

**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>

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

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

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

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

14 **NIST Technical Series Policies**

15 [Copyright, Use, and Licensing Statements](#)

16 [NIST Technical Series Publication Identifier Syntax](#)

17 **Publication History**

18 Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added in final release of publication]

19 **How to Cite this NIST Technical Series Publication:**

20 Fagan M, Megas K, Watrobski P, Marron J, Cuthill B, Lemire D, Hoehn B, Evans C (2024) Recommended
21 Cybersecurity Requirements for Consumer-Grade Router Products. (National Institute of Standards and
22 Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425A ipd.
23 <https://doi.org/10.6028/NIST.IR.8425A.ipd>

24 **Author ORCID iDs**

25 Michael Fagan: 0000-0002-1861-2609

26 Katerina N. Megas: 0000-0002-2815-5448

27 Paul Watrobski: 0000-0002-6449-3030

28 Jeffrey Marron: 0000-0002-7871-683X

29 Barbara B. Cuthill: 0000-0002-2588-6165

30 **Public Comment Period**

31 April 17, 2024 – May 17, 2024

32 **Submit Comments**

33 iotsecurity@nist.gov

34

35 National Institute of Standards and Technology

36 Attn: Applied Cybersecurity Division, Information Technology Laboratory

37 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

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

39 **Abstract**

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

47 **Keywords**

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

49 **Reports on Computer Systems Technology**

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

58

59 **Audience**

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

64 **Note to Reviewers**

65 On July 18th, 2023, the White House announced the next steps for the Cybersecurity Labeling
66 Program for Smart Devices to Protect American Consumers, referred to as the “U.S. Cyber Trust
67 Mark.” [\[WHAnnouncement\]](#) In addition to announcing participation by the Federal
68 Communications Commission and Departments of Energy and State, the White House also
69 directed NIST to “immediately undertake an effort to define cybersecurity requirements for
70 consumer-grade routers—a higher-risk type of product that, if compromised, can be used to
71 eavesdrop, steal passwords, and attack other devices and high value networks.” In response,
72 NIST worked to develop these requirements with a standards-based, transparent, community-
73 involved process. NIST welcomes any feedback on this draft. In particular, we seek any
74 recommendations of standards or guidance that can apply to consumer-grade routers and seek
75 feedback about the cybersecurity techniques discussed in Section 2.1 and noted in Appendix A.

76 Call for Patent Claims

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

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

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

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

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

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

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

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

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

103

104	Table of Contents	
105	1. Introduction	1
106	2. Scope of Consumer-Grade Routers	4
107	2.1. Cybersecurity Utilizing the Full Product.....	5
108	3. Conclusion	7
109	References	8
110	Appendix A. Crosswalk between Technical Outcomes and Consumer-Grade Router Cybersecurity and	
111	Firmware Requirements	11
112	A.1. Asset Identification	11
113	A.2. Product Configuration	12
114	A.3. Data Protection.....	13
115	A.4. Interface Access Control 1	15
116	A.5. Interface Access Control 2	17
117	A.6. Software Update.....	18
118	A.7. Cybersecurity State Awareness	19
119	Appendix B. Non-Technical Outcome Considerations	20
120	Appendix C. Consumer-Grade Router Acquisition Scenarios Discussion	23
121	Appendix D. Crosswalk Between Secure Software Development Tasks and Consumer-Grade Router	
122	Product Software Type	25
123	Appendix E. List of Symbols, Abbreviations, and Acronyms	29
124	Appendix F. Glossary	30
125	List of Tables	
126	Table 1. Non-technical cybersecurity outcomes and requirements from consumer-grade router	
127	standards	20
128	Table 2. Scope Coverage of the Consumer-Grade Router Standards Analyzed	23
129	Table 3. Crosswalk between consumer-grade router product software types and SSDF tasks.	25
130	List of Figures	
131	Fig. 1. Most requirements from the four consumer-grade router standards do not repeat	2
132	Fig. 2. Recommended guidance documents and standards support cybersecurity outcomes for all parts	
133	of consumer-grade router products throughout their development lifecycle.	3
134	Fig. 3. An example consumer-grade router product that includes a smartphone application and	
135	backend server in addition to the router device.	4
136		

137 1. Introduction

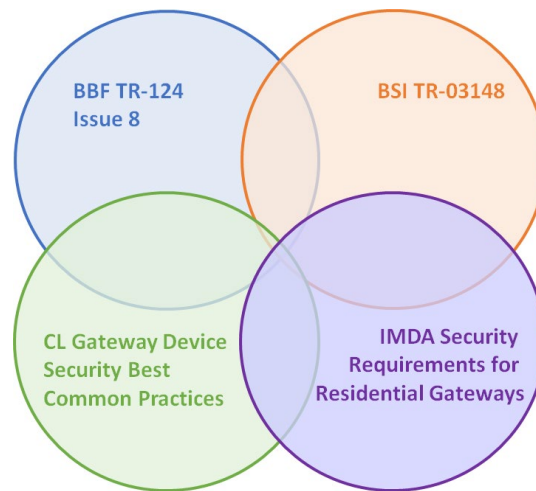
138 Router cybersecurity is of paramount importance in today's interconnected world, where digital
139 communication plays a central role in both personal and professional spheres. Routers serve as
140 the gatekeepers of our networks, managing the flow of data between devices in the home or
141 office and the internet. A compromised router opens the door to a host of potential exploited
142 vulnerabilities and impacts, ranging from unauthorized access, sensitive information
143 dissemination, to the possibility of malicious attacks on connected devices. Ensuring the
144 security of routers is crucial for safeguarding not only individual privacy and safety, but also the
145 integrity and availability of entire networks. With the increasing prevalence of smart home IoT
146 devices and remote work setups, the significance of consumer-grade router cybersecurity has
147 expanded, as these devices and applications often rely on routers in the home to connect to the
148 internet. A secure home router (i.e., one that is consumer-grade) not only protects U.S. citizens
149 against data theft and other cyberattacks but also contributes to the overall resilience of the
150 global digital infrastructure. As technology advances, the need for robust router cybersecurity
151 becomes ever more critical to maintain a safe and trustworthy digital environment.

152 This report presents the *consumer-grade router profile*, which recommends cybersecurity
153 outcomes for consumer-grade router products and associated requirements from consumer-
154 grade router standards. This profile was developed starting from the outcomes defined for
155 consumer IoT products in *Profile of the IoT Core Baseline for Consumer IoT Products*, NISTIR
156 8425 [\[IR8425\]](#). Though developed for consumer IoT products the NISTIR 8425 outcomes are
157 important cybersecurity guidance for any digital product. Outcomes can be technical (i.e.,
158 implemented through hardware and/or software) or non-technical (i.e., implemented as
159 procedures and processes by organizations or individuals). In this context, outcomes are broad,
160 flexible guidelines that can apply, albeit differently, to different use cases and contexts, while
161 requirements are targeted specifications that can define meeting an outcome for a specific use
162 case, context, technology, etc. The guidance in this document has been developed uniquely for
163 consumer-grade routers using cybersecurity considerations and standards specific to that
164 product type. **NIST recommends the use of the following standards for the cybersecurity of
165 consumer-grade router products:**

- 166 1. Broadband Forum (BBF) TR-124 Issue 8 – *Functional Requirements for Broadband*
167 *Residential Gateway Devices* [\[BBF\]](#)
- 168 2. CableLabs (CL) *Security Gateway Device Security Best Common Practices* [\[CableLabs\]](#)
- 169 3. Federal Office for Information Security (BSI) TR-03148: *Secure Broadband Router -*
170 *Requirements for secure Broadband Routers* [\[BSI\]](#)
- 171 4. Infocomm Media Development Authority (IMDA) *Technical Specification Security*
172 *Requirements for Residential Gateways* [\[IMDA\]](#)
- 173 5. *Platform Firmware Resiliency Guidelines*, SP 800-193 [\[SP800-193\]](#)
- 174 6. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*,
175 SP 800-161 Rev. 1 [\[SP800-161r1\]](#)

- 176 7. *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for*
177 *Mitigating the Risk of Software Vulnerabilities*, SP 800-218 [[SSDF](#)]
- 178 8. *Information technology — Security techniques — Vulnerability disclosure processes*,
179 ISO/IEC 29147 [[ISO29147](#)]
- 180 9. *Information technology — Security techniques — Vulnerability handling*, ISO/IEC 30111
181 [[ISO30111](#)]
- 182 10. *Risk management — Guidelines*, ISO 31000 [[ISO31000](#)]
- 183 11. *Systems and software engineering — Design and development of information for users*,
184 ISO/IEC/IEEE 26514 [[ISO26514](#)]

185 NIST recommends the use of four existing consumer-grade router standards¹ (i.e., items 1
186 through 4 in the list above). Requirements from the standards for consumer-grade routers
187 focused primarily on the router device, discussing many cybersecurity capabilities appropriate
188 for this equipment. **Figure 1** notionally² depicts that requirements of the four consumer-grade
189 router device standards were mostly unique and had minimal overlap. Few requirements from
190 the different standards repeat, and **each standard’s requirements offer useful details about**
191 **how cybersecurity outcomes can be met by consumer-grade router devices**. Additional
192 technical requirements for firmware are introduced by SP 800-193 (i.e., item 5). Appendix A
193 provides a crosswalk between technical cybersecurity outcomes for consumer-grade router
194 products and the technical requirements from these five standards.



195
196 **Fig. 1. Most requirements from the four consumer-grade router standards do not repeat.**

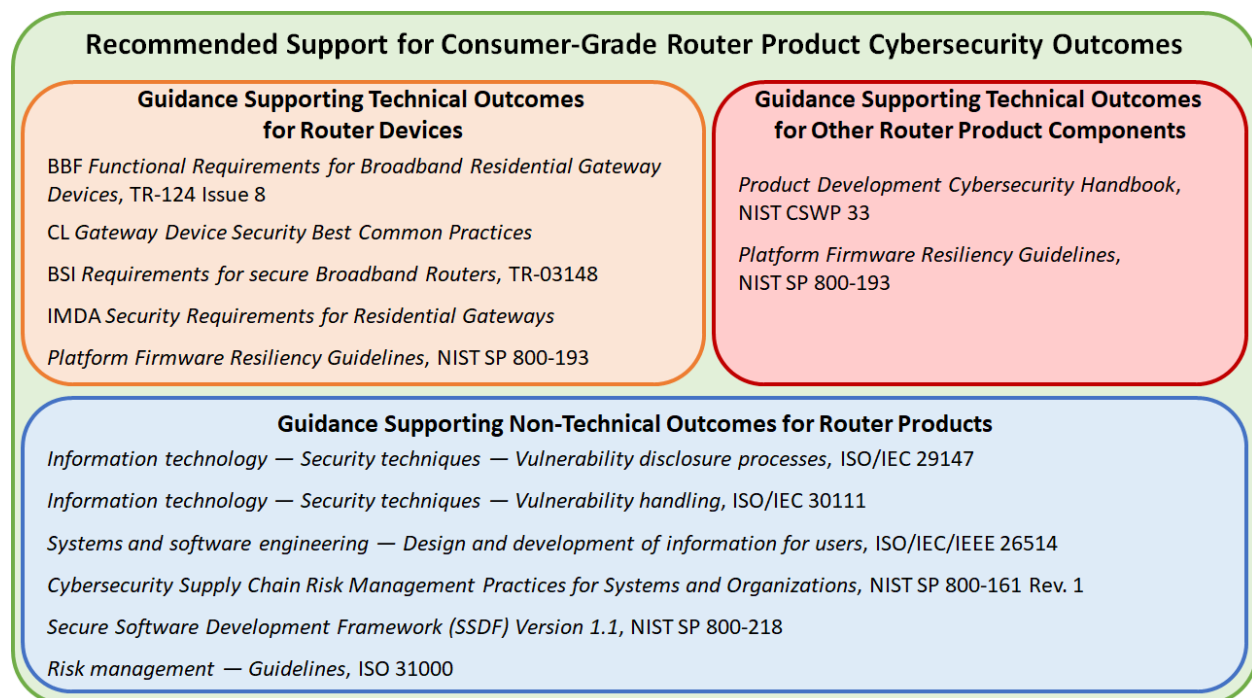
197 The requirements from the four router standards address technical cybersecurity for consumer-
198 grade router devices but not the non-technical cybersecurity outcomes nor cybersecurity for
199 product components other than the router device (e.g., backend, mobile application) since they

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).

200 contain few requirements for non-technical supporting capabilities and no requirements for
201 other product components (e.g., mobile application). Therefore, additional standards (i.e.,
202 items 6 through 11) are recommended to help fill some of those gaps in the consumer-grade
203 router standards, particularly for non-technical outcomes. Appendix B discusses some
204 additional considerations and guidance for non-technical outcomes.

205 **This list is intended as a minimum starting point** and may not address all the cybersecurity
206 considerations for every consumer-grade router product. Full support of all outcomes in this
207 profile by all consumer-grade router product components is expected. **To ensure cybersecurity**
208 **consideration of all consumer-grade router product components, the *Product Development***
209 ***Cybersecurity Handbook* [CSWP33] is recommended** in addition to the standards indicated
210 above. If a consumer-grade router product has additional product components, such as a smart
211 phone mobile application, additional technical product cybersecurity capability requirements
212 would also be necessary to meet the outcomes for the complete consumer-grade router
213 product. These considerations are discussed generally for digital products in the handbook.
214 **Figure 2** shows how the standards listed above relate to cybersecurity outcomes (i.e., the
215 technical vs. non-technical outcomes) and components of consumer-grade router products (i.e.,
216 consumer-grade router device vs. other consumer-grade router product components).



217
218 **Fig. 2. Recommended guidance documents and standards support cybersecurity outcomes for all parts of**
219 **consumer-grade router products throughout their development lifecycle.**

220 The rest of this document provides additional discussion of cybersecurity context and
221 expectations related to consumer-grade router products, structured as follows:

- 222 • Section 2 states the recommended scope of consumer-grade router products.
- 223 • Section 3 concludes the document.

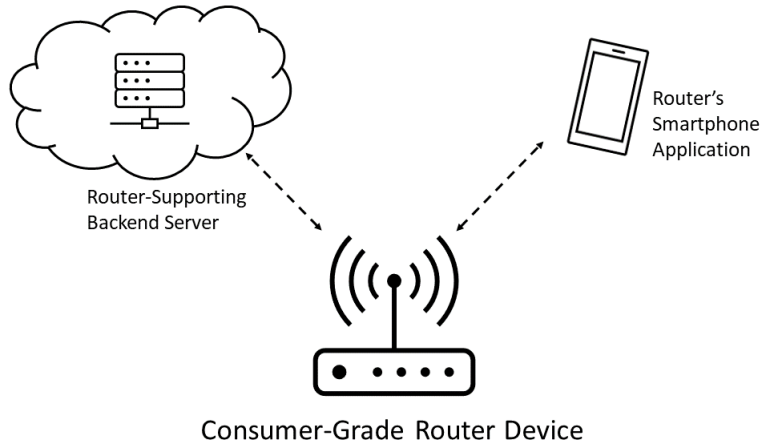
224 2. Scope of Consumer-Grade Routers

225 This profile identifies minimum cybersecurity for consumer-grade routers. Consumer-grade
226 routers are defined as networking devices which are primarily intended for residential use and
227 can be installed by the customer. Routers forward data packets, most commonly Internet
228 Protocol (IP) packets, between networked systems. **The profile makes no distinction in its
229 cybersecurity recommendations with regards to whether the product is owned by the
230 customer or leased from an internet service provider.**

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

237 Cybersecurity outcomes and requirements for products should be scoped to all product
238 components (e.g., smartphone applications) developed to be used with the router device.
239 Third-party applications are not generally considered in the product's scope, unless designated
240 by the product manufacturer as such. **Figure 3** below shows an example consumer-grade router
241 product where the router device is supported by both a backend and smartphone application.

Example Additional Router Product Components



242

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

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

251 2.1. Cybersecurity Utilizing the Full Product

252 The standards referenced in Section 1, particularly the four that are specific to consumer-grade
253 routers reflect general, minimal cybersecurity for this equipment. Manufacturers of consumer-
254 grade router products should look beyond these technical requirements for cybersecurity
255 features. The following concepts are examples of emerging techniques that may help improve
256 the cybersecurity provided by consumer-grade routers and of the products themselves:

- 257 • **Machine-readable asset identification support from consumer-grade router products.**
258 Consumer-grade routers serve as a central connection point for networks, where many
259 types of devices will gain access to the local network and usually internet. These devices
260 having machine-readable asset identifiers that are utilized by consumer-grade routers
261 can enable more proactive cybersecurity management of the network through better
262 identification and inventory of connected devices. Home users could utilize these
263 features, but they are more likely to be useful to small businesses or for routers leased
264 from internet service providers (ISPs), where ISPs may make use of this information.
265 Identification can also go beyond simple inventorying when extended by concepts like
266 device intent signaling (e.g., the “manufacturer usage description” [MUD]). Machine-
267 readable asset identifiers must be developed and used in ways that is privacy
268 preserving, particularly if they are to be used by organizations (e.g., ISPs) to help protect
269 the cybersecurity of individuals.
- 270 • **Interface and functionality minimization for consumer-grade router devices.** “Secure-
271 by-design” principles [[SecureByDesign](#)] applied to consumer-grade routers should guide
272 manufacturers to minimize the number of interfaces and general functionality provided
273 by the consumer-grade router device. The purpose of this product component should be
274 to perform routing capabilities. Extraneous functions should not be included in this
275 component. For example, configuration may be better managed by another consumer-
276 grade router product component (e.g., mobile application). This is not to suggest a
277 consumer-grade router product composed of only a consumer-grade router device is
278 necessarily less secure than those that can offload functions to other components. That
279 said, in the case there is only a consumer-grade router device, the cybersecurity
280 capabilities of that component should be reasonably maximized.
- 281 • **Robust network onboarding support from consumer-grade router product.**
282 Cybersecurity when provisioning new devices to the networks of consumer-grade
283 routers can go beyond a single password. When a consumer-grade router product is
284 composed of components such as mobile applications or backends, those components
285 can be used as part of a more robust onboarding mechanism. For example, when a
286 device is attempting to connect to the consumer-grade router device with (or without)
287 the password, the mobile application can notify the owner and ask for explicit approval
288 for the device to onboard. Though reliability needs to be considered to ensure
289 individuals can always access and use their routers, onboarding mechanisms for
290 consumer-grade routers that give individuals more access control over their networks is
291 beneficial.

- 292 • **Multiple signatures for software update packages when possible.** At a minimum, all
293 software update packages should be signed by the source of the update (e.g.,
294 manufacturer), but when applicable (e.g., when routers are leased from ISPs) other
295 entities may also cryptographically sign updates, adding another layer of security.

296 Several of these examples highlight ways consumer-grade router products can take advantage
297 of all product components to deliver cybersecurity capabilities. These and other cybersecurity
298 techniques should be considered by manufacturers to continually improve the cybersecurity of
299 consumer-grade routers as risks shift and new mitigations become available.

300 3. Conclusion

301 This consumer-grade router profile can help manufacturers determine adequate cybersecurity
302 to develop into their products. These recommendations draw from current effective practices
303 and promote adoption of accepted and vetted cybersecurity for consumer-grade routers. As
304 with any NIST report, as the referenced standards and effective practices change over time,
305 NIST may revisit this document and revise it. NIST welcomes ongoing feedback and
306 recommendations from the community as to standards and effective practices and solutions for
307 consumer-grade routers. That said, NIST encourages readers to identify if the standards
308 referenced here have been updated asynchronously from this report. NIST reiterates the
309 importance of a product-wide perspective to develop a comprehensive approach to providing
310 cybersecurity for consumer-grade router products.

311 References

- 312 [WHAnnouncement] White House (2023) Biden-Harris Administration Announces Cybersecurity
313 Labeling Program for Smart Devices to Protect American Consumers. (White House,
314 Washington, DC). [https://www.whitehouse.gov/briefing-room/statements-
315 releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-
316 program-for-smart-devices-to-protect-american-consumers/](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/)
- 317 [IR8425] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B (2022) Profile of the IoT Core
318 Baseline for Consumer IoT Products. (National Institute of Standards and Technology,
319 Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8425.
320 <https://doi.org/10.6028/NIST.IR.8425>
- 321 [BBF] Walls, J, Editor (2022) Functional Requirements for Broadband Residential Gateway
322 Devices. (Broadband Forum, Fremont, CA), Technical Report (TR) 124, Issue 8.
323 [https://www.broadband-forum.org/resources/tr-124-issue-8-functional-requirements-for-
324 broadband-residential-gateway-devices](https://www.broadband-forum.org/resources/tr-124-issue-8-functional-requirements-for-broadband-residential-gateway-devices)
- 325 [CableLabs] CableLabs Security (2021) Gateway Device Security Best Common Practices.
326 (CableLabs, Louisville, CO), CL-GL-GDS-BCP-V01-211007.
327 [https://community.cablelabs.com/wiki/plugins/servlet/cablelabs/alfresco/download?id=1
328 209eea3-bd81-40cb-9a18-21bd6cfcd80d](https://community.cablelabs.com/wiki/plugins/servlet/cablelabs/alfresco/download?id=1209eea3-bd81-40cb-9a18-21bd6cfcd80d)
- 329 [BSI] Federal Office for Information Security (2023) Secure Broadband Router: Requirements for
330 Secure Broadband Routers. (Federal Office for Information Security, Bonn, Germany), BSI
331 Technical Report (TR) 03148. [https://www.bsi.bund.de/EN/Themen/Unternehmen-und-
332 Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-
333 sortiert/tr03148/tr-03148.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03148/tr-03148.html)
- 334 [IMDA] Info-communications Media Development Authority of Singapore (2020) Security
335 Requirements for Residential Gateways. (Info-communications Media Development
336 Authority, Singapore), IMDA Technical Specification (TS) RG-SEC.
337 [https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-
338 standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf](https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/ict-standards/telecommunication-standards/radio-comms/imda-ts-rg-sec.pdf)
- 339 [SP800-193] Regenscheid, AR (2018) Platform Firmware Resiliency Guidelines. (National
340 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
341 800-193. <https://doi.org/10.6028/NIST.SP.800-193>
- 342 [SP800-161r1] Boyens JM, Smith AM, Bartol N, Winkler K, Holbrook A, Fallon M (2022)
343 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.
344 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
345 Publication (SP) 800-161r1. <https://doi.org/10.6028/NIST.SP.800-161r1>
- 346 [SSDF] Souppaya MP, Scarfone KA, Dodson DF (2022) Secure Software Development Framework
347 (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities.
348 (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special
349 Publication (SP) 800-218. <https://doi.org/10.6028/NIST.SP.800-218>
- 350 [ISO29147] International Organization for Standardization (2018) Information technology —
351 Security techniques — Vulnerability disclosure. (ISO Standard No. 29147:2018).
352 <https://www.iso.org/standard/72311.html>

- 353 [ISO30111] International Organization for Standardization (2019) Information technology —
354 Security techniques — Vulnerability handling processes. (ISO Standard No. 30111:2019).
355 <https://www.iso.org/standard/69725.html>
- 356 [ISO31000] International Organization for Standardization (2018) Risk management —
357 Guidelines. (ISO Standard No. 31000:2018). <https://www.iso.org/standard/65694.html>
- 358 [ISO26514] International Organization for Standardization (2022) Systems and software
359 engineering — Design and development of information for users. (ISO Standard No.
360 26514:2022). <https://www.iso.org/standard/77451.html>
- 361 [CSWP33] Fagan M, Megas KN, Watrobski P, Marron J, Cuthill B, Lemire D, Hoehn B (2024).
362 Product Development Cybersecurity Handbook: Concepts and Considerations for IoT
363 Product Manufacturers. (National Institute of Standards and Technology, Gaithersburg,
364 MD), Draft NIST Cybersecurity White Paper (CSWP) 33.
365 <https://doi.org/10.6028/NIST.CSWP.33.ipd>
- 366 [SecureByDesign] Cybersecurity and Infrastructure Security Agency (2023). Secure-by-Design
367 Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design
368 Software. (Cybersecurity and Infrastructure Security, Washington, DC).
369 https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf
- 370 [MUD] Lear E, Droms R, Romascano D (2019) Manufacturer Usage Description Specification.
371 (Internet Engineering Taskforce), IETF Request for Comments (RFC) 8520.
372 <https://datatracker.ietf.org/doc/html/rfc8520>
- 373 [SP800-40r4] Souppaya MP, Scarfone KA (2022) Guide to Enterprise Patch Management
374 Planning: Preventive Maintenance for Technology. (National Institute of Standards and
375 Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-40, Rev. 4.
376 <https://doi.org/10.6028/NIST.SP.800-40r4>
- 377 [RFC6092] Woodyatt, J, Editor (2011) Recommended Simple Security Capabilities in
378 Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service.
379 (Internet Engineering Task Force), IETF Request for Comment (RFC) 6092.
380 <https://datatracker.ietf.org/doc/html/rfc6092>
- 381 [IR8320] Bartock MJ, Souppaya MP, Savino R, Knoll T, Shetty U, Cherfaoui M, Yeluri R, Malhotra
382 A, Banks D, Jordan M, Pendarakis D, Rao JR, Romness P, Scarfone KA (2022) Hardware-
383 Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge
384 Computing Use Cases. (National Institute of Standards and Technology, Gaithersburg, MD),
385 NIST Interagency or Internal Report (IR) 8320. <https://doi.org/10.6028/NIST.IR.8320>
- 386 [SP800-37r2] Joint Task Force (2018) Risk Management Framework for Information Systems
387 and Organizations: A System Life Cycle Approach for Security and Privacy. (National
388 Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP)
389 800-37, Rev. 2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- 390 [RFC6092] Woodyatt J, Ed. (2011) Recommended Simple Security Capabilities in Customer
391 Premises Equipment (CPE) for Providing Residential IPv6 Internet Service. (Internet
392 Engineering Taskforce), IETF Request for Comments (RFC) 6029.
393 <https://datatracker.ietf.org/doc/rfc6092/>
- 394 [ParksRouterResearch] Parks Associates (2022) Parks Associates: 52% of Consumers Acquired
395 Their Routers From Their ISP. (PRNewswire, Dallas, TX).

396 [https://www.prnewswire.com/news-releases/parks-associates-52-of-consumers-acquired-](https://www.prnewswire.com/news-releases/parks-associates-52-of-consumers-acquired-their-routers-from-their-isp-301593338.html)
397 [their-routers-from-their-isp-301593338.html](https://www.prnewswire.com/news-releases/parks-associates-52-of-consumers-acquired-their-routers-from-their-isp-301593338.html)

398 **Appendix A. Crosswalk between Technical Outcomes and Consumer-Grade Router** 399 **Cybersecurity and Firmware Requirements**

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

402 Sections A.1 to A.7 below show which requirements from the four consumer-grade router
403 standards are related to the technical outcomes for consumer-grade routers. Each subsection
404 from A.1 to A.7 states the high-level outcome along with each sub-outcome that defines the
405 high-level outcome. The language for the consumer-grade router profile cybersecurity
406 outcomes was developed by modifying the outcomes from NISTIR 8425. Two new sub-
407 outcomes were also added based on review of the consumer-grade router standards, noted
408 with a †.

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

411 **BBF's TR-124 Issue 8** [[BBF](#)]

412 **CL's Security Gateway Device Security Best Common Practices** [[CableLabs](#)]

413 **BSI's Secure Broadband Routers** [[BSI](#)]

414 **IMDA's Security Requirements for Residential Gateways** [[IMDA](#)]

415 In the development of firmware for consumer-grade routers and their components, NIST
416 recommends the use of Special Publication 800-193 [[SP800-193](#)]. Section 4 of that document
417 details technical cybersecurity capabilities to help mitigate firmware vulnerabilities. These
418 capabilities are supportive of the outcomes for consumer-grade router products defined in this
419 document. Thus, in addition to the four consumer-grade router standards, requirements from
420 Section 4 of SP 800-193 are also included in the following sub-sections when applicable.

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

425 **A.1. Asset Identification**

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

428 **A.1.1. Asset Identification 1**

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

432 *Related Standards Requirements:*

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

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

435 **BSI** (3.1.2.1)

436 **IMDA** None

437 **A.1.2. Asset Identification 2**

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

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

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

450 **A.2. Product Configuration**

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

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

459 **A.2.3. Product Configuration 1**

460 Utilizing strong authentication mechanisms (e.g., multi-factor authentication), authenticated
461 and authorized individuals (e.g., customer, ISP), services, and other consumer-grade router
462 product components can access the consumer-grade router product's configuration interfaces
463 (e.g., administration page) and change the configuration settings of the consumer-grade router
464 product via one or more consumer-grade router product components.

465 *Related Standards Requirements:*

466 **BBF** MGMT.LOCAL.2

- 467 **CL** OOB-007, DE-007, MI-002, MI-010, MI-011
468 **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)
469 **IMDA** 4.2, 4.2.3, 4.4

470 **A.2.4. Product Configuration 2**

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

475 *Related Standards Requirements:*

- 476 **BBF** MGMT.LOCAL.10
477 **CL** OOB-009, DE-003, DE-004, DE-006
478 **BSI** (4.6)
479 **IMDA** 4.1.1, 4.2.1, 4.2.3
480 **SP 800-193** 4.2.4(5), 4.4.2(5)

481 **A.2.5. Product Configuration 3**

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

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

489 **A.3. Data Protection**

490 The consumer-grade router product protects data stored across all consumer-grade router
491 product components and transmitted both between consumer-grade router product
492 components and outside the consumer-grade router product from unauthorized access,
493 disclosure, and modification using strong encryption (e.g., FIPS 140-3 compliant modules).

494 **A.3.6. Data Protection 1**

495 Each consumer-grade router product component protects data it stores via secure means, such
496 as strong encryption (e.g., FIPS 140 Rev. 3 compliant modules). All stored data, including data
497 used for authentication (e.g., salting and hashing stored passwords or passphrases) must be
498 protected. Critical data (including firmware images) can be securely backed up and recovered.

499 *Related Standards Requirements:*

500 **BBF SEC.FIRMWARE.2**

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

502 **BSI** (4.1.1)

503 **IMDA** 4.5

504 **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),
505 4.4.2(1-2, 4, 6-8, 10)

506 **A.3.7. Data Protection 2**

507 The consumer-grade router product has the ability to delete or render inaccessible stored data
508 that are either collected from or about the customer, home, family, etc.

509 *Related Standards Requirements:*

510 **BBF** None

511 **CL** OOB-009

512 **BSI** (4.6)

513 **IMDA** 4.2.3

514 **A.3.8. Data Protection 3**

515 When data are sent between consumer-grade router product components or outside the
516 product, strong protections (e.g., FIPS 140-3 compliant encryption modules) are used for the
517 data transmission. This includes using HTTP over TLS for external communications via the
518 consumer-grade router product and for using device management interfaces or web portals for
519 configuration management.

520 *Related Standards Requirements:*

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

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

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

525 **IMDA** 4.2.2, 4.2.5

526 **A.4. Interface Access Control 1**

527 Each consumer-grade router product component controls access to and from all interfaces³ in
528 order to limit access to only authorized entities.

529 **A.4.9. Interface Access Control 1a**

530 Use and have access only to interfaces necessary for the consumer-grade router product's
531 operation. All other channels and access to channels are removed or secured. For example,
532 disable by default remote access to the router, especially via the WAN interface.

533 *Related Standards Requirements:*

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

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

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

539 **IMDA** 4.2, 4.2.1

540 **SP 800-193** 4.2.1.2

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

546 **A.4.10. Interface Access Control 1b**

547 For all interfaces necessary for the consumer-grade router product's use, access control
548 measures are in place.⁴ At a minimum this includes:

- 549 1. Assigning consumer-grade router products unique initial passwords that are required to
550 be changed to a strong password or passphrase upon installation. Support for
551 multifactor authentication is recommended.
- 552 2. Placing a timeout limit on account sessions.
- 553 3. Protecting against authentication brute force attacks (e.g., limiting failed log-in
554 attempts).
- 555 4. Making physical developer interface ports inaccessible from the outside of a
556 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.

- 557 5. Ensuring closed ports are not revealed during scans.
558 6. Prohibiting the reply to requests over a port for an API or Protocol that doesn't use that
559 port.

560 *Related Standards Requirements*⁵:

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

566 **CL** OOB-001, OOB-004, OOB-006, OOB-008, OOB-010, OOB-012, MI-004, MI-007, MI-
567 008, MI-009, MI-010, MI-013, DIAG-002, NETS-007, NETS-008, NETA-001, NETA-002,
568 NETA-003, MI-002

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

570 **IMDA** 4.1.1, 4.1.2, 4.2, 4.2.1

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

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

577 **A.4.11. Interface Access Control 1c**

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

581 *Related Standards Requirements:*

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

583 **CL** MI-006

584 **BSI** (3.1), (3.1.2), (3.2)

585 **IMDA** 4.2

586 **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.

587 **A.5. Interface Access Control 2**

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

590 **A.5.12. Interface Access Control 2a**

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

594 *Related Standards Requirements:*

595 **BBF** None

596 **CL** MI-012, NETS-006

597 **BSI** None

598 **IMDA** 4.6

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

600 **A.5.13. Interface Access Control 2b**

601 Prevent unauthorized transmissions or access to other product components.

602 *Related Standards Requirements:*

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

604 **CL** MI-005, NETS-006

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

606 **IMDA** 4.2.1

607 **A.5.14. Interface Access Control 2c**

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

610 *Related Standards Requirements:*

611 **BBF** None

612 **CL** None

613 **BSI** (3.1.2.3), (3.2)

614 **IMDA** 4.1.1, 4.2, 4.2.1

615 **A.6. Software Update**

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

620 **A.6.15. Software Update 1**

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

623 *Related Standards Requirements:*

624 **BBF** GEN.OPS.22, GEN.OPS.23

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

626 **BSI** (4.2)

627 **IMDA** 4.3

628 **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)

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

632 **A.6.16. Software Update 2**

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

638 *Related Standards Requirements:*

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

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

641 **BSI** (4.1.2), (4.2)

642 **IMDA** 4.3

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

644 **A.6.17. Software Update 3[†]**

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

647 *Related Standards Requirements:*

648 **BBF** GEN.OPS.15, GEN.OPS.24

649 **CL** SU-004

650 **BSI** None

651 **IMDA** None

652 **SP 800-193** 4.3.1(3)

653 **A.7. Cybersecurity State Awareness**

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

656 **A.7.18. Cybersecurity State Awareness 1**

657 The consumer-grade router product securely captures and records information about the state
658 of consumer-grade router components that can be used to detect cybersecurity incidents
659 affecting or affected by consumer-grade router product components and the data they store
660 and transmit. Information that the consumer-grade router product shall provide includes login
661 attempts, administrative events, system status, firewall status, status of all consumer-grade
662 router product components, other connected products, and timing synchronization.

663 *Related Standards Requirements:*

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

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

666 **BSI** (4.1.2), (4.8)

667 **IMDA** None

668 **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)

669 **A.7.19. Cybersecurity State Awareness 2[†]**

670 The consumer-grade router product informs authorized entities about or responds directly to
671 changes in cybersecurity information.

672 *Related Standards Requirements:*

673 **BBF** GEN.OPS.6

674 **CL** AR-002

675 **BSI** None

676 **IMDA** None

677 **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)

678 **Appendix B. Non-Technical Outcome Considerations**

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

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

Consumer-Grade Router Profile Non-Technical Outcome	Related Requirements
Documentation <i>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.</i>	CL HR-005, MI-014, DIAG-001, SBOM-004, SBOM-005
Information and Query Reception <i>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.</i>	-
Information Dissemination <i>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.</i>	CL AR-001, SBOM-011 BSI (4.2) IMDA 4.3e
Education and Awareness <i>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.</i>	-

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

698 **Risk management** in both planning and execution of consumer-grade router products
 699 will help identify and mitigate cybersecurity risks throughout the product lifecycle. Risks
 700 faced by consumer-grade router products can be significant. Consumer-grade router

701 devices have a unique vantage and access to home networks. They also have robust
702 networking capabilities, giving them utility for a wide range of attacks. Other consumer-
703 grade router product components present their own risks. Backends may aggregate
704 data from one or more customers, making them attractive targets for attackers. Mobile
705 applications may be installed in relatively hostile environments due to malware and
706 other vectors of attack. ISO 31000 [[ISO31000](#)] is a foundational resource that developers
707 should use for risk management. NIST's *Risk Management Framework for Information*
708 *Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP
709 800-37 Rev. 2 [[SP800-37r2](#)] may also be useful guidance for risk management.

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

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

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

742 to and is recommended for consumer-grade router product developers as they create
743 the manual and other materials for the device that a customer may seek out for
744 cybersecurity instructions related to the product.

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

750 **Appendix C. Consumer-Grade Router Acquisition Scenarios Discussion**

751 *Routers* are network devices that forward data packets, most commonly Internet Protocol (IP)
 752 packets, between networked systems. They may be wired (e.g., Ethernet), wireless (e.g., Wi-Fi),
 753 or both. *Consumer-grade* identifies those routers that may appear in an individual’s residence
 754 such that their primary use case is residential rather than enterprise, industrial, etc. However,
 755 some small businesses may choose to use consumer grade equipment given the limited
 756 performance needs of those businesses. The presumption for consumer equipment, or small
 757 businesses that use consumer grade equipment, is that the manufacturer cannot assume the
 758 user has cybersecurity expertise or an ability to take significant action to secure the product.

759 Consumer-grade routers may be acquired by households in at least two ways⁶:

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

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

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

Consumer-Grade Router Standard	Applicable to...	
	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

767
 768 As summarized in **Table 2**, the scope statements of three of the four standards examined either
 769 make no distinction about how the router is acquired by customers or state that the guidance
 770 applies to both scenarios.

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

778 CableLabs directly acknowledges both scenarios: “This Gateway Device Security document
 779 specifies best common practices to serve as an industry metric for retail and leased devices
 780 (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]

781 chain, hardware and firmware configuration procedures, software, and management
782 protocols.”

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

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

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

799 This appendix presents a informational crosswalk listing all SSDF tasks, copied directly from the
 800 SSDF. To provide additional insight into NIST’s thinking of how the SSDF can be used in the
 801 context of consumer-grade routers, applicability of each SSDF task to three kinds of code
 802 commonly part of consumer-grade router products: router firmware, mobile applications,
 803 remote backend or web applications.

- 804 • *Router firmware* is a form of device firmware specific to consumer-grade router devices.
 805 *Device firmware* generally is “the collection of non-host processor firmware and
 806 Expansion ROM firmware that is only used by a specific device. This firmware is typically
 807 provided by the device manufacturer” [SP800-193].
- 808 • *Mobile applications* are software intended to be installed and/or executed on small
 809 profile platforms that can connect to cellular data networks. For example, applications
 810 made to run on Apple’s iOS or Alphabet’s Android operating systems.
- 811 • *Remote backend or web applications* are software intended to be hosted and executed
 812 on dedicated or shared servers that may provide services to many products at once. For
 813 example, code supporting consumer-grade routers that is hosted in a cloud
 814 environment.

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

818 **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.)

819 **Appendix E. List of Symbols, Abbreviations, and Acronyms**

- 820 BBF
- 821 Broadband Forum

- 822 BSI
- 823 Federal Office for Information Security

- 824 CL
- 825 CableLabs

- 826 IMDA
- 827 Infocomm Media Development Authority

- 828 IoT
- 829 Internet of Things

830 **Appendix F. Glossary**

831 **consumer-grade router device**

832 Networking devices which are primarily intended for residential use and can be installed by the customer. Routers
833 forward data packets, most commonly Internet Protocol (IP) packets, between networked systems.

834 **consumer-grade router product**

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

837 **cybersecurity outcome**

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

841 **non-technical supporting capability**

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

844 **product cybersecurity capability**

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