

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date September 20, 2022

Original Release Date June 17, 2022

Superseding Document

Status Final

Series/Number NIST IR 8425

Title Profile of the IoT Core Baseline for Consumer IoT Products

Publication Date September 2022

DOI <https://doi.org/10.6028/NIST.IR.8425>

CSRC URL <https://csrc.nist.gov/publications/detail/nistir/8425/final>

Additional Information <https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program>

NIST IR 8425 ipd

Profile of the IoT Core Baseline for Consumer IoT Products

Initial Public Draft

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffery Marron
Barbara Cuthill

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

NIST IR 8425 ipd

Profile of the IoT Core Baseline for Consumer IoT Products

Initial Public Draft

Michael Fagan
Katerina N. Megas
Paul Watrobski
Jeffrey Marron
Barbara B. Cuthill

*Applied Cybersecurity Division
Information Technology Laboratory*

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

June 2022



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

National Institute of Standards and Technology
Secretary of Commerce for Standards and Technology

53 National Institute of Standards and Technology Interagency or Internal Report 8425
54 Initial Public Draft
55 31 pages (June 2022)

56 This publication is available free of charge from:
57 <https://doi.org/10.6028/NIST.IR.8425.ipd>

58 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
59 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
60 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
61 available for the purpose.

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

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

71 **Public comment period:** June 17, 2022 – July 31, 2022

72 **Submit comments on this publication to:** iotsecurity@nist.gov

73 National Institute of Standards and Technology
74 Attn: Applied Cybersecurity Division, Information Technology Laboratory
75 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

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

77

78

Reports on Computer Systems Technology

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

87

Abstract

88 This publication documents the consumer profile of NIST's IoT core baseline and identifies
89 cybersecurity capabilities commonly needed for the consumer IoT sector (i.e., IoT products for
90 home or personal use). It can also be a starting point for small businesses to consider in the
91 purchase of IoT products. The consumer profile was developed as part of NIST's response to
92 Executive Order 14028 and was initially published in *Recommended Criteria for Cybersecurity*
93 *Labeling for Consumer Internet of Things (IoT) Products*. The consumer profile capabilities are
94 phrased as cybersecurity outcomes that are intended to apply to the entire IoT product. This
95 document also discusses the foundations to developing the recommended consumer profile and
96 related considerations. NIST reviewed a landscape of relevant source documents to inform the
97 consumer profile and engaged with stakeholders across a year-long effort to develop the
98 recommendations.

99

Keywords

100 Internet of Things (IoT); consumer IoT; cybersecurity; IoT products; privacy; safety; securable
101 products.

102

103

Acknowledgments

104 The authors wish to thank all contributors to this publication, including the participants in
105 workshops and other interactive sessions; the individuals and organizations from the private and
106 public sectors, including manufacturers from various sectors as well as several manufacturer
107 trade organizations, who provided feedback during NIST's Executive Order 14028 response
108 period. Special thanks to Cybersecurity for IoT team members Brad Hoehn and David Lemire.

109

Audience

110 The intended audience for this report consists of manufacturers of consumer products, especially
111 product security officers, retailers and related integrators and technical support firms serving the
112 consumer and small business sectors, and testing and certification bodies interested in
113 establishing baselines of IoT cybersecurity capabilities.

114

Note to Reviewers

115 This consumer profile is a minor update of the *Recommended Criteria for Cybersecurity*
116 *Labeling for Consumer Internet of Things (IoT) Products* [EO Criteria] published in February,
117 2022. NIST is seeking feedback from stakeholders as the profile moves into the core
118 cybersecurity for IoT guidance. NIST is especially inviting stakeholders to provide feedback on
119 how the profile applies across the entire IoT product and on the outcome oriented approach used
120 in this profile. NIST seeks specific comments addressing the guidance needed for the
121 specialization of profiles for specific classes of devices and how those classes are determined as
122 well as any special considerations for allocation of capabilities among IoT product components.
123 Stakeholders requested additional opportunities for input during the process of developing the
124 original recommended criteria and NIST seeks to respond to that request.

125

126
127

Call for Patent Claims

128 This public review includes a call for information on essential patent claims (claims whose use
129 would be required for compliance with the guidance or requirements in this Information
130 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
131 directly stated in this ITL Publication or by reference to another publication. This call also
132 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
133 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.
134

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

137

- 138 a) assurance in the form of a general disclaimer to the effect that such party does not hold
139 and does not currently intend holding any essential patent claim(s); or
- 140 b) assurance that a license to such essential patent claim(s) will be made available to
141 applicants desiring to utilize the license for the purpose of complying with the guidance
142 or requirements in this ITL draft publication either:
 - 143 i. under reasonable terms and conditions that are demonstrably free of any unfair
144 discrimination; or
 - 145 ii. without compensation and under reasonable terms and conditions that are
146 demonstrably free of any unfair discrimination.

147 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
148 on its behalf) will include in any documents transferring ownership of patents subject to the
149 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
150 the transferee, and that the transferee will similarly include appropriate provisions in the event of
151 future transfers with the goal of binding each successor-in-interest.
152

153 The assurance shall also indicate that it is intended to be binding on successors-in-interest
154 regardless of whether such provisions are included in the relevant transfer documents.
155

156 Such statements should be addressed to: iotsecurity@nist.gov
157
158
159
160
161

162	
163	Table of Contents
164	1 Introduction 1
165	2 Consumer Profile of IoT Core Baseline..... 3
166	2.1 IoT Product Scope Statement..... 3
167	2.2 Consumer Profile 3
168	2.2.1 IoT Product Capabilities 5
169	2.2.2 IoT Product Non-Technical Supporting Capabilities 11
170	3 Consumer Sector Considerations Used to Create Profile..... 17
171	3.1 Gathering Source Information about Consumer IoT Product Cybersecurity . 17
172	3.2 Assessing Consumer IoT Product Cybersecurity Sources..... 19
173	References..... 22
174	
175	List of Appendices
176	Appendix A— Acronyms 23
177	Appendix B— Glossary 24
178	
179	List of Figures
180	Figure 1 – Capabilities Identified for the Consumer Profile. 4
181	
182	List of Tables
183	Table 1 – Example Consumer IoT Vulnerabilities and the Relevant Capabilities from the
184	Consumer Profile. 17
185	Table 2 – Highlighted Insights and Key Takeaways From the Consumer Profiling
186	Process 20
187	

188 1 Introduction

189 On May 12, 2021, the President issued Executive Order (EO) 14028 which, among other
190 directives, called for NIST to recommend requirements for a consumer IoT product
191 cybersecurity labeling program. As part of NIST's response to this directive¹, a profile of the IoT
192 core baseline² for consumer IoT products was created. This profile served as part of the
193 recommendations that NIST published in response to the EO in February 2022 titled
194 *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT)*
195 *Products* [[EO Criteria](#)].

196 The profile builds on the NISTIR 8259 series by extending the IoT Core Baseline for consumer
197 IoT products. NISTIR 8259, *Foundational Cybersecurity Activities for IoT Device*
198 *Manufacturers* [[IR8259](#)], provides foundational guidance for IoT device manufacturers
199 pertaining to developing IoT devices that can be used securely by customers. NISTIR 8259 does
200 not target any specific IoT sector but discusses how manufacturers can approach cybersecurity
201 for IoT devices in general. NISTIR 8259A, *IoT Device Cybersecurity Capability Core Baseline*
202 [[IR8259A](#)], and NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*
203 [[IR259B](#)] define the IoT device cybersecurity capability core baseline (also referred to as the
204 *core baseline*), a starting point for manufacturers to use in identifying the cybersecurity
205 capabilities their customers may expect from the IoT devices they create. NISTIR 8259A
206 discusses device cybersecurity capabilities, which are functions or features implemented by the
207 device through its own hardware and software. For example, NISTIR 8259A discusses concepts
208 such as data protection, access control, and software update, among others. NISTIR 8259B
209 discusses non-technical supporting capabilities, which are actions taken by organizations to
210 support the cybersecurity of the device. For example, NISTIR 8259B discusses concepts such as
211 education and awareness, and information and query reception (by manufacturers).

212 Like NISTIR 8259, these baseline documents do not consider any sector or use case specific
213 considerations, and instead present a starting point for *any* IoT device. Tailoring the baseline
214 capabilities for a specific sector and/or use case requires a form of profiling. The profiling
215 process using NISTIR 8259/A/B directs a profiler to gather sector-/use case-specific information
216 and interpret the relevant impacts of this information to select the baseline capabilities most
217 applicable to and responsive of the needs and goal of customers for the sector/use case.

218 The rest of this document describes the results of this profiling process for the consumer sector
219 and is organized as follows:

¹ For more information about NIST's response to EO 14028's call for recommendations for a consumer IoT product cybersecurity label, visit <https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/cybersecurity-labeling-consumers-0>

² The terms *core baseline*, *IoT core baseline*, and *IoT device core capability baseline* all refer to the set of capabilities presented in NISTIRs 8259A and 8259B.

- 220 • Section 2 explains the intended applicability of the consumer profile to consumer IoT
221 products and defines the consumer profile.
222 • Section 3 describes the process used to develop the consumer profile in more depth.
223 Section 4 explores some additional considerations readers should consider when using
224 the consumer profile.

225 2 Consumer Profile of IoT Core Baseline

226 This section build on the whitepaper, *Recommended Criteria for Cybersecurity Labeling for*
227 *Consumer Internet of Things (IoT) Products* [[EO Criteria](#)]. First, the scope of an “IoT product” is
228 defined, then the consumer IoT product profile of the IoT core baseline is presented.

229 2.1 IoT Product Scope Statement

230 Consumer² IoT products often constitute a set of system components that work together
231 to deliver functionality realized at the end point or ‘device’ component of the product.
232 NIST describes an IoT device as computing equipment with at least one transducer (i.e.,
233 sensor or actuator) and at least one network interface [[IR8259](#)].³ All IoT products
234 contain at least one IoT device and may contain only this product component.⁴ In many
235 cases, the IoT product may be purchased as one piece of equipment (i.e., the IoT device)
236 but still requires other components to operate, such as a backend (i.e., cloud server) or
237 companion user application on a personal computer or smartphone.

238
239 Complex IoT products may contain multiple physical IoT devices, contain other kinds of
240 equipment, or connect to multiple backends or companion applications as components.
241 Though there are possibly a large number of component combinations that may create
242 an IoT product, it is helpful to think of three specific kinds of IoT product components
243 (other than the IoT device itself, which is always present in an IoT product):

- 244
- 245 • Specialty networking/gateway hardware (e.g., a hub within the system where
246 the IoT device is used).
 - 247 • Companion application software (e.g., a mobile app for communicating with
248 the IoT device).
 - 249 • Backends (e.g., a cloud service, or multiple services, that may store and/or
250 process data from the IoT device).

251 These additional product components have access to the IoT device and the data it
252 creates and uses – making them potential attack vectors that could impact the IoT
253 device, customer, and others (e.g., via attacks on systems, local networks, or the Internet
254 at large). Since these additional components can introduce new or unique risks to the
255 IoT product, the entire IoT product, including auxiliary components, must be securable.
256 In this context, an IoT product is defined as an IoT device or IoT devices and any additional
257 product components that are necessary to use the IoT device beyond basic operational features.⁵
258 For example, an unconnected smart lightbulb may still illuminate in one color, but its smart
259 features, such as color changes, cannot be used without other product components.

260 2.2 Consumer Profile

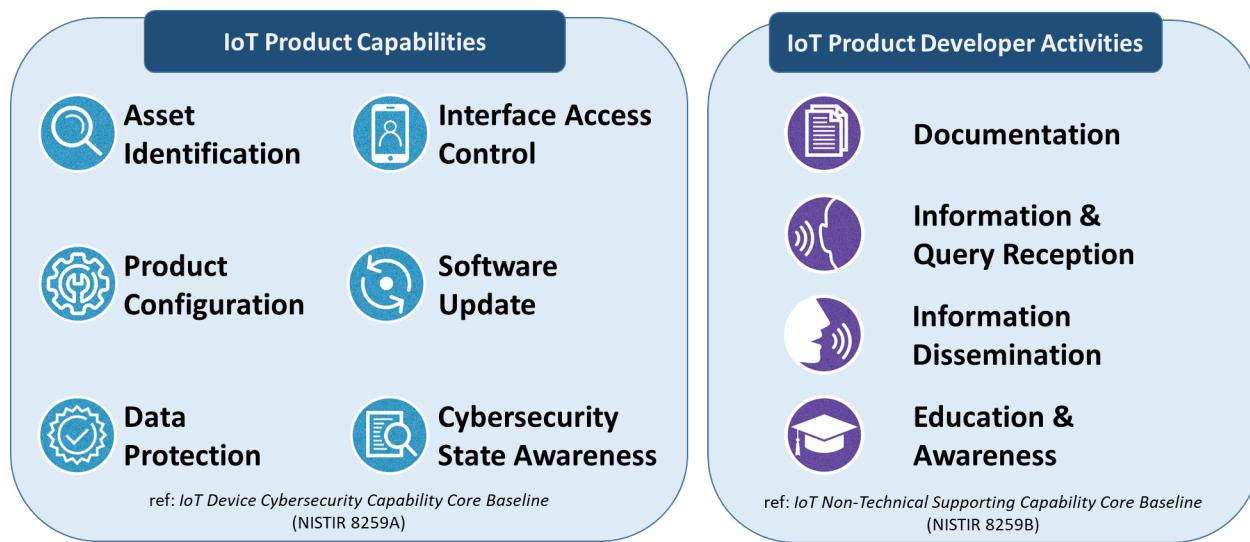
261 This section defines the cybersecurity capabilities³ expected of IoT products and IoT product

³ The term capability is generally used in this document to follow from NISTIR 8259 series, but these same capabilities were presented as “outcomes” in Section 2.2 of *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of*

262 developers as a part of a Consumer profile.

263 Product criteria are recommended to apply to the IoT product overall, as well as to each
264 individual IoT product component, as appropriate.⁶ Most criteria concern the IoT
265 product directly and are expected to be satisfied by software and/or hardware means
266 implemented in the IoT product. Some criteria apply to the IoT product developer rather
267 than to the IoT product directly. These criteria are expected to be satisfied through
268 actions and supported by assertions and evidence from the developer rather than from
269 the IoT product itself.

270 The following figure lays out the high level IoT product capabilities and IoT product
271 developer activities developed based on NISTIRs 8259A and 8259B, respectively that
272 are discussed in the sections below.



273

274 **Figure 1 – Capabilities Identified for the Consumer Profile.**

275 Each capability's name and high-level definition of the capability are presented,
276 followed by additional sub-criteria for each capability. For some sub-criteria, additional
277 detail to the outcome (i.e., normative text) is listed following **bolded** text, while
278 additional explanation and examples (i.e., informative text) are listed following *italicized*
279 text. Finally, each capability is accompanied by a short description of the intended
280 cybersecurity utility of the capability.

281

Things (IoT) Products. These terms are synonymous and could be used interchangeably in the context of this document and the whitepaper.

282 **2.2.1 IoT Product Capabilities**



Asset Identification

283

284 The IoT product is uniquely identifiable and inventories all of the IoT product's
285 components.

286

- 287 1. The IoT product can be uniquely identified by the customer and other authorized
288 entities (e.g., the IoT product developer).
- 289 2. The IoT product uniquely identifies each IoT product component and maintains
290 an up-to- date inventory of connected product components.

291 Cybersecurity utility: The ability to identify IoT products and their components is
292 necessary to support asset management for updates, data protection, and digital forensics
293 capabilities for incident response.

294



Product Configuration

295

296 The configuration of the IoT product is changeable, there is the ability to restore a secure
297 default setting, and any and all changes can only be performed by authorized individuals,
298 services, and other IoT product components.

299

- 300 1. The customer can change the configuration settings of the IoT product via one
301 or more IoT product components.
302 2. The IoT product applies configuration settings to applicable IoT components.

303 Cybersecurity utility: The ability to change aspects of how the IoT product functions
304 can help customers tailor the IoT product's functionality to their needs and goals.
305 Customers can configure their IoT products to avoid specific threats and risk they
306 know about based on their risk appetite.

307



Data Protection

308

309 The IoT product and its components protect data stored (across all IoT product
310 components) and transmitted (both between IoT product components and outside the IoT
311 product) from unauthorized access, disclosure, and modification.

312

- 313 1. Each IoT product component protects data it stores via secure means,
314 including the ability to delete or render inaccessible data stored that is either
315 collected from or about the customer, home, family, etc.
- 316 2. When data is sent between IoT product components or outside the product,
317 protections are used for the data transmission.⁴

318 *Cybersecurity utility:* Maintaining confidentiality, integrity, and availability of data is
319 foundational to cybersecurity for IoT products. Customers will expect that data is
320 protected and that protection of data helps to ensure safe and intended functionality
321 of the IoT product.

322

⁴ This may include the ability to communicate with product components that cannot fully implement the Product Component Data Protection sub-capability (e.g., cannot support adequate cryptography) in a way that reduces the subsequent risk (e.g., data transmitted with sub-par or limited protection), such as short-range and/or local network transmission protocol (e.g., Zigbee, Bluetooth) to communicate with some product components in limited, but necessary circumstances.



Interface Access Control

- 323
- 324 The IoT product and its components restrict logical access to local and network
325 interfaces – and to protocols and services used by those interfaces – to only authorized
326 individuals, services, and IoT product components.
- 327
- 328 1. Each IoT product component controls access (to and from) all interfaces
329 (e.g., local interfaces, network interfaces, protocols, and services) in order to
330 limit access to only authorized entities. **At a minimum, the IoT product**
331 **and its components shall:**
- 332 a. Use and have access only to interfaces necessary for the IoT product's
333 operation. All other channels and access to channels are removed or
334 secured.
- 335 b. For all interfaces necessary for the IoT product's use, access control
336 measures are in place (e.g., unique password-based multifactor
337 authentication).
- 338 c. For all interfaces, access and modification privileges are limited.
- 339 2. The IoT product executes means via some, but not necessarily all, components
340 to protect and maintain interface access control. **At a minimum, the IoT**
341 **product shall:**
- 342 a. Validate that data shared among IoT product components matches
343 specified definitions of format and content.
- 344 b. Prevent unauthorized transmissions or access to other product components.
- 345 c. Maintain appropriate access control during initial connection (i.e., on-
346 boarding) and when reestablishing connectivity after disconnection or
347 outage.
- 348 *Cybersecurity utility:* Inventorying and controlling access to all internal and
349 external interfaces to the IoT product will help preserve the confidentiality,
350 integrity, and availability of the IoT product, its components, and data by helping
351 prevent unauthorized access and modification.
- 352



Software Update

353

354 The software⁵ of all IoT product components can be updated by authorized individuals, services,
355 and other IoT product components only by using a secure and configurable mechanism, as
356 appropriate for each IoT product component.

357

- 358 1. Each IoT product component can receive, verify, and apply verified software updates.
359 2. The IoT product implements measures to keep software on IoT product
360 components up to date (i.e., automatic application of updates or consistent
361 customer notification of available updates via the IoT product).

362 Cybersecurity utility: Software may have vulnerabilities discovered after the IoT
363 product has been deployed; software update capabilities can ensure secure delivery
364 of security patches.

365

⁵ This includes executable code, as well as software libraries, support packs, and other non-executable software data.



Cybersecurity State Awareness

366

367 **Cybersecurity State Awareness:** The IoT product supports detection of cybersecurity
368 incidents affecting or affected by IoT product components and the data they store and
369 transmit.

370

371 1. The IoT product captures and records information about the state of IoT
372 components that can be used to detect cybersecurity incidents affecting or
373 affected by IoT product components and the data they store and transmit.

374

375 **Cybersecurity utility:** Protection of data and ensuring proper functionality can be
376 supported by the ability to alert the customer when the device starts operating in
377 unexpected ways, which could mean that unauthorized access is being attempted,
378 malware has been loaded, botnets have been created, device software errors have
379 happened, or other types of actions have occurred that was not initiated by the IoT
380 product user or intended by the developer.

381 **2.2.2 IoT Product Non-Technical Supporting Capabilities**



Documentation

- 382
- 383 The IoT product developer creates, gathers, and stores⁶ information relevant to
- 384 cybersecurity of the IoT product and its product components prior to customer purchase,
- 385 and throughout the development of a product and its subsequent lifecycle.
- 386
- 387 1. Throughout the development lifecycle, the IoT product developer creates or
- 388 gathers and stores information relevant to the cybersecurity of the IoT product
- 389 and its product components, **including**:
- 390 a. Assumptions made during the development process and other
- 391 expectations related to the IoT product, **including**:
- 392 i. Expected customers and use cases.
- 393 ii. Physical use, including security of the location of the IoT product
- 394 and its product components (e.g., a camera for use inside the
- 395 home that has an off switch on the device vs. a security camera for
- 396 use outside the home that does not have an off switch on the
- 397 device), and characteristics.
- 398 iii. Network access and requirements (e.g., bandwidth requirements).
- 399 iv. Data created and handled by the IoT product.
- 400 v. Any expected data inputs and outputs (including error codes,
- 401 frequency, type/form, range of acceptable values, etc.).
- 402 vi. The IoT product developer's assumed cybersecurity
- 403 requirements for the IoT product.
- 404 vii. Any laws and regulations with which the IoT product and related
- 405 support activities comply.
- 406 viii. Expected lifespan and anticipated cybersecurity costs related to
- 407 the IoT product (e.g., price of maintenance), and length and
- 408 terms of support.
- 409 b. All IoT components, including but not limited to the IoT device, that
- 410 are part of the IoT product.
- 411 c. How the baseline product criteria are met by the IoT product across its
- 412 product components, including which baseline product criteria are not
- 413 met by IoT product components and why (e.g., the capability is not

⁶ The documentation discussed in this criterion is maintained and controlled by the IoT product developer. Sharing of this information may be appropriate and can be limited to authorized technicians and cybersecurity experts seeking more information about the IoT product (e.g., in assessing the IoT product for labeling, investigating a breach), but the documented information is not intended, in all cases, to be shared directly with consumers.

- 414 needed based on risk assessment).
- 415 d. Product design and support considerations related to the IoT product, *for example*:
- 416 i. All hardware and software components, from all sources (e.g.,
417 open source, proprietary third-party, internally developed) used to
418 create the IoT product (i.e., used to create each product
419 component).
- 420 ii. IoT platform used in the development and operation of the IoT
421 product, its product components, including related documentation.
- 422 iii. Protection of software and hardware elements implemented to
423 create the IoT product and its product components (e.g., secure
424 boot, hardware root of trust, and secure enclave).
- 425 iv. Consideration for the known risks related to the IoT product and
426 known potential misuses.
- 427 v. Secure software development and supply chain practices used.
- 428 vi. Accreditation, certification, and/or evaluation results for
429 cybersecurity – related practices.
- 430 vii. The ease of installation and maintenance of the IoT product by a
431 customer (i.e., the usability of the product [[ISO9241](#)]).
- 432 e. Maintenance requirements for the IoT product, *for
433 example*:
- 434 i. Cybersecurity maintenance
435 expectations and associated instructions
436 or procedures (e.g., vulnerability/patch
437 management plan).
- 438 ii. How the IoT product developer identifies
439 authorized supporting parties who can
440 perform maintenance activities (e.g.,
441 authorized repair centers).
- 442 iii. Cybersecurity considerations of the
443 maintenance process (e.g., how customer
444 data unrelated to the maintenance process
445 remains confidential even from
446 maintainers).
- 447 f. The secure system lifecycle policies and
448 processes associated with the IoT product,
449 **including**:
- 450 i. Steps taken during development to ensure
451 the IoT product and its product
452 components are free of any known,
453 exploitable vulnerabilities.
- 454 ii. The process of working with component
455 suppliers and third-party vendors to ensure

456
457
458
459
460
461
462
463
464

the security of the IoT product and its product components is maintained for the duration of its supported lifecycle.

- iii. Any post end-of-support considerations, such as the discovery of a vulnerability which would significantly impact the security, privacy, or safety of customers who continue to use the IoT product and its product components.

g. The vulnerability management policies and processes associated with the IoT product, **including**:

- i. Methods of receiving reports of vulnerabilities (see Information and Query Reception below).
- ii. Processes for recording reported vulnerabilities.
- iii. Policy for responding to reported vulnerabilities, including the process of coordinating vulnerability response activities among component suppliers and third-party vendors.
- iv. Policy for disclosing reported vulnerabilities.
- v. Processes for receiving notification from component suppliers and third- party vendors about any change in the status of their supplied components, such as end of production, end of support, deprecated status (e.g., the product is no longer recommended for use), or known insecurities.

486 *Cybersecurity utility*: Generating, capturing, and storing important information about the
487 IoT product and its development (e.g., assessment of the IoT product and development
488 practices used to create and maintain it) can help inform the IoT product developer
489 regarding the product's actual cybersecurity posture.

490



Information and Query Reception

- 491
492 The ability of the IoT product developer to receive information relevant to cybersecurity
493 and respond to queries from the customer and others about information relevant to
494 cybersecurity.
- 495
- 496 1. The IoT product developer can receive information related to the cybersecurity of
497 the IoT product and its product components and can respond to queries related to
498 cybersecurity of the IoT product and its product components from customers and
499 others, **including:**
- 500 a. The ability of the IoT product developer to identify a point of contact to
501 receive maintenance and vulnerability information (e.g., bug reporting
502 capabilities and bug bounty programs) from customers and others in the
503 IoT product ecosystem (e.g., repair technician acting on behalf of the
504 customer).
- 505 b. The ability of the IoT product developer to receive queries from and
506 respond to customers and others in the IoT product ecosystem about the
507 cybersecurity of the IoT product and its components.

508 Cybersecurity utility: As IoT products are used by customers, those customers may have
509 questions or reports of issues that can help improve the cybersecurity of the IoT product
510 over time.

511



Information Dissemination

- 512
513 The IoT product developer broadcasts (e.g., to the public) and distributes (e.g., to the
514 customer or others in the IoT product ecosystem) information relevant to cybersecurity.
515
516 1. The IoT product developer can broadcast to many/all entities via a channel
517 (e.g., a post on a public channel) to alert the public and customers of the IoT
518 product about cybersecurity relevant information and events throughout the
519 support lifecycle. **At a minimum, this information shall include:**
520 a. Updated terms of support (e.g., frequency of updates and
521 mechanism(s) of application) and notice of availability and/or
522 application of software updates.
523 b. End of term of support or functionality for the IoT product.
524 c. Needed maintenance operations.
525 d. New IoT device vulnerabilities, associated details, and mitigation actions
526 needed from the customer.
527 e. Breach discovery related to an IoT product and its product components
528 used by the customers, associated details, and mitigation actions
529 needed from the customer (if any).
530 2. The IoT product developer can distribute information relevant to cybersecurity of
531 the IoT product and its product components to alert appropriate ecosystem
532 entities (e.g., common vulnerability tracking authorities, accreditors and
533 certifiers, third-party support and maintenance organizations) about cybersecurity
534 relevant information, *for example*:
535 a. Applicable documentation captured during the design and development of
536 the IoT product and its product components.
537 b. Cybersecurity and vulnerability alerts and information about resolution of
538 any vulnerability.
539 c. An overview of the information security practices and safeguards used by
540 the IoT product developer.
541 d. Accreditation, certification, and/or evaluation results for the IoT
542 product developer's cybersecurity-related practices.
543 e. A risk assessment report or summary for the IoT product developer's
544 business environment risk posture.
545 Cybersecurity utility: As the IoT product, its components, threats, and mitigations
546 change, customers will need to be informed about how to securely use the IoT product.

547



Product and Education Awareness

- 548
- 549 The IoT product developer creates awareness of and educates customers and others in
550 the IoT product ecosystem about cybersecurity-related information (e.g., considerations,
551 features) related to the IoT product and its product components.
552
- 553 1. The IoT product developer creates awareness and provides education targeted at
554 customers about information relevant to cybersecurity of the IoT product and its
555 product components, **including**:
- 556 a. The presence and use of IoT product cybersecurity capabilities,
557 **including at a minimum:**
- 558 i. How to change configuration settings and the cybersecurity
559 implications of changing settings, if any.
- 560 ii. How to configure and use access control functionality (e.g., set and
561 change passwords).
- 562 iii. How software updates are applied and any instructions
563 necessary for the customer on how to use software update
564 functionality.
- 565 iv. How to manage device data including creation, update, and
566 deletion of data on the IoT product.
- 567 b. How to maintain the IoT product and its product components during its
568 lifetime, including after the period of security support (e.g., delivery of
569 software updates and patches) from the IoT product developer.
- 570 c. How an IoT product and its product components can be securely re-
571 provisioned or disposed of.
- 572 d. Vulnerability management options (e.g., configuration and patch
573 management and anti-malware) available for the IoT product or its
574 product components that could be used by customers.
- 575 e. Additional information customers can use to make informed purchasing
576 decisions about the security of the IoT product (e.g., the duration and
577 scope of product support via software upgrades and patches).
- 578

579 Cybersecurity utility: Customers will need to be informed about how to securely use the
580 device to lead to the best cybersecurity outcomes for the customers and the consumer
581 IoT product marketplace.

582
583
584
585

586 **3 Consumer Sector Considerations Used to Create Profile**

587 NIST used the concepts of profiling the IoT device cybersecurity capability core baseline to
588 develop the consumer profile. The first step was to gather sources and other information about
589 consumer IoT product cybersecurity. Next, NIST used this information to create the consumer
590 profiling using the sources, information, and resulting takeaways and insights.

591 **3.1 Gathering Source Information about Consumer IoT Product Cybersecurity**

592 The consumer profile stemmed from NIST's response to Executive Order 14028, which directed
593 NIST to develop recommendations for a consumer IoT product cybersecurity label program. The
594 recommendations were broader than the development of a consumer profile of the IoT core
595 baseline, but the profile was a key element of this task. Therefore, NIST was able to gather
596 sources and engage in discussions with external stakeholders about the needs and goals of
597 consumer IoT product customers. Across a year of events, meetings, and other engagements,
598 hundreds of comments were gathered related to cybersecurity labeling for consumer IoT
599 products, many of which informed the profiling of the core baseline for this sector.

600 NIST also looked across the public domain to identify applicable vulnerabilities for the
601 consumer IoT product sector. This information is important to determine a cross-sectional view
602 of vulnerabilities for consumer IoT products that can serve as the basis for determining which
603 threats and vulnerabilities. These threats and vulnerabilities inform the profiling process,
604 particularly aspects of minimal securability. Table 1, reproduced from the *Consumer*
605 *Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward* Whitepaper
606 [[Path Forward](#)] lists a number of applicable, well-documented vulnerabilities, their associated
607 MITRE ATT&CK Framework attack categories, and the profiled capabilities that can help
608 address the vulnerability.

609 **Table 1 – Example Consumer IoT Vulnerabilities and the Relevant Capabilities from the Consumer Profile.**

Vulnerability	Relevant Consumer Profile Capabilities
Marai Malware Variants Attacks – Use of weak authentication to enable the loading of malware onto the device and use that device in DDOS and other attacks.	
<i>Unauthorized access to the IoT device</i>	Asset Identification Interface Access Control Information Dissemination Education and Awareness
<i>Malicious code can be loaded on the IoT device</i>	Software Update Cybersecurity State Awareness Education and Awareness

Vulnerability	Relevant Consumer Profile Capabilities
<i>Commands can be launched using the device</i>	Interface Access Control Documentation
Unauthorized Publication of Fitness Tracker Data – Fitness tracker location data for military personnel was publicly posted even when product was configured for privacy.	
<i>Web application vulnerabilities</i>	Product configuration Cybersecurity State Awareness Documentation Information Dissemination
<i>Mobile application vulnerabilities</i>	Product Configuration Cybersecurity State Awareness Documentation Information Dissemination
<i>Ability for de-identified data to be re-identified</i>	Product Configuration Data Protection Documentation
Unauthorized access to home security camera data – Unauthorized access to data and views of the inside and outside of buildings occurred with multiple brands of security cameras.	
<i>Weak authentication</i>	Interface Access Control
<i>Unauthorized data sharing</i>	Data Protection Documentation Information Dissemination
<i>Non-responsive to questions and complaints to the developers</i>	Information and Query Reception
<i>Lack of monitoring capabilities and procedures</i>	Asset Identification Product Configuration Documentation
<i>Lack of data recording/collection controls</i>	Asset Identification Product Configuration Documentation Information Dissemination

Vulnerability	Relevant Consumer Profile Capabilities
	Education and Awareness

610 NIST also looked into the existing standards, conformity, and labeling ecosystem for IoT devices
611 and products to understand where others had accounted for consumer IoT product
612 considerations. Approximately 30 source documents were reviewed, including IoT cybersecurity
613 laws, catalogs of cybersecurity capabilities, sets of baseline capabilities, and tiering schemes.⁷
614 All specifically addressed the IoT device itself, but several included the cloud, mobile app, hub,
615 or other external components in their considerations. Throughout the public comment periods
616 and discussions with stakeholders, the broader view was supported, as NIST observed much
617 consensus in the need to include all components of an IoT product in the scope for an established
618 set of cybersecurity capabilities.

619 **3.2 Assessing Consumer IoT Product Cybersecurity Sources**

620 Source documents can be most directly compared to the technical and non-technical supporting
621 capabilities established in NISTIRs 8259A and 8259B. Of the 30 source documents collected, a
622 sub-sample of 8 that were most directly related to consumer IoT products. This sub-sample was
623 compared to the capabilities described in NISTIR 8259A/B, which showed there was broad
624 alignment with the technical capabilities, though some common technical capabilities not found
625 in NISTIR 8259A were used to adapt the core baseline for the consumer profile. However, few
626 source documents addressed the non-technical capabilities. As the intended users of consumer
627 IoT devices are, by definition, not experts in cybersecurity, these non-technical supporting
628 capabilities are essential to ensure secure operation.

629 This was confirmed through public comments and verbal feedback throughout the work on the
630 EO response, another sources for information NIST drew from to inform the consumer profile.
631 Through these sources, NIST also heard a number of other ways the consumer sector may be
632 different than the general case or other sectors. For example, the cybersecurity risk management
633 of enterprise customers is generally more structured and formalized compared to the
634 cybersecurity risk management approach used by customers in the consumer sector. Enterprises
635 also, typically, have greater access to cybersecurity expertise than typical consumers. These
636 differences and other insights have implications for how cybersecurity capabilities must be
637 approached and delivered. Table 2 highlights key insights used in the development of the
638 consumer profile.

⁷ EO 14028 directed NIST to consider tiers for this profile/the consumer IoT labeling recommendations, but NIST research and subsequent feedback did not yield a clear and effective set of or framework for developing tiers. Existing sources that addressed tiers did not do so in a consensus way. Furthermore, NIST heard feedback that tiers should reflect increasing levels of risk related to consumer IoT products, but the variety of consumer IoT use cases makes clustering those use cases based on risk, a prerequisite to tiering them, a task that could not be completed within the one-year timeframe for response to EO 14028.

639

640

Table 2 – Highlighted Insights and Key Takeaways From the Consumer Profiling Process

Highlighted Insight	Key Takeaway
Cybersecurity insights for the consumer sector based on risks and vulnerabilities are similar as for the general core baseline case. (e.g., those listed in Table 1)	Most capabilities have similar cybersecurity concepts as core baseline
Device level cybersecurity guidelines would be insufficient based on customers' needs and goals for this sector, including but not limited to their lack of distinction between IoT device and supporting components.	Product is the preferred level for consumer IoT cybersecurity guidelines.
Privacy and safety are prominent concerns for consumer IoT products along with cybersecurity.	Cybersecurity capabilities must be designed to not create risks in these areas, and to support general approaches to privacy and safety risk mitigation.
There is no clear, universal set of consumer needs and goals for cybersecurity in the consumer sector and NIST identified several approaches to addressing customer needs and goals among the source documents included in the landscape review.	Capabilities should be based on universally accepted and generally applicable cybersecurity functions.
Needs and goals for this sector are clear that customers will have different, potentially very limited knowledge and abilities with IoT/IT technologies and cybersecurity functions.	Human-factors related to cybersecurity capabilities is paramount.

641 These insights and resulting takeaways lead NIST to the following considerations regarding a
642 consumer profile:

- 643 1. It became clear that many consumer IoT devices are supported by additional components,
644 such as a back-end and/or mobile app that are critical to using the IoT device to the point
645 that the device cannot be meaningfully used without these components.
- 646 2. Additionally, home consumers many times have little control over these additional
647 components. Therefore, when considering how device-centricity will apply to the
648 consumer sector, the conception should expand just beyond the device to include the full
649 product, which may have additional components including some that the consumer
650 interacts with only indirectly.

- 651 3. Must be implemented in the context of key privacy and safety perceptions and
652 considerations for the sector. Safety and privacy considerations are dynamic for
653 consumer IoT products, though, owing to the fact that even in this specific sector, use
654 cases for IoT products may vary significantly. In some cases, there may be clear safety
655 implications to a product and its operation, but this is not always the case. The same goes
656 for privacy, and this is exacerbated by the fact that different use cases may share broad
657 safety and/or privacy considerations, but the specifics and impacts on capabilities to
658 mitigate risks in these areas may be very different. This all means that our profile's
659 cybersecurity capabilities must look to how it can broadly support and/or not hinder these
660 areas.
- 661 4. Considerations of the customers (i.e., home consumers) that would be managing
662 consumer IoT products. The unpredictable and ad hoc nature of customer risk mitigation
663 for consumer IoT products encourages that broadly useful and generally recommended
664 cybersecurity practices be reflected in the profile.
- 665 5. Additionally, an important cybersecurity need for this sector is usable cybersecurity
666 capabilities that apply across the entire product, and are implemented to need
667 minimal/efficient customer set-up and interaction for use is , since these customers will
668 not have deep knowledge or resources to leverage if capabilities are not usable to them.
- 669 6. Finally, specific standards, solutions, implementations, or mitigations should be fit to an
670 IoT product's functionality and use case meaning so single set of specific requirements
671 can be applicable to all consumer IoT products. Therefore, the consumer profile describes
672 IoT product-level cybersecurity guidelines in terms of outcomes to be achieved and
673 supported by the product as a whole. These outcomes provide guidance for a variety of
674 technologies and use cases, but allow flexibility in the application of the consumer profile
675 to specific IoT products.

676 NIST applied these considerations to the NISTIRs 8259A/B core baseline capabilities to adapt
677 the general IoT approach for the consumer sector. The resulting consumer profile, though more
678 directly tailored for the sector, is still meant to speak to a broad range of IoT technologies, use
679 cases, and risk mitigation considerations. Therefore, application of the consumer profile to a
680 specific product or product type may require additional, but similar gathering and consideration
681 of information as described in this Section.

682

683

References

- [EO Criteria] National Institute of Standards and Technology (2022) Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. <https://doi.org/10.6028/NIST.CSWP.24>
- [8259] Fagan M, Megas KN, Scarfone K, Smith M (2020) Foundational Cybersecurity Activities for IoT Device Manufacturers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259. <https://doi.org/10.6028/NIST.IR.8259>
- [8259A] Fagan M, Megas KN, Scarfone K, Smith M (2020) IoT Device Cybersecurity Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259A. <https://doi.org/10.6028/NIST.IR.8259A>
- [8259B] Fagan M, Marron J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2020) IoT Non-Technical Supporting Capability Core Baseline. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8259B. <https://doi.org/10.6028/NIST.IR.8259B>
- [ISO9241] International Organization for Standardization/International Electrotechnical Commission (2018) ISO 9241-11:2018 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts (ISO Geneva, Switzerland). Available at <https://www.iso.org/standard/63500.html>
- [Path Forward] National Institute of Standards and Technology (2021) Consumer Cybersecurity Labeling for IoT Products: Discussion Draft on the Path Forward. (National Institute of Standards and Technology, Gaithersburg, MD). Available online [here](#).

684

685 **Appendix A—Acronyms**

686 Selected acronyms and abbreviations used in this paper are defined below.

687 DDoS Distributed Denial of Service

688 EO Executive Order

689 ITL Information Technology Laboratory

690 IoT Internet of Things

691 NIST National Institute of Standards and Technology

692 NISTIR NIST Internal Report

693

694

Appendix B—Glossary

Consumer IoT Product	IoT products that are intended for personal, family, or household use.
Core Baseline	A set of device cybersecurity capabilities and non-technical supporting capabilities needed to support common cybersecurity controls that protect the customer’s devices and device data, systems, and ecosystems.
Device Cybersecurity Capability	Cybersecurity features or functions that computing devices provide through their own technical means (i.e., device hardware and software).
IoT Device	Devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world.
IoT Product	An IoT device or IoT devices and any additional product components (e.g., backend, mobile app) that are necessary to use the IoT device beyond basic operational features.
Non-Technical Supporting Capability	Non-technical supporting capabilities are actions an organization performs in support of the cybersecurity of an IoT device.

695