, KEY-005, SB-001, SU-001, SU-005, SBOM-009, SB-002, SU-003

BSI (4.2)

IMDA 4.3

SP 800-193 4.1.1(4), 4.1.2(1-4), 4.2.1.1, 4.2.1.2(1), 4.2.4(3, 5), 4.3.1(2), 4.4.1(2-6)

All software update packages should be signed by the source of the update (e.g., manufacturer), but when applicable (e.g., when routers are leased from ISPs) other entities may also cryptographically sign updates, adding another layer of security.

A.6.16. Software Update 2

The consumer-grade router product implements measures to keep software (including firmware) on router product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via router components), including provisions to prevent firmware rollback attacks (e.g., not allowing the rollback of firmware to a version with known vulnerabilities).

Related Standards Requirements:

BBF GEN.OPS.19, GEN.OPS.20, MGMT.LOCAL.15, MGMT.LOCAL.21, MGMT.LOCAL.22

CL SB-003, SU-002, SU-006, SBOM-003, SBOM-007, SBOM-008, SBOM-010

BSI (4.1.2), (4.2)

IMDA 4.3

SP 800-193 4.1.2(5), 4.2.1.3, 4.4.1(1, 10, 11, 13)

A.6.17. Software Update 3†

The integrity of data, including configuration, is preserved when an update is applied. In the case of a failed update, the product should revert to a usable state.

Related Standards Requirements:

BBF GEN.OPS.15, GEN.OPS.24

CL SU-004

BSI *None*

IMDA *None*

SP 800-193 4.3.1(3)

A.7. Cybersecurity State Awareness

The consumer-grade router product supports detection of cybersecurity incidents affecting or affected by product components and the data they store and transmit.

A.7.18. Cybersecurity State Awareness 1

The consumer-grade router product securely collects and stores information about the status of its components. This aids in identifying cybersecurity incidents that affect the router product and the data it manages. Information that the router product shall provide includes login attempts, administrative events, system status, firewall status, status of all product components, and time synchronization. Deletion of this log information should be limited to resetting the product to factory default settings.

Related Standards Requirements:

BBF GEN.OPS.18, LAN.FW.2, LAN.FW.3, LAN.FW.4, MGMT.LOCAL.18, MGMT.LOCAL.20

CL SB-004, LOG-001, LOG-002, LOG-003, LOG-004, LOG-005, SB-002, TS-001

BSI (4.1.2), (4.8)

IMDA *None*

SP 800-193 4.1.1(4), 4.1.3, 4.3.1(1, 5), 4.3.2(1-2, 4), 4.4.1(8), 4.4.2(3)

A.7.19. Cybersecurity State Awareness 2†

The consumer-grade router product informs authorized entities about changes in cybersecurity information and responds to any changes.

Related Standards Requirements:

BBF GEN.OPS.6

CL AR-002

BSI *None*

IMDA *None*

SP 800-193 4.1.3(3), 4.3.1(2-4, 6), 4.3.2(3, 5-6), 4.4.1(9, 11), 4.4.2(9)

Appendix B. Non-Technical Outcome Considerations

Table 1 below states the non-technical cybersecurity outcomes NIST has defined for the consumer-grade router profile with the requirements from the four standards that are related to these outcomes.

Table 1. Non-technical cybersecurity outcomes and requirements from consumer-grade router standards

Consumer-Grade Router Profile Non-Technical Outcome	Related Requirements
Documentation *The consumer-grade router product developer creates, gathers, and stores information relevant to cybersecurity of the product and its product components prior to customer purchase, and throughout the development of a product and its subsequent lifecycle.*	**CL** HR-005, MI-014, DIAG-001, SBOM-004, SBOM-005
Information and Query Reception *The consumer-grade router product developer has the ability to receive information relevant to cybersecurity and respond to queries from the customer and others about information relevant to cybersecurity.*	-
Information Dissemination *The consumer-grade router product developer broadcasts (e.g., to the public) and distributes (e.g., to the customer or others in the product ecosystem) information relevant to cybersecurity.*	**CL** AR-001, SBOM-011 **BSI** (4.2) **IMDA** 4.3e
Education and Awareness *The consumer-grade router product developer creates awareness of and educates customers and others in the product ecosystem about cybersecurity-related information (e.g., considerations, features, risks) related to the router product and its components.*	-

The standards do not thoroughly address the non-technical outcomes, but NIST reiterates that consumer-grade router products should be supported by all the non-technical outcomes included in this profile. Implementation of non-technical outcomes may not have to be tailored for a product type and may be deployed similarly for different digital products. For example, procedures for a vulnerability management program are not likely to vary significantly in implementation for consumer-grade routers, smart thermostats, personal computers, etc. though the scale may be different due to the size and complexity of the software involved. Thus, product-agnostic approaches to the non-technical outcomes as discussed in the *Product Development Cybersecurity Handbook* are recommended in addition to the non-technical requirements included in the four standards. The handbook guides a developer through important cybersecurity considerations when developing digital products. Though the handbook is generally contextualized around IoT products, the concepts discussed can apply to any digital product with a physical component in the customer's environment (e.g., router device). There are many non-technical cybersecurity considerations discussed in the handbook, but the following are key considerations for consumer-grade router products given the role these devices play in home networks:

> **Risk management** in both planning and execution of consumer-grade router products will help identify and mitigate cybersecurity risks throughout the product lifecycle. Risks faced by router products can be significant. Router devices have a unique vantage and

access to home networks. They also have robust networking capabilities, giving them utility for a wide range of attacks. Other router product components present their own risks. Backends may aggregate data from one or more customers, making them attractive targets for attackers. Mobile applications may be installed in relatively hostile environments due to malware and other vectors of attack. ISO 31000 [ISO31000] is a foundational resource that developers should use for risk management. NIST's *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37 Rev. 2 [SP800-37r2] may also be useful guidance for risk management.

Secure development processes for both hardware and software are also critical for the cybersecurity of consumer-grade router products. *Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*, NISTIR 8320 [IR8320] may be a helpful resource for router product developers as they consider hardware in relation the cybersecurity of their products. A recommended resource available to all software developers is NIST's Secure Software Development Framework [SSDF], which includes fundamental, sound, and secure software development practices. The SSDF can help a software developer align and prioritize its secure software development activities with its business and mission requirements, risk tolerances, and resources. Like NISTIR 8425, the SSDF's practices are outcome-based. The SSDF's practices, tasks, and implementation examples represent a starting point to consider. In the context of consumer-grade router products, all SSDF practices are recommended to be implemented as part of the software development lifecycle of a router products' firmware and other software. Some SSDF practices may be more applicable to certain types of software. Appendix B presents a detailed crosswalk listing all SSDF tasks and their applicability to three kinds of firmware or software commonly part of consumer-grade router products: router firmware, mobile applications, remote backend or web applications.

Vulnerability management is critical for consumer-grade router products and is addressed by portions of all four non-technical cybersecurity outcomes. Manufacturers should develop a robust vulnerability management plan for their products that will identify vulnerabilities to quickly and effectively mitigate them in their products. For this, they should use ISO/IEC 29147 [ISO29147] and ISO/IEC 30111 [ISO30111], which are important resources for vulnerability disclosure and handling, respectively. From NIST, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, SP 800-40 Rev. 4 [SP800-40r4] can also be a helpful resource for product developers as they plan for, discover, prioritize, and respond to vulnerabilities in their products.

Customer engagement on cybersecurity, which is called Education and Awareness in the non-technical outcomes, facilitates use of technical cybersecurity features and adoption of good cybersecurity by customers. ISO/IEC/IEEE 26514 [ISO26514] provides guidance on the design and development of information for users, which may be helpful

to and is recommended for product developers as they create the manual and other materials for the device that a customer may seek out for cybersecurity instructions related to the product.

These are highlighted considerations. Manufacturers should implement robust non-technical cybersecurity support that includes all aspects of documenting cybersecurity pertinent information, establishing means to receive and disseminate cybersecurity pertinent information related to the product, and fostering cybersecurity education and awareness among customers related to the product.

Appendix C. Consumer-Grade Router Acquisition Scenarios Discussion

Routers are network devices that forward data packets, most commonly Internet Protocol (IP) packets, between networked systems. Their physical interfaces may be a combination of wired (e.g., Ethernet) and wireless (e.g., Wi-Fi, long term evolution (LTE), 5G). *Consumer-grade* identifies those routers that may appear in an individual's residence such that their primary use case is residential rather than enterprise, industrial, etc. However, some small businesses may choose to use consumer-grade equipment given the limited performance needs of those businesses. The presumption for consumer equipment or small businesses that use consumer-grade equipment is that the manufacturer cannot assume the user has cybersecurity expertise or the ability to take significant action to secure the product.

Consumer-grade routers may be acquired by households in at least two ways[8]:

1. Purchase of the equipment directly from a retailer.
2. Bundling and/or renting of the equipment from a service provider.

Each of these scenarios may have implications for how cybersecurity outcomes could be met by the consumer-grade router product. Consumer-owned equipment may be fully managed by the household or may have some security services provided externally. Alternatively, bundled and/or rental equipment will likely be managed in part by the service provider.

Table 2. Scope Coverage of the Consumer-Grade Router Standards Analyzed

Consumer-Grade Router Standard	Applicable to Consumer-Owned Routers?	Applicable to ISP-Owned, Customer-Leased Routers?
TR-124 Issue 8 [BBF]	Yes	Yes
Gateway Device Security Best Common Practices [CableLabs]	Yes	Yes
Secure Broadband Routers [BSI]	Yes	Yes
Security Requirements for Residential Gateways [IMDA]	Yes	No

As summarized in Table 2, the scope statements of three of the four standards examined either make no distinction about how the router is acquired by customers or state that the guidance applies to both scenarios.

The Broadband Forum's document does not distinguish between the two methods of acquisition, stating "a Residential Gateway implementing the general requirements of TR-124 will incorporate at least one embedded WAN interface, routing, bridging, a basic or enhanced firewall, one or multiple LAN interfaces and home networking functionality that can be deployed as a consumer self-installable device." It notably highlights that included are products that can be deployed as "consumer self-installable," which includes the customer purchased scenario, as well as most instances of service provider supplied routers.

CableLabs directly acknowledges both scenarios: "This Gateway Device Security document specifies best common practices to serve as an industry metric for retail and leased devices

[8] As of 2022, about half of consumer-grade routers are received from ISPs rather than acquired by customers directly. [ParksRouterResearch]

(both gateways and cable modems) for security—this includes manufacturing process, supply chain, hardware and firmware configuration procedures, software, and management protocols."

The German Federal Office for Information Security (BSI) focuses its requirements on how the product is used rather than acquired, stating "In scope of this Technical Guideline are requirements on a router as a hardware component with an installed operating system and services provided to an end-user. The router serves the purpose of establishing a connection to the infrastructure of an Internet Access Provider (IAP) to gain internet access. From the end-user's perspective the router offers a gateway to the internet as well as management functionalities for the end-user's private network. The Technical Guideline describes requirements on the router that should be implemented to offer a secure operation of the router for the end-user." Thus, the requirements can be applied to the scenario of when customers purchase a router and when a router is provided by or rented from a service provider.

Unlike the others, the IMDA alludes to a focus on only routers purchased by customers, stating that the goal is "ensuring that these devices are better protected when purchased and deployed by consumers."

Appendix D. Crosswalk Between Secure Software Development Tasks and Consumer-Grade Router Product Software Type

This appendix presents an informational crosswalk listing all SSDF tasks, copied directly from the SSDF. The SSDF tasks can be applied to three kinds of code commonly part of consumer-grade router products: router firmware, mobile applications, and remote backend or web applications.

- *Router firmware* is a form of device firmware specific to consumer-grade router devices. *Device firmware* generally is "the collection of non-host processor firmware and Expansion ROM firmware that is only used by a specific device. This firmware is typically provided by the device manufacturer" [SP800-193].
- *Mobile applications* references software intended to be installed on handheld or portable devices. .. For example, applications made to run on Apple's iOS or Android operating systems.
- *Remote backend or web applications* are software intended to be hosted and executed on dedicated or shared servers that may provide services to many products at once. For example, code supporting consumer-grade routers that is hosted in a cloud environment.

Table 3 below indicates which SSDF tasks may be most appropriate for each kind of firmware or software. SSDF tasks that may be appropriate to a software type, but utilization of the task may be contextual to the development process or environment, are noted with (parentheses).

Table 3. Crosswalk between consumer-grade router product software types and SSDF tasks.

SSDF Task	Recommended for Router…
PO.1.1: Identify and document all security requirements for the organization's software development infrastructures and processes and maintain the requirements over time.	Firmware, Mobile App., Web App.
PO.1.2: Identify and document all security requirements for organization-developed software to meet, and maintain the requirements over time.	Firmware, Mobile App., Web App.
PO.1.3: Communicate requirements to all third parties who will provide commercial software components to the organization for reuse by the organization's own software. [Formerly PW.3.1]	Firmware, Mobile App., Web App.
PO.2.1: Create new roles and alter responsibilities for existing roles as needed to encompass all parts of the SDLC. Periodically review and maintain the defined roles and responsibilities, updating them as needed.	Firmware, Mobile App., Web App.
PO.2.2: Provide role-based training for all personnel with responsibilities that contribute to secure development. Periodically review personnel proficiency and role-based training, and update the training as needed.	Firmware, Mobile App., Web App.
PO.2.3: Obtain upper management or authorizing official commitment to secure development, and convey that commitment to all with development-related roles and responsibilities.	(Firmware), (Mobile App.), (Web App.)

SSDF Task	Recommended for Router…
PO.3.1: Specify which tools or tool types must or should be included in each toolchain to mitigate identified risks, as well as how the toolchain components are to be integrated with each other.	Firmware, Mobile App., Web App.
PO.3.2: Follow recommended security practices to deploy, operate, and maintain tools and toolchains.	Firmware, Mobile App., Web App.
PO.3.3: Configure tools to generate artifacts of their support of secure software development practices as defined by the organization.	(Firmware), (Mobile App.), (Web App.)
PO.4.1: Define criteria for software security checks and track throughout the SDLC.	(Firmware), (Mobile App.), (Web App.)
PO.4.2: Implement processes, mechanisms, etc. to gather and safeguard the necessary information in support of the criteria.	Firmware, Mobile App., Web App.
PO.5.1: Separate and protect each environment involved in software development.	Firmware, Mobile App., Web App.
PO.5.2: Secure and harden development endpoints (i.e., endpoints for software designers, developers, testers, builders, etc.) to perform development-related tasks using a risk-based approach.	Firmware
PS.1.1: Store all forms of code – including source code, executable code, and configuration-as-code – based on the principle of least privilege so that only authorized personnel, tools, services, etc. have access.	Firmware, Mobile App., Web App.
PS.2.1: Make software integrity verification information available to software acquirers.	(Web App.)
PS.3.1: Securely archive the necessary files and supporting data (e.g., integrity verification information, provenance data) to be retained for each software release.	Firmware, Mobile App.
PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (e.g., in a software bill of materials).	Firmware, Mobile App.
PW.1.1: Use forms of risk modeling – such as threat modeling, attack modeling, or attack surface mapping – to help assess the security risk for the software.	Firmware, (Mobile App.), (Web App.)
PW.1.2: Track and maintain the software's security requirements, risks, and design decisions.	Firmware, Mobile App., Web App.
PW.1.3: Where appropriate, build in support for using standardized security features and services (e.g., enabling software to integrate with existing log management, identity management, access control, and vulnerability management systems) instead of creating proprietary implementations of security features and services. [Formerly PW.4.3]	Firmware, Mobile App., Web App.
PW.2.1: Have 1) a qualified person (or people) who were not involved with the design and/or 2) automated processes instantiated in the toolchain review the software design to confirm and enforce that it meets all of the security requirements and satisfactorily addresses the identified risk information.	Firmware
PW.4.1: Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from commercial, open-source, and other third-party developers for use by the organization's software.	Firmware, Mobile App., Web App.

SSDF Task	Recommended for Router…
PW.4.2: Create and maintain well-secured software components in-house following SDLC processes to meet common internal software development needs that cannot be better met by third-party software components.	Firmware, Mobile App., Web App.
PW.4.4: Verify that acquired commercial, open-source, and all other third-party software components comply with the requirements, as defined by the organization, throughout their life cycles.	Firmware, Mobile App., Web App.
PW.5.1: Follow all secure coding practices that are appropriate to the development languages and environment to meet the organization's requirements.	Firmware, Mobile App., Web App.
PW.6.1: Use compiler, interpreter, and build tools that offer features to improve executable security.	Firmware, Mobile App., Web App.
PW.6.2: Determine which compiler, interpreter, and build tool features should be used and how each should be configured, then implement and use the approved configurations.	Firmware, Mobile App., Web App.
PW.7.1: Determine whether code review (a person looks directly at the code to find issues) and/or code analysis (tools are used to find issues in code, either in a fully automated way or in conjunction with a person) should be used, as defined by the organization.	Firmware, Mobile App., Web App.
PW.7.2: Perform the code review and/or code analysis based on the organization's secure coding standards, and record and triage all discovered issues and recommended remediations in the development team's workflow or issue tracking system.	Firmware, Mobile App., Web App.
PW.8.1: Determine whether executable code testing should be performed to find vulnerabilities not identified by previous reviews, analysis, or testing and, if so, which types of testing should be used.	Firmware, Mobile App., Web App.
PW.8.2: Scope the testing, design the tests, perform the testing, and document the results, including recording and triaging all discovered issues and recommended remediations in the development team's workflow or issue tracking system.	Firmware, (Mobile App.), (Web App.)
PW.9.1: Define a secure baseline by determining how to configure each setting that has an effect on security or a security-related setting so that the default settings are secure and do not weaken the security functions provided by the platform, network infrastructure, or services.	Firmware, Mobile App., Web App.
PW.9.2: Implement the default settings (or groups of default settings, if applicable), and document each setting for software administrators.	Firmware, Mobile App., Web App.
RV.1.1: Gather information from software acquirers, users, and public sources on potential vulnerabilities in the software and third-party components that the software uses, and investigate all credible reports.	Firmware, Mobile App., Web App.
RV.1.2: Review, analyze, and/or test the software's code to identify or confirm the presence of previously undetected vulnerabilities.	Firmware, Mobile App., Web App.
RV.1.3: Have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy.	Firmware, Mobile App., Web App.
RV.2.1: Analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response.	Firmware, Mobile App., Web App.

SSDF Task	Recommended for Router…
RV.2.2: Plan and implement risk responses for vulnerabilities.	Firmware, Mobile App., Web App.
RV.3.1: Analyze identified vulnerabilities to determine their root causes.	Firmware, Mobile App., Web App.
RV.3.2: Analyze the root causes over time to identify patterns, such as a particular secure coding practice not being followed consistently.	Firmware, Mobile App., Web App.
RV.3.3: Review the software for similar vulnerabilities to eradicate a class of vulnerabilities, and proactively fix them rather than waiting for external reports.	(Firmware), (Mobile App.), (Web App.)
RV.3.4: Review the SDLC process, and update it if appropriate to prevent (or reduce the likelihood of) the root cause recurring in updates to the software or in new software that is created.	(Firmware), (Mobile App.), (Web App.)

Appendix E. List of Symbols, Abbreviations, and Acronyms

BBF
Broadband Forum

BSI
Federal Office for Information Security

CL
CableLabs

IMDA
Infocomm Media Development Authority

IoT
Internet of Things

Appendix F. Glossary

consumer-grade router device
Networking devices that are primarily intended for residential use and can be installed by the customer. Routers forward data packets, most commonly Internet Protocol (IP) packets, between networked systems.

consumer-grade router product
Consumer-grade router device and any additional product components (e.g., backend, smartphone application) that are necessary to use the consumer-grade router device beyond basic operational features. [IR8425, adapted]

cybersecurity outcome
Statement of what is expected either from a product or from an organization in support of a product related to the cybersecurity of that product. Can be technical, in the form of product cybersecurity capabilities or non-technical, in the form of non-technical supporting capabilities.

non-technical supporting capability
Non-technical supporting capabilities are actions an organization performs in support of the cybersecurity of a product. [IR8425, adapted]

product cybersecurity capability
Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software). [IR8425]