NIST Internal Report
NIST IR 8425A ipd

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Initial Public Draft

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.ipd

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

NIST Internal Report
NIST IR 8425A ipd

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Initial Public Draft

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.ipd

April 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

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/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

[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

[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.

Sections A.1 to A.7 below show which requirements from the four consumer-grade router standards are related to the technical outcomes for consumer-grade routers. 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 consumer-grade router profile cybersecurity outcomes was developed by modifying the outcomes from NISTIR 8425. Two new sub-outcomes were also added based on review of the consumer-grade router standards, noted with a †.

For each sub-outcome, a set of related requirements from the four consumer-grade router 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]

In the development of firmware for consumer-grade routers and their components, NIST recommends the use of Special Publication 800-193 [SP800-193]. Section 4 of that document details technical cybersecurity capabilities to help mitigate firmware vulnerabilities. These capabilities are supportive of the outcomes for consumer-grade router products defined in this document. Thus, in addition to the four consumer-grade router 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 consumer-grade router products, but should be considered by consumer-grade 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 consumer-grade router standards were mapped to this outcome. Consumer-grade router products composed of only a consumer-grade router device would natively meet this outcome. When a consumer-grade router 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 consumer-grade 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 consumer-grade router product components.

Configuration control of networking equipment, including consumer-grade router products is critical to network cybersecurity. If possible, configuration may be better managed by another consumer-grade router product component (e.g., mobile application) to minimize interfaces (and thus attack surface) of the consumer-grade 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 consumer-grade router product components can access the consumer-grade router product's configuration interfaces (e.g., administration page) and 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

A.4. Interface Access Control 1

Each consumer-grade router product component controls access to and from all interfaces[3] in order to limit access to only authorized entities.

A.4.9. 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. For example, disable by default remote access to the router, especially via the WAN interface.

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 consumer-grade router product overall, but particularly attention should be given to minimizing the interfaces included on the consumer-grade router devices. Extraneous interfaces unnecessary to the core features of the router device should be implemented via other consumer-grade router products, be turned off by default, or be removed entirely.

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.[4] 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.
2. Placing a timeout limit on account sessions.
3. Protecting against authentication brute force attacks (e.g., limiting failed log-in attempts).
4. Making physical developer interface ports inaccessible from the outside of a component.

[3] 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.
[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. Ensuring closed ports are not revealed during scans.
6. Prohibiting the reply to requests over a port for an API or Protocol that doesn't use that port.

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

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 consumer-grade 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

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

IMDA 4.2

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

[5] 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.

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 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

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 consumer-grade router product components only by using a secure and configurable mechanism, as appropriate for each consumer-grade 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 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 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), 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†

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 consumer-grade router product components and the data they store and transmit.

A.7.18. 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. Information that the consumer-grade router product shall provide includes login attempts, administrative events, system status, firewall status, status of all consumer-grade router product components, other connected products, and timing synchronization.

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 or responds directly to changes in cybersecurity information.

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 consumer-grade router standards that 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 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) **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, risks) related to the consumer-grade router product and its product 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 (i.e., consumer-grade routers) and may be deployed similarly for different digital products. For example, a vulnerability management program is not likely to vary significantly in implementation for consumer-grade routers, smart thermostats, personal computers, etc. 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 consumer-grade router 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., consumer-grade 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 consumer-grade router products can be significant. Consumer-grade 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 consumer-grade 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 consumer-grade 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 consumer-grade 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 consumer-grade router 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 consumer-grade router 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. 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.
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

	Applicable to…	
Consumer-Grade Router Standard	Consumer-Owned Routers?	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.

BBF 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 (both gateways and cable modems) for security—this includes manufacturing process, supply

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

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 a informational crosswalk listing all SSDF tasks, copied directly from the SSDF. To provide additional insight into NIST's thinking of how the SSDF can be used in the context of consumer-grade routers, applicability of each SSDF task to three kinds of code commonly part of consumer-grade router products: router firmware, mobile applications, 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* are software intended to be installed and/or executed on small profile platforms that can connect to cellular data networks. For example, applications made to run on Apple's iOS or Alphabet's 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 which 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]