NIST Internal Report
Publication Identifier

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Initial Preliminary Draft

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

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

NIST Internal Report
Publication Identifier

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Initial Preliminary Draft

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

David Lemire
Brad Hoehn
Chris Evans
HII

December 2023

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

NIST Technical Series Policies

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

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

Preliminary Draft Release Period

November 30th, 2023 - December 21st, 2023

Submit Feedback and Comments

iotsecurity@nist.gov

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

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

Abstract

Ensuring the security of routers is crucial for safeguarding not only individual privacy but also the integrity of entire networks. With the increasing prevalence of smart homes, IoT devices, and remote work setups, the significance of consumer-grade router cybersecurity has expanded, as these devices 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 consumer-grade router standards.

Keywords

Cybersecurity; consumer-grade routers

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Audience

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

Note to Reviewers

On July 18th, 2023, the White House announced the next steps for the Cybersecurity Labeling Program for Smart Devices to Protect American Consumers, referred to as the "U.S. Cyber Trust Mark." [WHAnnouncement] In addition to announcing participation by the Federal Communications Commission and Departments of Energy and State, the White House also directed NIST to "immediately undertake an effort to define cybersecurity requirements for consumer-grade routers—a higher-risk type of product that, if compromised, can be used to eavesdrop, steal passwords, and attack other devices and high value networks." In response, NIST worked to develop these requirements with a standards-based, transparent, community-involved process. Two discussion essays, one including a standards crosswalk [StandardsCrosswalk] were published for community feedback. **This draft is a pre-comment NISTIR preliminary draft intended to inform feedback at a discussion forum NIST will host on December 7th, 2023**. **An official NISTIR public draft release and comment period will occur after December 7th, 2023.**

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: iotsecurity@nist.gov

Table of Contents

List of Tables

List of Figures

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 and the internet. A compromised router opens the door to a host of potential threats, ranging from unauthorized access to sensitive information to the possibility of malicious attacks on connected devices. Ensuring the security of routers is crucial for safeguarding not only individual privacy but also the integrity of entire networks. With the increasing prevalence of smart homes, IoT devices, and remote work setups, the significance of consumer-grade router cybersecurity has expanded, as these devices often rely on routers in the home to connect to the internet. A secure home router (i.e., one that is consumer-grade) not only protects U.S. citizens against data theft and other cyberattacks but also contributes to the overall resilience of the global digital infrastructure. As technology advances, the need for robust router cybersecurity becomes ever more critical to maintain a safe and trustworthy digital environment.

This report presents the *consumer-grade router profile*, which includes cybersecurity outcomes for consumer-grade routers and associated requirements from consumer-grade router standards. In this context, outcomes are broad, flexible guidelines that can apply, albeit differently, to different use cases and contexts, while requirements are targeted specifications that can define meeting an outcome for a specific use case, context, technology, etc. Four existing standards[1] for consumer-grade routers are referred to in this document:

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]

NIST recommends use of the full set of requirements from all four consumer-grade router standards. Requirements from the standards for consumer-grade routers focused primarily on the router device. A few requirements addressed non-technical cybersecurity support and no requirements were given for other product components (e.g., mobile application). Thus, **the requirements from the four standards address technical cybersecurity for consumer-grade router devices**, but not the non-technical cybersecurity outcomes, nor cybersecurity for product components other than the router device (e.g., backend, mobile app).

Full support of all outcomes by all consumer-grade router product components is expected, as shown in **Table 1** below.[2] Additional requirements are needed to meet all consumer-grade router product non-technical outcomes. If a consumer-grade router product has additional product

[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 identification of requirements for these gaps is on-going and NIST welcomes recommendations of standards and guidance that can inform the process.

components, such as a smart phone mobile application, additional requirements would also be necessary to meet the outcomes for the complete consumer-grade router product. Work on identifying these additional requirements is on-going and NIST welcomes feedback on standards and guidance applicable to these gaps for consumer-grade routers.

Table 1. Requirements for all consumer-grade router product components

Consumer-grade router…	Technical Outcomes	Non-technical Outcomes
Device	Sections 3.1-3.7	Section 3.8 + *TBD*
Additional Product Components	*TBD*	*TBD*

The rest of this document is structured as follows:

- Section 2 states the recommended scope of consumer-grade router products.
- Section 3 presents an informative cross-walk between the technical and non-technical cybersecurity outcomes for consumer-grade router products and the related requirements from the four consumer-grade router standards.
- Section 4 concludes the document.

2. Scope of Consumer-Grade Routers

This profile identifies minimum cybersecurity for consumer-grade routers. Consumer-grade routers are defined as networking devices that forward data packets, most commonly Internet Protocol (IP) packets, between networked systems which are primarily intended for residential use and can be installed by the customer. The profile makes no distinction in its cybersecurity recommendations with regards to whether the product is owned by the customer or leased. Additional discussion and justification for this scope can be found in Appendix A.

Cybersecurity outcomes and requirements for products should be scoped to all product components (e.g., smartphone applications) in addition to the router device. **Fig. 1** below shows an example consumer-grade router product where the router device is supported by both a backend and smartphone application.

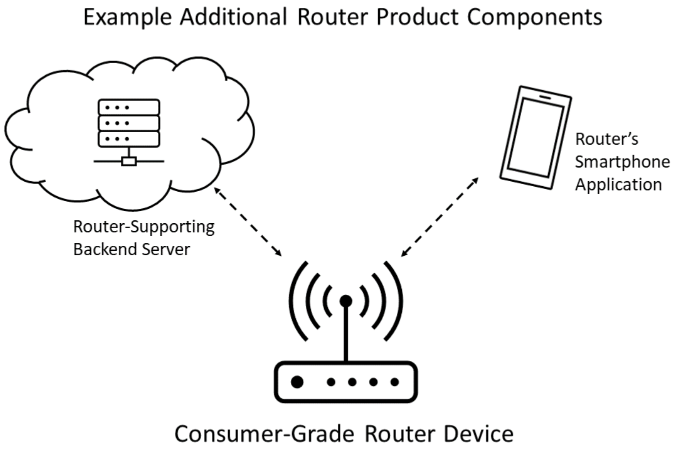
Example Additional Router Product Components
Router-Supporting Backend Server
Router's Smartphone Application
Consumer-Grade Router Device

Fig. 1. An example consumer-grade router product that includes a smartphone application and backend server in addition to the router device.

Due to available standards specific to the product type, the requirements used to define the profile focuses on the cybersecurity of the consumer-grade router device, but the presence of other product components should not be ignored. NIST recommends the use of general standards or guidance to understand appropriate cybersecurity for these other product components.[3]

3. Crosswalk between NISTIR 8425 Outcomes and Consumer-Grade Router Cybersecurity Requirements

This section provides additional information about how the requirements from the four router standards relate to the consumer-grade router profile outcomes.

Sections 3.1-3.7 below shows which requirements from the four consumer-grade router standards are related to the technical outcomes that have been expanded and adapted from *Profile of the IoT Core Baseline for Consumer IoT Products*, NISTIR 8425 [IR8425] for consumer-grade routers. Each subsection from 3.1-3.7 states the high-level outcome along with each sub-outcome that defines the high-level outcome. For each sub-outcome, a set of related requirements from the four consumer-grade router standards are 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* [CL]

BSI's *Secure Broadband Routers* [BSI]

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

Requirements related to the non-technical cybersecurity outcomes from these standards are presented in Section 3.8.

3.1. Asset Identification

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

3.1.1. Asset Identification 1

The consumer-grade router product can be uniquely identified by the customer and other authorized entities.

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)

[3] NIST is working to identify standards and guidance related to IoT product cybersecurity, technical and non-technical, for the full product scope, including all IoT product components. Please refer to https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program for additional information.

IMDA *None*

3.1.2. 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 consumer-grade router standards were mapped to this outcome. This outcome relates to a specifically product-wide concept (i.e., inventory of product components), and thus it is expected that standards including device-focused requirements would not address a product-focused outcome.

3.2. 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 consumer-grade router product components.

3.2.1. Product Configuration 1

Authorized individuals (i.e., customer), services, and other consumer-grade router product components can change the configuration settings of the consumer-grade router product via one or more consumer-grade router product components.

Related Standards Requirements:

BBF MGMT.LOCAL.2

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

BSI (3.1.2)[3], (3.1.2)[3], (3.1.2)[4], (3.1.2.1), (3.1.2.2), (4), (4.1.1)[1], (4.1.1)[1], (4.1.1)[3], (4.1.1)[6], (4.1.1)[6], (4.1.1)[7], (4.1.2)[Table6], (4.1.2)[2], (4.2)[2], (4.3)[2], (4.3)[3], (4.4), (4.5), (4.5), (4.8), (4.8), (4.9), (4.10)[1]

IMDA 4.2, 4.2.3, 4.4

3.2.2. Product Configuration 2

Authorized individuals (i.e., customer), services, and other consumer-grade router product components have the ability to restore the consumer-grade router product to a secure default (i.e., uninitialized) configuration.

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

3.2.3. Product Configuration 3

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

No requirements from the consumer-grade router standards were mapped to this outcome. This outcome relates to a specifically product-wide concept (i.e., application of configuration across all product components), and thus it is expected that standards including device-focused requirements would not address a product-focused outcome.

3.3. Data Protection

The consumer-grade router product protects data stored across all consumer-grade router product components and transmitted both between consumer-grade router product components and outside the consumer-grade router product from unauthorized access, disclosure, and modification.

3.3.1. Data Protection 1

Each consumer-grade router product component protects data it stores via secure means.

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)[7]

IMDA 4.5

3.3.2. 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, etc.

Related Standards Requirements:

BBF *None*

CL OOB-009

BSI (4.6)

IMDA 4.2.3

3.3.3. Data Protection 3

When data are sent between consumer-grade router product components or outside the product, protections are used for the data transmission.

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), (3.1.2.2), (4.1.1)[1], (4.1.1)[6], (4.1.1)[6], (4.1.1)[7], (4.1.2)[2], (4.1.2)[2], (4.4), (4.10)[1]

IMDA 4.2.2, 4.2.5

3.4. Interface Access Control 1

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

3.4.1. Interface Access Control 1a

Use and have access only to interfaces necessary for the consumer-grade router product's operation. All other channels and access to channels are removed or secured.

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), (3.1)[2], (3.1.2)[3], (3.2)[3], (4.1.1)[6], (4.1.1)[5]

IMDA 4.2, 4.2.1

3.4.2. Interface Access Control 1b

For all interfaces necessary for the consumer-grade router product's use, access control measures are in place.[4]

Related Standards Requirements[5]*:*

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

[4] 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.

[5] IMDA 4.1.2 discusses password requirements, as does BSI (4.1.1)[1]. IMDA's requirement is more stringent than BSIs (i.e., minimum password character length of 10 versus 8) and is recommend with BSI's requirement.

BSI (3.1)[1,2], (3.1.2.1), (3.2)[3], (3.2)[3], (3.2)[3], (4.1.1)[1], (4.1.1)[1], (4.1.1)[2], (4.1.1)[2], (4.1.1)[5], (4.4)

IMDA 4.1, 4.1.1, 4.1.2, 4.2, 4.2.1

3.4.3. Interface Access Control1c

For all interfaces, access and modification privileges are limited.

Related Standards Requirements:

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

CL MI-006

BSI (3.1)[1,2], (3.1.2)[4], (3.2)[3], (3.2)[3], (3.2)[3]

IMDA 4.2

3.5. Interface Access Control 2

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

3.5.1. Interface Access Control 2a

Validate that data shared among consumer-grade 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

3.5.2. 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)[3], (3.1.2)[3], (3.1.2)[4], (4.3)[1], (4.3)[3], (4.7)[1], (4.7)[1], (4.9)[1], (4.9)[1]

IMDA 4.2.1

3.5.3. 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)[2]

IMDA 4.1, 4.1.1, 4.2, 4.2.1

3.6. Software Update

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

3.6.1. Software Update 1

Each consumer-grade router product component can receive, verify, and apply verified software updates.

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)[1], (4.2)[3], (4.2)[3], (4.2)[6]

IMDA 4.3

3.6.2. Software Update 2

The consumer-grade router product implements measures to keep software on consumer-grade router product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via consumer-grade router components).

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)[Table 6], (4.2)[1], (4.2)[2]

IMDA 4.3

3.6.3. Software Update 3 (New Addition Relative to NISTIR 8425)

New addition relative to NISTIR 8425.

Integrity of data, including configuration is preserved when an update is applied.

Related Standards Requirements:

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

CL SU-004

BSI *None*

IMDA *None*

3.7. Cybersecurity State Awareness

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

3.7.1. Cybersecurity State Awareness 1

The consumer-grade router product securely captures and records information about the state of consumer-grade router components that can be used to detect cybersecurity incidents affecting or affected by consumer-grade router product components and the data they store and transmit.

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)[1], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[Table 6], (4.1.2)[2], (4.8)

IMDA *None*

3.7.2. Cybersecurity State Awareness 2 (New Addition Relative to NISTIR 8425)

New addition relative to NISTIR 8425.

The consumer-grade router product can inform authorized entities about or respond directly to changes in cybersecurity information.

Related Standards Requirements:

BBF GEN.OPS.6

CL AR-002

BSI *None*

IMDA *None*

3.8. Non-Technical Outcomes

Table 2 below states the non-technical cybersecurity outcomes NIST has defined for the consumer-grade router profile with the requirements from the four consumer-grade router standards that related to these outcomes.

Table 2. 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 consumer-grade router 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 consumer-grade router product ecosystem) information relevant to cybersecurity.*	**CL** AR-001, SBOM-011 **BSI** (4.2)[4] **IMDA** 4.3e
Education and Awareness *The consumer-grade router product developer creates awareness of and educates customers and others in the consumer-grade router product ecosystem about cybersecurity-related information (e.g., considerations, features) related to the consumer-grade router product and its product components.*	-

4. Conclusion

This consumer-grade router profile can help manufacturers and others determine adequate cybersecurity to develop into their products. These recommendations draw from current best practices and guides broad adoption of accepted and vetted cybersecurity for consumer-grade routers of any type. NIST reiterates the importance of a product-wide perspective on cybersecurity and further recommends consideration of it 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/

[StandardsCrosswalk] National Institute of Standards and Technology (2023) Crosswalk of Consumer-Grade Router Cybersecurity Standards to NIST's Baseline for Consumer IoT Products. (National Institute of Standards and Technology, Gaithersburg, MD). https://www.nist.gov/system/files/documents/2023/10/25/Consumer-Grade%20Router%20Standards%20Crosswalk.pdf

[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/resources/tr-124-issue-8-functional-requirements-for-broadband-residential-gateway-devices

[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

[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

[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

[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. Consumer-Grade Router Scope Discussion

Routers are network devices that forward data packets, most commonly Internet Protocol (IP) packets, between networked systems. They may be wired (e.g., Ethernet), wireless (e.g., Wi-Fi), or both. *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 an ability to take significant action to secure the product.

Consumer-grade routers may be acquired by households in at least two ways[6]:

1. Purchase of the equipment directly from a retailer.

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

2. Bundling and/or renting of the equipment from a service provider.

Each of these vectors 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/rental equipment will likely be managed in part by the service provider. Additionally, these variations and use cases potentially have significantly different features and capabilities to consider as part of the product, and thus may have different risk profiles and cybersecurity outcomes.

Table 3. Scope Coverage of the Consumer-Grade Router Standards Analyzed

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

As summarized in **Table 3**, the scope statements of three of four standards examined related to consumer-grade router cybersecurity either make no distinction about how the router is acquired by customers or state that the guidance applies to both contexts.

BBF similarly 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 in scope are products that can be deployed as “consumer self-installable,” but this includes the customer purchased context, as well as most instances of service provider supplied routers.

CableLabs directly acknowledges both contexts and scopes in both: “This Gateway Device Security document specifies best common practices to serve as an industry metric for retail and leased devices (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 on scoping its requirements related to 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 case 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 scope of only routers purchased by customers, stating that the goal is “ensuring that these devices are better protected when purchased and deployed by consumers.”

Appendix B. 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 C. Glossary

Consumer-Grade Router Device
Networking devices that forward data packets, most commonly Internet Protocol (IP) packets, between networked systems which are primarily intended for residential use and can be installed by the customer.

Consumer-Grade Router Product
Consumer-grade router device and any additional product components (e.g., backend, smartphone application) that are necessary to use the IoT 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 or non-technical.