

Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn and is provided solely for historical purposes.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

Withdrawal Date May 8, 2026

Original Release Date December 9, 2025

The attached draft document is followed by:

Stage Final

Series/Number NIST SP 800-70r5

Title National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

Publication Date May 2026

DOI <https://doi.org/10.6028/NIST.SP.800-70r5>

CSRC URL <https://csrc.nist.gov/pubs/sp/800/70/r5/final>

Additional Information



NIST Special Publication 800
NIST SP 800-70r5 ipd

National Checklist Program for IT Products

Guidelines for Checklist Users and Developers

Initial Public Draft

Stephen D. Quinn
Blair Heiserman

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-70r5.ipd>

NIST Special Publication 800
NIST SP 800-70r5 ipd

National Checklist Program **for IT Products**

Guidelines for Checklist Users and Developers

Initial Public Draft

Stephen D. Quinn
Computer Security Division
Information Technology Laboratory

Blair Heiserman
Information Technology Security & Networking Division
Office of Information Systems Management

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-70r5.ipd>

December 2025



U.S. Department of Commerce
Howard Lutnick, Acting Secretary of Commerce

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

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

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

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

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

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

[NIST Technical Series Publication Identifier Syntax](#)

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added to final publication.]

Supersedes NIST Series XXX (Month Year) DOI [Will be added to final publication, if applicable.]

How to Cite this NIST Technical Series Publication

Quinn SD, Heiserman B (2025) National Checklist Program for IT Products: Guidelines for Checklist Users and Developers. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 8000-70r5 ipd. <https://doi.org/10.6028/NIST.SP.800-70r5.ipd>

Author ORCID iDs

Stephen Quinn: 0000-0003-1436-684X

Blair Heiserman: 0009-0003-8779-6231

NIST SP 800-70r5 ipd (Initial Public Draft)
December 2025

National Checklist Program for IT Products:
Guidelines for Checklist Users and Developers

Public Comment Period

December 9, 2025 – January 16, 2026

Submit Comments

checklists@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information

Additional information about this publication is available at <https://csrc.nist.gov/pubs/sp/800/70/r5/ipd>, including related content, potential updates, and document history.

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

1 **Abstract**

2 A security configuration checklist is a document or technical content that contains instructions
3 or procedures for securely configuring an IT product to match an operational environment’s risk
4 tolerance, verifying that the product has been configured properly, and/or identifying
5 unauthorized changes to the product. Using these checklists can minimize the attack surface,
6 reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might
7 otherwise go undetected. NIST established the National Checklist Program (NCP) to facilitate
8 the generation of security checklists from authoritative sources, centralize the location of
9 checklists, and make checklists broadly accessible. This publication explains how to use the NCP
10 to find and retrieve checklists and describes the policies, procedures, and general requirements
11 for participation in the NCP.

12 **Keywords**

13 benchmark; change detection; checklist; information security; National Checklist Program
14 (NCP); Security Automation; secure configuration; security configuration checklist; Security
15 Content Automation Protocol (SCAP); software configuration; vulnerability.

16 **Reports on Computer Systems Technology**

17 The Information Technology Laboratory (ITL) at the National Institute of Standards and
18 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
19 leadership for the Nation’s measurement and standards infrastructure. ITL develops tests, test
20 methods, reference data, proof of concept implementations, and technical analyses to advance
21 the development and productive use of information technology. ITL’s responsibilities include
22 the development of management, administrative, technical, and physical standards and
23 guidelines for the cost-effective security and privacy of other than national security-related
24 information in federal information systems. The Special Publication 800-series reports on ITL’s
25 research, guidelines, and outreach efforts in information system security, and its collaborative
26 activities with industry, government, and academic organizations.

27

28 **Document Conventions**

29 This document was created for current and potential checklist developers and users in both the
30 public and private sectors. Checklist developers include IT vendors, consortia, industry,
31 government organizations, and others in the public and private sector. Checklist users include
32 end users, system administrators, and IT managers within government agencies, corporations,
33 small businesses, and other organizations, as well as private citizens.

34 It is assumed that readers of this document are familiar with general computer security
35 concepts.

36 **Trademark Information**

37 All names are registered trademarks or trademarks of their respective companies, as denoted in
38 this document.

39

40 **Call for Patent Claims**

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

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

- 50 a) assurance in the form of a general disclaimer to the effect that such party does not hold
51 and does not currently intend holding any essential patent claim(s); or
- 52 b) assurance that a license to such essential patent claim(s) will be made available to
53 applicants desiring to utilize the license for the purpose of complying with the guidance
54 or requirements in this ITL draft publication either:
- 55 i. under reasonable terms and conditions that are demonstrably free of any unfair
56 discrimination; or
- 57 ii. without compensation and under reasonable terms and conditions that are
58 demonstrably free of any unfair discrimination.

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

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

66 Such statements should be addressed to: checklists@nist.gov

67

68	Table of Contents	
69	Executive Summary	1
70	1. Introduction	2
71	1.1. Purpose and Scope.....	6
72	1.2. Document Organization.....	6
73	2. NIST National Checklist Program	7
74	2.1. Overview of the NCP.....	7
75	2.2. Security Configuration Checklists.....	7
76	2.3. Benefits of Using Security Checklists.....	9
77	2.4. Types of Checklists Listed by NCP.....	10
78	3. Operational Environments for Checklists	11
79	3.1. Stand-Alone Environment.....	11
80	3.2. Managed Environment (Enterprise).....	11
81	3.3. Custom Environments.....	12
82	3.3.1. Specialized Security-Limited Functionality Environment.....	12
83	3.3.2. Legacy Environment.....	12
84	4. Checklist Usage	14
85	4.1. Determining Local Requirements.....	15
86	4.2. Browsing and Retrieving Checklists.....	16
87	4.3. Reviewing, Customizing, Documenting, and Testing Checklists.....	18
88	4.4. Applying Checklists to IT Products.....	19
89	4.5. Providing Feedback on Checklists.....	20
90	5. Checklist Development	22
91	5.1. Developer Steps for Creating, Testing, and Submitting Checklists.....	22
92	5.2. Initial Checklist Development.....	23
93	5.3. Checklist Testing.....	23
94	5.4. Checklist Documented.....	24
95	5.5. Checklist Submitted to NIST.....	26
96	5.6. NIST Steps for Reviewing and Finalizing Checklists for Publication.....	27
97	5.7. NIST Screening of the Checklist Package.....	27
98	5.8. Public Review and Feedback for the Candidate Checklist.....	27
99	5.9. Final Listing on Checklist Repository.....	28
100	5.10. Checklist Maintenance and Archival.....	28
101	References	29
102	Appendix A. Checklist Program Operational Procedures	30

103	A.1. Overview and General Considerations	31
104	A.2. Checklist Submission and Screening.....	33
105	A.3. Candidate Checklist Public Review	33
106	A.4. Final Checklist Listing.....	34
107	A.5. Final Checklist Update, Archival, and Delisting.....	34
108	A.6. Record Keeping.....	35
109	Appendix B. Participation and Logo Usage Agreement Form	36
110	Appendix C. Automating NIST CSF 2.0.....	39
111	C.1. How the Path Connects Policy to Automation.....	39
112	C.2. Implementation and Traceability.....	39
113	C.3. Checklist Development Guidance	40
114	C.4. Operational Environment Tailoring and Considerations	40
115	C.5. Checklist Submission and Maintenance.....	40
116	C.6. Appendix References	41
117	Appendix D. List of Symbols, Abbreviations, and Acronyms.....	42
118	Appendix E. Glossary.....	45
119	Appendix F. Change Log	48
120	List of Tables	
121	Table 1. Checklist Description Form Fields	24
122	List of Figures	
123	Fig. 1. Checklist user process overview	14
124		
125		

126 **Executive Summary**

127 A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a
128 series of instructions or procedures for securely configuring an IT product to a particular risk
129 tolerance for an operational environment, verifying that the product has been configured
130 properly, and/or identifying unauthorized changes to the product. The checklist may be for a
131 commercial, open-source, or government-off-the-shelf (GOTS) IT product.

132 Checklists can comprise a mix of templates, automated scripts, patch information, Extensible
133 Markup Language (XML) files, and other procedures. Typically, checklists are created by IT
134 vendors for their own products; however, checklists are also created by other organizations,
135 such as academia, consortia, and government agencies. The use of well-written, standardized
136 checklists can markedly reduce the attack surface and vulnerability exposure of IT products.

137 NIST maintains the National Checklist Repository, which is a publicly available resource of
138 security configuration checklists for IT products. The repository is located at
139 <https://checklists.nist.gov/> and contains metadata describing each checklist. The repository
140 links to the website where a checklist is hosted. Users can browse and search the repository to
141 locate a particular checklist using a variety of criteria. Having a centralized checklist repository
142 makes it easier for organizations to find current, authoritative versions of security checklists
143 and to determine which ones best meet their needs.

144 This document is intended for users and developers of security configuration. For checklist
145 users, this document makes recommendations on how they should select checklists from the
146 NIST National Checklist Repository, evaluate and test checklists, and apply them to IT products.
147 For checklist developers, this document sets forth the policies, procedures, and general
148 requirements for participation in the NIST National Checklist Program (NCP).

149 Major recommendations made in this document for checklist users and developers include the
150 following:

- 151 • Organizations should apply checklists to operating systems and applications to reduce
152 the number of vulnerabilities that attackers can attempt to exploit and to lessen the
153 impact of successful attacks.
- 154 • When selecting checklists, users should carefully consider each checklist’s degree of
155 automation, source, use of standards, and other relevant characteristics.
- 156 • Checklist users should customize and test checklists before applying them to production
157 systems.
- 158 • Checklist users should consider their operational environments when selecting
159 checklists.,.
- 160 • Checklist creators are encouraged to adopt a “catalog of controls” approach for
161 products to facilitate custom checklist re-use.
- 162 • NIST strongly encourages IT product vendors to develop security configuration checklists
163 for their products and contribute them to the NIST National Checklist Repository.

164 **1. Introduction**

165 There are many threats to users' computers, and new vulnerabilities in IT products (e.g.,
166 operating systems, applications) are discovered daily. Patches may not be immediately
167 available for new vulnerabilities, causing the need to rapidly deploy temporary mitigations
168 through product reconfiguration until patches are available. Moreover, restrictive security
169 settings in IT products may be disabled by default to ensure maximum functionality and
170 interoperability for a wide variety of users, which means that many IT products may be
171 immediately vulnerable in their default configuration. It is a complicated, arduous, and time-
172 consuming task to define a reasonable set of security settings for IT products, even for
173 experienced system administrators.

174 One simple yet effective tool is the security configuration checklist (also called a lockdown,
175 hardening guide, or benchmark). NIST developed the NCP for IT products to facilitate the
176 development of security configuration checklists and meet the requirements of the Cyber
177 Security Research and Development Act of 2002 (Public Law 107-305) (CSFDA) [3].

178 There is no checklist that can make a system or product completely secure, and using a
179 checklist does not eliminate the need for ongoing security maintenance, such as patch
180 installation. However, using a checklist that emphasizes hardening systems against software
181 flaws (e.g., by applying patches and eliminating unnecessary functionality) and securely
182 configuring systems will typically reduce the number of ways in which the systems can be
183 attacked, resulting in greater levels of product security and protection from future threats.
184 Checklists can be particularly helpful to small organizations and individuals with limited
185 resources for securing their systems. Organizations should use a risk-based approach, and
186 checklists should be tailored by each organization to meet its particular security and
187 operational requirements.

188 Mapping and Acquisition Considerations

189 Checklists can also verify the configuration state of technical security controls for system
190 assessments, such as confirming compliance with certain Federal Information Security
191 Modernization Act (FISMA) requirements, security frameworks (e.g., the NIST Cybersecurity
192 Framework), and security controls.

193 According to the Federal Acquisition Regulation (FAR) Part 39, Federal agencies are required to
194 use appropriate security configuration checklists from the NCP. Specifically, paragraph (c) of
195 section 39.101 states,

196 In acquiring information technology, agencies shall include the appropriate
197 information technology security policies and requirements, including use of
198 common security configurations available from the National Institute of
199 Standards and Technology's website at <https://checklists.nist.gov>. Agency
200 contracting officers should consult with the requiring official to ensure the
201 appropriate standards are incorporated. [1]

202 FISMA also requires each federal agency to determine minimally acceptable system
203 configuration requirements and ensure compliance with them [2]. Federal agencies and

204 vendors of products for the Federal Government should create and share checklists using the
205 NCP. NIST encourages checklist developers to map the security controls delineated in NIST
206 Special Publication (SP) 800-53 to IT product technical controls, which facilitates FISMA
207 compliance checking for federal agencies.¹

208 Selecting Checklists

209 Organizations should consider and prioritize product selection based on the availability of
210 security configuration checklists during their IT product selection processes.

211 Organizations are encouraged to tailor checklists to reflect their operational context and risk
212 posture. Any deviation from checklist settings should be accompanied by a documented
213 justification with risk acceptance, recognizing that checklists serve as guidance rather than a
214 universal prescription.

215 NIST recognizes that some checklists are more automated and standards-based than others. For
216 example, non-automated checklists provide prose-based descriptions of how a person can
217 manually alter a product's configuration, while automated checklists are generally machine-
218 executable. The NIST open-source macOS Security Compliance Project (mSCP) is an example of
219 a well-automated checklist package that focuses on standards-based formats to provide
220 security configuration guidance to organizations more quickly and in a machine-consumable
221 format. The mSCP continuously curates and updates machine-consumable macOS guidance to
222 address the continuous release cycle of the vendor. The latest macOS security baseline content
223 is maintained and updated on the mSCP GitHub page.

224 Checklist developers, like the mSCP program, take a programmatic approach to generating and
225 using security configuration baselines. Projects like these can be used to create customized
226 security baselines of technical security controls by leveraging a library of rules that are each
227 mapped to requirements in one or more existing security standards, regulations, or
228 frameworks. This approach provides versioning, consistency, and the generation of checklists in
229 standardized formats that are either native to the platform or in widely accepted security
230 configuration standard formats. Unifying, standardizing, and updating security guidance is
231 simplified and radically accelerated, even as new features and versions of the operating system
232 or application are introduced.

233 Not all checklist generation requires this degree of programmatic sophistication. Automated
234 checklists may be a Group Policy Object (GPO), stand-alone OVAL file, kickstart script, shell
235 script, or simple utility that assesses the security settings on a system. No matter the format,
236 developers of automated checklists are encouraged to use the constructs that are most
237 germane to the platform being configured, be transparent regarding their methods, and assign
238 Common Configuration Enumeration identifiers (CCEs) (i.e., globally unique identifiers) to their
239 individual configuration settings.

240 Another example of an automated checklist is one that fully adheres to the Security Content
241 Automation Protocol (SCAP). These checklists are often referred to as SCAP content and include
242 mappings between low-level security settings and high-level security requirements. These

¹ Organizations are also encouraged to include information in their checklists that supports mapping to other sets of requirements, such as the Health Insurance Portability and Accountability Act (HIPAA).

243 checklists have undergone syntactic testing to ensure adherence to the SP 800-126 SCAP
244 specification using the NIST SCAP Content Validation Tool (SCAPVal) located at [GitHub -](https://github.com/usnistgov/scapval)
245 [usnistgov/scapval](https://github.com/usnistgov/scapval).

246 ○ **Automated checklists**

247 When multiple checklists are available for a particular product, organizations should
248 consider the degree of automation and use of standards for each checklist. Generally,
249 automated checklists can be used more consistently and efficiently than others. There
250 may be other significant differences among checklists; for example, one checklist may
251 include software bundled with an operating system (e.g., web browser, email client),
252 while another addresses the operating system only. Another example is the
253 assumptions on which the checklists are based (e.g., operational environment). A user
254 should identify such differences and determine which checklists seem appropriate and
255 merit further analysis. Checklists can be tailored to suit the risk tolerance of the
256 environment in which they are used.

257 ○ **Government Checklist Precedence**

258 Checklist source is particularly important for users from federal civilian agencies, who
259 should first search for government-authorized or mandated checklists (e.g., mandated
260 by Part 39 of the FAR [1]). In general, these users should search for NIST-produced
261 checklists, which are tailored for civilian agency use. If no NIST-produced checklist is
262 available, then agency-produced checklists from the Defense Information Systems
263 Agency (DISA), the National Security Agency (NSA), or the Cybersecurity and
264 Infrastructure Security Agency (CISA) should be used. If formal government-authorized
265 checklists do not exist, organizations are encouraged to use vendor-produced checklists.
266 If vendor-produced checklists are not available, other checklists that are posted on the
267 NCP website may be used. Although government-sourced checklists generally consider
268 the necessary compliance criteria (e.g., use of FIPS-140 based encryption when
269 encryption is necessary, access control criteria), they may need further tailoring to fit
270 the specific operational and risk-based needs of the environment in which they are
271 used.

272 *Checklist Considerations*

273 A checklist should be considered a starting point for an organization. Checklists should be
274 customized to match an organization's risk posture and requirements, including specific
275 deviations with documented justifications, risk acceptance, and compensating controls.
276 Checklist settings are recommended to prevent security threats and vulnerabilities, but they
277 cannot address organization-specific security and operational requirements and the presence
278 of existing security controls and other factors that may necessitate changes to an organizational
279 checklist. Organizations should carefully evaluate the checklist settings and then make any
280 changes necessary to adapt the settings to the organization's environment, requirements,
281 policies, risk tolerance, and security objectives. This is particularly true for checklists that are
282 intended for an environment with significantly different security needs. For example, producers
283 of checklists in the military can harmonize on the specific types of hardware and software used

284 in their environment, which can allow for more stringent settings. These security configuration
285 settings generally represent a high-water mark rather than a baseline for civilian agencies
286 attempting to use this guidance. The wholesale adoption of a high-water mark in a civilian
287 environment may lead to unintended consequences, and each setting should be specifically
288 tested and validated before widescale deployment. All deviations from the checklist settings
289 should be documented for future reference and include the reason behind each deviation and
290 the impact of deviating from the setting.

291 All checklists should be tested in non-production environments before use in production
292 environments. Each checklist in the NIST repository has been tested by its developer, but there
293 are often significant differences between a developer's testing environment and an
294 organization's operational environment. Security control modification can negatively impact a
295 product's functionality, usability, and security controls. Testing and documentation can help
296 organizations address significant issues.

297 Checklists are significantly more useful when they can run in common operational
298 environments. The NCP has identified several broad and specialized operational environments
299 (e.g., Stand-Alone, Managed), and at least one of the environments should be common to most
300 audiences. Thoroughly identifying and describing these environments will make it easier for
301 users to select the security checklists that are most appropriate for their operating
302 environments and enable developers to better target their checklists to the general security
303 characteristics associated with their operating environments.

304 Organizations that create content, particularly security baselines, should adopt a risk-based
305 approach for selecting the appropriate settings and defining values that consider the context
306 under which the baseline will be utilized. Checklist content can leverage a library of rules that
307 are each mapped to requirements in one or more existing security standards, regulations, or
308 frameworks to create multiple customized security baselines. This approach provides versioning
309 and consistency of the content. Generally, the technical security settings in products do not
310 drastically change between releases. By pursuing a rules-based approach, rules that remain
311 applicable can be reused and incorporated into guidance for the latest release. This enables
312 quicker adoption of new security features that are not offered in prior versions. Settings that
313 are no longer applicable can be retired by specifying a maximum version.²

314 NIST encourages IT product vendors to develop security configuration checklists for their
315 products, since vendors have the most expertise on possible security configuration settings and
316 their relationships.

317 Vendors that create security configuration checklists should submit them for inclusion in the
318 National Checklist Repository through the NCP. The NCP provides a process and guidance for
319 developing checklists in a consistent fashion. For checklist developers, steps include the initial
320 development of the checklist, checklist testing, documenting the checklist according to the
321 guidelines of the NCP, and submitting a checklist package to NIST. NIST then screens the
322 checklist according to program requirements and releases the checklist for a 30-day public

² The mSCP is an open-source project that provides a programmatic approach to generating and using macOS security configuration baselines that adopt this recommendation.

323 review. After the public review period and subsequent resolution of issues, the checklist is
324 listed on the NIST checklist repository with its information. Checklist maintenance may
325 potentially be performed by the vendor, resulting in the release of updated checklists. NIST
326 retires or archives checklists as they become outdated or incorrect.

327 **1.1. Purpose and Scope**

328 This document describes the use, benefits, and management of checklists and checklist control
329 catalogs as well as the policies, procedures, and general requirements for participation in the
330 NIST National Checklist Program (NCP).

331 **1.2. Document Organization**

332 Section 2 provides an overview of checklists and the advantages of the NCP.

333 Section 3 provides additional details on predefined checklist operational environments that are
334 used in the NCP to help developers create checklists that are consistent with security practices.
335 The material presented in Sec. 3 can also help checklist users select the checklists that best
336 match their own operational environments.

337 Section 4 contains information for potential checklist users. It describes how to use the NCP to
338 find and retrieve checklists that best match their identified needs. It also provides guidance on
339 how to implement checklists, including how to analyze the specific operating environment and
340 then tailor checklists as applicable.

341 Section 5 provides guidance for current and prospective checklist developers, including
342 procedures for preparing and submitting a checklist to NIST for inclusion in the checklist
343 repository.

344 The 29 section lists the documents cited throughout this document.

345 Appendix A describes the programmatic and legal requirements that must be satisfied to
346 participate in the NCP.

347 Appendix B provides the NCP participation and logo usage agreement form.

348 Appendix C contains steps for automating the frameworks with checklists.

349 Appendix D lists the acronyms used in this document.

350 Appendix E presents a glossary of the terms used in this document.

351 Appendix F provides a log of changes made since the last version of this document was
352 published.

353

354 2. NIST National Checklist Program

355 This section provides an overview of the NCP and the contents of security configuration
356 checklists, which improve the base level of security for an organization.

357 2.1. Overview of the NCP

358 Organizational checklists can vary widely in terms of purpose, quality, usability, and the level of
359 security they provide. They may also become outdated as software updates and upgrades are
360 released. Without a central checklist repository, finding security checklists can be difficult. NIST
361 established the NCP to facilitate the development of security checklists for IT products and to
362 make checklists more organized and usable. The NCP's broad goals are to:

- 363 • Facilitate the development and sharing of checklists by providing a formal framework
364 for vendors and other checklist developers to submit checklists to NIST
- 365 • Provide guidance to developers to help them create standardized, high-quality
366 checklists that conform to common operational environments
- 367 • Help developers and users by providing guidelines for documentation and usability
- 368 • Encourage software vendors and other parties to develop checklists
- 369 • Provide a managed process for the reviewing, updating, and maintaining checklists
- 370 • Provide an easy-to-use repository of checklist information
- 371 • Provide checklist content in a standardized format
- 372 • Encourage the use of automation technologies for applying checklists.

373 Federal agencies are required to use security configuration checklists from the NCP when
374 available. In January 2017, Part 39 of the Federal Acquisition Regulation (FAR) was updated.
375 Paragraph (c) of section 39.101 states,

376 In acquiring information technology, agencies shall include the
377 appropriate information technology security policies and requirements,
378 including use of common security configurations available from the
379 National Institute of Standards and Technology's website at
380 <https://checklists.nist.gov>. Agency contracting officers should consult
381 with the requiring official to ensure the appropriate standards are
382 incorporated. [1]

383 2.2. Security Configuration Checklists

384 A *security configuration checklist*³ (or simply, "checklist") is a document that contains
385 instructions, procedures, or machine-automated content to configure an IT product to a specific

³ This may also be referred to as a lockdown guide, a hardening guide, a security guide, secure configuration, security technical implementation guide (STIG), or a benchmark.

386 risk posture for an operational environment, verify that the product has been configured
387 properly, identify unauthorized configuration changes to the product, and/or produce artifacts
388 showing the security posture of the product. The IT product may be commercial, open source,
389 government-off-the-shelf (GOTS), or developed in-house.

390 Using well-written, standardized configuration checklists can reduce the vulnerability exposure
391 of IT products and help secure systems. Checklists can be developed by IT vendors and other
392 organizations with technical competence in IT product security. A security configuration
393 checklist might include any of the following:

- 394 • Automated content that sets or verifies security-related settings (e.g., executables,
395 scripts, security templates, SCAP XML files)⁴
- 396 • Documentation that guides the checklist user to manually configure an IT product
- 397 • Documents that explain the recommended methods to securely install and configure a
398 device
- 399 • Rule files that use policy and programmatic documents to define recommended settings
400 for technical controls, such as auditing, authentication mechanisms (e.g., multi-factor
401 authentication, passwords), and firewall security

402 Not all instructions in a security configuration checklist need to solely address security settings.
403 Checklists can also include administrative practices, such as enabling energy-saving features or
404 specialized security functions (e.g., looking for indicators of compromised artifacts on a host).

405 Typically, a checklist is deployed as part of enterprise management to apply settings across all
406 systems. When done manually, a system administrator or end user follows the instructions in
407 the checklist to configure or verify that a product or system has implemented the security
408 controls in the checklist. Through enterprise or local implementation, the system administrator
409 may need to include modifications or deviations to the checklist to ensure that the local
410 security policy enables the risk posture needed for the purpose of the device.

411 Security checklists are intended for a variety of devices and software, including:

- 412 • General-purpose operating systems and mobile operating systems
- 413 • Common applications, such as email clients, web browsers, word processors, personal
414 firewalls, and antivirus software
- 415 • Infrastructure devices, such as software-as-a-service (SaaS) providers, infrastructure-as-
416 a-service (IaaS) providers, platform-as-a-service (PaaS) providers, virtualization
417 platforms, routers, switches, firewalls, virtual private network (VPN) gateways, intrusion
418 detection systems (IDSs), wireless access points, and telecommunication systems
- 419 • Application servers, such as Domain Name System (DNS), Dynamic Host Configuration
420 Protocol (DHCP), proxy and web servers, Simple Mail Transfer Protocol (SMTP), and
421 database servers

⁴ More information about SCAP can be found at <https://scap.nist.gov/> and SP 800-126 [4].

- 422 • Other network devices, such as Internet of Things (IoT) devices, scanners, printers, and
423 copiers
- 424 • Artificial intelligence (AI) systems, including hardware and software components
425 comprising the stack

426 **2.3. Benefits of Using Security Checklists**

427 Security checklists help users configure IT products securely so that they have more protection
428 than default settings. Applying checklists to operating systems and applications can reduce the
429 number of vulnerabilities that attackers attempt to exploit and lessen the impacts of successful
430 attacks. Using checklists improves the consistency and predictability of system security,
431 particularly in conjunction with user training and awareness activities and other supporting
432 security controls. Additional benefits associated with using checklists include:

- 433 • Providing a base level of security to protect against common local and remote threats
434 (e.g., malware, denial-of-service attacks, unauthorized access, inappropriate usage)
- 435 • Verifying the configuration of technical security controls specified by the checklist for
436 system assessments, such as confirming compliance with certain Federal Information
437 Security Modernization Act (FISMA) requirements, and understanding the exposure
438 caused by misconfigurations
- 439 • Providing artifacts of compliance from the verified implementation of controls at the
440 endpoint to support a near real-time understanding of technical security posture and
441 risk
- 442 • Creating catalogs of product technical controls, which significantly reduces the time
443 required to research and develop appropriate security configurations for installed IT
444 products
- 445 • Allowing smaller organizations to implement recommended practice security
446 configurations
- 447 • Reducing the likelihood of public loss of confidence or embarrassment resulting from a
448 compromise of systems (e.g., a major breach of personally identifiable information [PII])

449 Using security checklists for security compliance purposes can significantly improve overall
450 levels of security in organizations, but using a checklist cannot make a system or product
451 completely secure. Using checklists that emphasize the hardening of systems will typically result
452 in greater levels of product security and potential protection from future threats (e.g., zero-day
453 vulnerabilities). IT vendors that configure their products using checklists that adhere to the
454 FISMA-associated security control requirements⁵ will provide more consistency in configuration
455 settings within federal agencies. Applying checklists establishes minimum configuration

⁵ See the NIST Cybersecurity and Privacy Reference Tool at https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_2_0/home.

456 settings, even if the agencies must tailor the checklists for their specific risk tolerances and
457 operational environments.

458 **2.4. Types of Checklists Listed by NCP**

459 The NCP deals with checklists that are tied to *specific* IT products, such as a checklist for a
460 specific operating system version. Some checklists may also incorporate the use of other
461 checklists. For example, a checklist for a database product may reference a checklist for the
462 operating system on which the database product runs. The NCP includes two major groups of
463 checklists:

- 464 • **Automated.** An automated checklist is machine-executable and usable by one or more
465 tools that automatically alter or verify settings based on the contents of the checklist.
466 Checklists can be written in product-native scripting languages, such as shell scripts,
467 PowerShell, Group Policy Objects, Jumpstart scripts, XML, and others.
- 468 • **Non-automated.** As the name implies, a non-automated checklist is one that is designed
469 to be used manually, such as prose instructions that describe the steps an administrator
470 should take to secure a system or verify its security settings.

471 Security configuration checklists in the NCP can help organizations comply with FISMA, which
472 requires federal agencies to determine minimally acceptable system configuration
473 requirements and ensure compliance with them. Checklists can also map specific technical
474 control settings to the corresponding SP 800-53 controls and other existing security standards,
475 regulations, or frameworks, which makes the verification of compliance more consistent and
476 efficient. Federal agencies and vendors of products for the Federal Government are encouraged
477 to develop and share such checklists using the NIST repository. This helps reduce silos of effort
478 to identify sufficiently secure settings for IT products that are widely used in the Federal
479 Government, such as common operating systems, servers, and client applications.

480 The NIST checklist repository (located at <https://checklists.nist.gov/>) provides information on
481 automated and non-automated checklists that have been developed and screened to meet the
482 requirements of the NCP. The repository hosts copies of checklists, primarily those developed
483 by the Federal Government, and points to other submitted checklist locations. Users can
484 browse checklist descriptions to locate and retrieve a particular checklist using a variety of
485 different fields.

486 3. Operational Environments for Checklists

487 To ensure that as many users as possible receive value from checklists, authors should create
488 catalogs of controls from which checklists can be generated for specific operational
489 environments and risk postures. The NCP identifies several broad and specialized operational
490 environments, at least one of which should be common to most audiences. Identifying and
491 describing these environments allows developers to better target their checklists to the general
492 security requirements and risk postures of those environments and allows end users to select
493 the most appropriate checklists.

494 This section describes the operational environments defined for the NCP and the general threat
495 description and fundamental technical security practices for each environment. The two broad
496 operational environments are referred to as **Stand-Alone** (or small office/home office [SOHO])
497 and **Managed** (or Enterprise). Three typical **Custom** environments that could be subsets of the
498 broader environments are **Specialized Security-Limited Functionality (SSLF)** and **Legacy**.

499 IT product users may find it useful to consult this section of the document when initially
500 identifying their own security requirements and needs (see Sec. 4). Developers may find this
501 section useful when building and tailoring security compliance checklists for diverse products
502 while still adhering to the uniform technical security practices and settings associated with the
503 environments (see Sec. 5). Before submitting a checklist to NIST, developers should ensure that
504 they have the most recent version of this document because updates to the criteria for
505 operational environments may occur periodically. The most recent version is available as a
506 separate file at <https://checklists.nist.gov/>.⁶

507 3.1. Stand-Alone Environment

508 The **Stand-Alone** environment describes individually managed devices (e.g., desktops, laptops,
509 smartphones, tablets). It focuses on functionality and are typically the least secure. Stand-Alone
510 checklists should be relatively simple for home users or novice system administrators to
511 understand and implement. They are an entry point to defining a configuration for reuse across
512 a handful of systems and improving from the base vendor security posture.

513 3.2. Managed Environment (Enterprise)

514 The Managed environment (also referred to as Enterprise) is based on centrally managed IT
515 products and devices (i.e., many devices managed by a single organization), including cloud
516 SaaS providers, IaaS providers, PaaS providers, virtualization platforms, servers, desktops,
517 laptops, smartphones, tablets, and IoT. The Managed environment provides more security but
518 less functionality than the Stand-Alone environment.⁷ It also tends to implement several layers

⁶ As new information becomes available, NIST may update the criteria and information for the operational environments as well as other criteria contained in this document.

⁷ Checklists should be customized within Managed environments to meet organizational risk tolerance and requirements (regulatory, security standards and frameworks). For example, making exceptions for groups of users (or devices) with a specific need to deviate from a checklist setting or settings, rather than deviating the setting across the entire enterprise. Tailored deviations, based on documented justification of the needs of a subset of users (or devices) is preferred to preventing users from performing their duties as long as the risk is accepted by an authorizing official.

519 of defense (e.g., firewalls, endpoint detection and response, automated patch management
520 systems, email protections).

521 Managed checklists are intended for advanced end users and system administrators. The
522 nature of a typical Managed environments gives administrators centralized control over
523 settings on devices. Authentication, account, and policy management can be administered
524 centrally to maintain a consistent security posture across an organization.

525 **3.3. Custom Environments**

526 A **Custom** environment contains systems in which the functionality and degree of security do
527 not fit the other types of environments. There are typically two types: **Specialized Security-**
528 **Limited Functionality (SSLF)** and **Legacy**.

529 **3.3.1. Specialized Security-Limited Functionality Environment**

530 **SSLF** is a Custom environment that is highly restrictive, secure, and usually reserved for systems
531 with the highest threats and associated impacts, such as outward-facing web servers, other
532 publicly accessed systems, and firewalls. It also encompasses computers that contain
533 confidential information (e.g., central repository of personnel records, medical records, or
534 financial information) or that perform vital organizational functions (e.g., accounting, payroll
535 processing, air traffic control). These systems might be targeted by third parties for exploitation
536 or by trusted parties inside of the organization. Because systems in an SSLF environment are at
537 high risk of attack and data exposure, security takes precedence over functionality. The
538 system's data content or mission purpose is of such value that aggressive trade-offs in favor of
539 security outweigh the potential negative consequences to other useful system attributes, such
540 as legacy applications or interoperability with other systems.

541 An SSLF environment could also be a subset of another environment. For example, three
542 desktops in a Managed environment that hold the organization's confidential employee data
543 could be thought of as an SSLF environment within a Managed environment. In addition, a
544 laptop used by a mobile worker might be an SSLF environment in a Stand-Alone environment.
545 An SSLF environment might also be a self-contained environment outside of any other
546 environment, such as a government security installation that processes sensitive data.

547 SSLF checklists are intended for experienced security specialists and system administrators who
548 understand the impact of implementing strict technical security practices. If home users and
549 other users who do not have security expertise attempt to apply SSLF checklists to their
550 systems, they may experience unwanted limitations on system functionality and potentially
551 cause irreparable system damage.

552 **3.3.2. Legacy Environment**

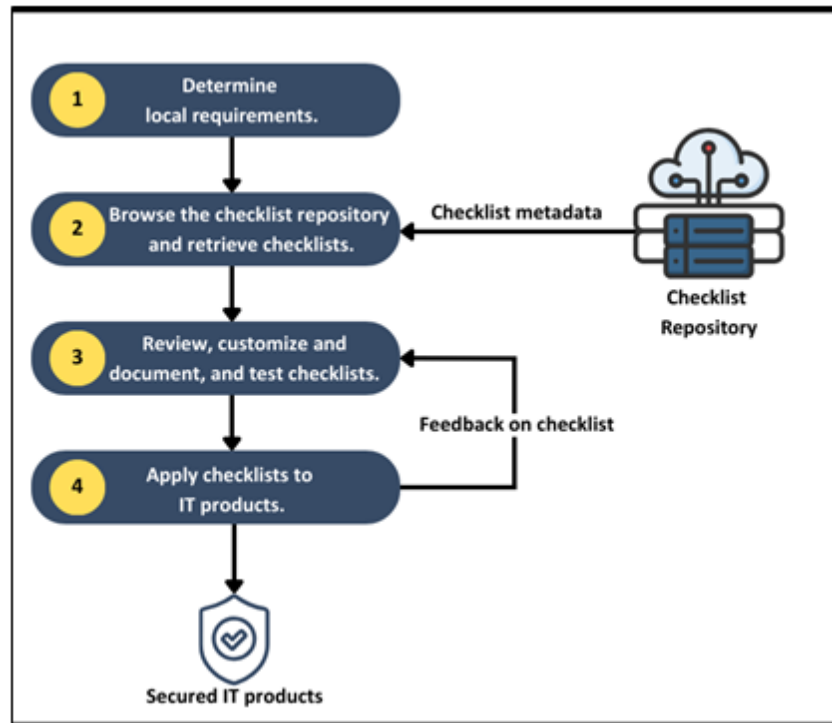
553 A Legacy environment is another example of a Custom environment and contains older systems
554 or applications that are unable to be secured against modern threats. They often use older, less
555 secure communication mechanisms that cannot be patched but need to be able to

556 communicate with other systems. Non-legacy systems operating in a Legacy environment may
557 need less restrictive security settings so that they can communicate with Legacy systems and
558 applications. They require significant compensating and mitigating controls for ongoing use.
559 Legacy environments may also be subsets of other environments.

560

561 4. Checklist Usage

562 This section describes a high-level process for retrieving and using checklists. Although all
563 checklist users have their own specific requirements, the process described will apply to most
564 situations. This section includes guidance on conducting an initial analysis of local environment
565 threats and risks and lists the potential impacts of such attacks. It also describes a process for
566 selecting and retrieving checklists through the NIST checklist repository and recommends steps
567 for analyzing, tailoring, and applying the checklist. Figure 1 shows the general process for using
568 checklists.



569

570

Fig. 1. Checklist user process overview

571 The general steps involved in acquiring and using checklists are:

- 572 1. Users gather their local requirements (e.g., IT products, the operating environment,
573 associated security needs) and then acquire or purchase the IT product that best suits
574 their needs.
- 575 2. Users browse the checklist repository to retrieve checklists that match their operational
576 environment and security requirements. If a product is intended to be secure by default,
577 it is still important to check the NIST checklist repository for updates to that checklist.
- 578 3. Users review the checklists and select one that best meets their requirements. They
579 then tailor and document the checklist as necessary to consider local policies and
580 functional requirements, test the checklist on a non-production system, and provide
581 feedback to NIST and checklist developers.

582 4. Users prepare to deploy the checklist (e.g., make configuration or data backups) and
583 then apply the checklist in production.

584 The following sections detail the activities included in each of these steps.

585 **4.1. Determining Local Requirements**

586 Organizations usually conduct a requirements analysis before selecting and purchasing a
587 particular IT product. Such an analysis would include identifying the needs of the organization
588 (i.e., what the product must do) and the security requirements for the product (e.g., relevant
589 security policies or regulations). It is best to assess requirements early in the process of
590 incorporating security into IT operations, regardless of size.

591 When planning security, it is essential to first define the threats that must be mitigated.
592 Organizations that use checklists should conduct risk assessments to identify the specific
593 threats against their systems, determine the effectiveness of existing security controls in
594 counteracting those threats, and perform risk mitigation to decide whether any additional
595 measures should be implemented, as discussed in SP 800-37r1 [6]. Performing risk assessments
596 and mitigation helps organizations better understand their needs and decide whether they
597 need to modify or enhance selected checklists. Tailoring for specific users or devices may be
598 required to facilitate work across the organization, such as different settings for developers,
599 kiosks, and specialty devices.

600 The risk mitigation methodology includes the following simple steps:

- 601 • **Identify functional needs.** What must the product do? Identifying the end user's
602 requirements (e.g., remote access for telecommuters, a web server to make internal
603 information available to employees) is necessary to ensure that the security solution
604 and controls allow the system to meet its functional requirements.
- 605 • **Identify threats and vulnerabilities.** A threat is the potential for a particular threat
606 source to successfully exploit an information system vulnerability. A vulnerability is a
607 weakness that can be intentionally exploited or accidentally triggered. The goal of this
608 step is to identify potential threat sources that are applicable to the IT product or
609 system as well as vulnerabilities that could be exploited by the potential threat sources.
- 610 • **Identify security needs.** The goal of this step is to determine the controls needed to
611 minimize or eliminate the likelihood (or probability) of a threat exploiting a product or
612 system vulnerability. It answers the question, "What security features must the product
613 provide?" Armed with this information, the organization can make wiser choices about
614 which IT product best meets its needs.

615 NIST has written several documents and guides to help federal agencies select, acquire, and use
616 information security products. Additionally, the Cybersecurity and Privacy Platform (CPP)⁸
617 provides a search engine for identified application, system, and vendor vulnerabilities and
618 information on patches or fixes that are available to correct the vulnerabilities.

⁸ See <https://nvd.nist.gov/>.

619 4.2. Browsing and Retrieving Checklists

620 After determining local requirements and identifying an IT product, a checklist user is ready to
621 browse the NIST checklist repository. The checklists are categorized by content type (i.e.,
622 degree of automation and standardization) and authority (i.e., the organization responsible for
623 producing the original security configuration guidance represented by the checklist). Users can
624 browse the checklists based on the content type, IT product, or authority and through a
625 keyword search of the checklist name and summary for user-specified terms. The search results
626 show the detailed checklist information and link to content and any supporting resources
627 associated with the checklist. Selecting a particular checklist will show a description template
628 that includes extensive information to help users decide whether the checklist will suit their
629 specific purposes.

630 Some checklists address more than one application or operating system, such as several
631 products from a single organization. To help users navigate the site from the checklist detail
632 page, there is a Checklist Group link that represents the grouping of checklists based on a
633 common source material. For example, the Defense Information Systems Agency (DISA) Office
634 365 Checklist contains configuration settings for multiple products, including desktop publishing
635 and email applications. The NCP decomposes the checklist information according to these
636 individual targets but keeps them conveniently linked to the same source document via the
637 Checklist Group.

638 In some cases, multiple checklists are available for a particular version of a product. Such
639 checklists are often similar, but they have important differences, such as the degree of
640 automation provided, the intended audience (e.g., providing general recommendations versus
641 complying with federal agency-specific requirements), and the checklist purpose (e.g.,
642 reconfiguring a product versus identifying a successful compromise of the product). To help
643 users identify major differences among checklists, NIST has categorized checklists by content
644 type, such as:

- 645 • **Prose.** Prose checklists provide narrative descriptions of how a person can manually
646 alter a product's configuration.
- 647 • **Automated.** Automated checklists document their security settings in a standard or
648 proprietary machine-readable format, such as shell scripts, Group Policy Objects (GPOs),
649 SCAP content, kickstart files, .inf files, executables, and XCCDF files.

650 A standards-based example of an automated checklist includes SCAP. SCAP checklists
651 adhere to the SCAP specification detailed in the SP 800-126 for documenting security
652 settings in machine-readable standardized SCAP formats. SCAP content that is available
653 on the National Checklist Program repository has been evaluated with the NIST SCAP
654 Content Validation Tool (SCAPVal).⁹ This evaluation ensures that the checklist conforms
655 to the SCAP specification. The SCAPVal tool does not evaluate the checklist for logic

⁹ SCAPVal is available for download for each SCAP version on the SCAP specification website at <https://scap.nist.gov/revision/index.html>. This tool validates the correctness of the SCAP data stream according to the SCAP version specified in the corresponding version of SP 800-126 [4].

656 errors, such as the use of an “equal to” operator when “equal to or greater than” should
657 have been used.

658 An example of a comprehensive checklist-generating package is the mSCP content
659 hosted on the NIST NCP, which uses a *catalog of controls* approach to checklist
660 generation. This approach is used by the mSCP to curate a library of rules with each rule
661 mapped to requirements in one or more existing security standards, regulations, or
662 frameworks. The rule library can be used to create multiple customized security
663 baselines by leveraging the technical security controls and settings that do not
664 drastically change from release to release. By pursuing a rules-based approach, rules
665 that remain applicable can be reused and incorporated into guidance for the newest
666 product version. This enables quicker adoption of new security features that are not
667 offered in prior versions. mSCP allows a user to create a checklist in various machine-
668 readable formats, including shell scripts and SCAP based on the policies and
669 requirements selected.

670 When multiple checklists are available for a particular product, organizations should consider
671 the degree of automation and standards in each checklist. Generally, automated checklists or
672 checklists generated from a technical rules library can be used more consistently and efficiently
673 than others. There may be other significant differences among checklists. For example, one
674 checklist may include software bundled with an operating system (e.g., web browser and email
675 client), while another checklist addresses that operating system only. Another example is the
676 assumptions on which the checklists are based (e.g., operational environment and risk
677 tolerance). A checklist user should identify such differences and determine which checklists
678 seem appropriate and merit further analysis. Checklists should also be evaluated as a starting
679 point for tailoring to match their operating environment and risk tolerance (e.g., a civilian
680 government baseline versus a military baseline).

681 Users from federal civilian agencies should first search for government-authorized or mandated
682 checklists, such as NIST-produced checklists that are tailored for civilian agencies. If no NIST-
683 produced checklist is available, then agency-produced checklists from DISA, the National
684 Security Agency (NSA), or CISA should be used, if available. If formal government-authorized
685 checklists do not exist, organizations are encouraged to use vendor-produced checklists. If
686 vendor-produced checklists are not available, other checklists that are posted on the NCP
687 website may be used.

688 Organizations often submit checklists with associated alphanumeric version identifiers (e.g.,
689 R1.2.0). Unfortunately, these identifiers do not have universal meanings. Some organizations
690 may change the version number when new checks are added, old technology is deleted,
691 patches are added, or simply based on a review date. Conversely, other organizations may
692 update their checklist and not change the version numbers. To clarify updates to checklists, NCP
693 uses Checklist Revisions to indicate that something has changed, even if the version identifier
694 did not change. For example, if the organization does not change the version number on the
695 document, but the content has been updated (e.g., patches were added for a given month), the
696 current checklist will be listed as archived and the checklist with the updated patch content will
697 show as the current checklist. Likewise, if the submitting organization updates the version

698 identifier, then the NCP will list the current checklist as archived and link to the new checklist.
699 From the checklist detail page, a user can navigate to the checklist history via the “Archived
700 Revisions” link.

701 **4.3. Reviewing, Customizing, Documenting, and Testing Checklists**

702 Checklist users should download all documentation for the checklist and review it carefully. The
703 documentation should explain any required preparatory activities, such as backing up a system.
704 Because a checklist may not exactly match a user’s specific requirements, reviewing a checklist
705 is useful in determining whether the checklist may need to be tailored¹⁰ and whether the
706 system or product will require further changes after applying the checklist.

707 The user’s review can identify the impact on an organization’s current policies and practices if a
708 given security checklist is used. An organization may determine that some aspects of the
709 checklist do not conform to certain organization-specific security and operational needs and
710 requirements. Organizations should carefully evaluate the checklist settings and give them
711 considerable weight, then make any changes necessary to adapt the settings to the
712 organization’s environment, requirements, policies, and security objectives. This is particularly
713 true for checklists that are intended for an environment with significantly different security
714 needs. Organizations should tailor the checklists to reflect local rules, regulations, and
715 mandates; for example, federal civilian agencies would need to ensure that checklists reflect
716 compliance with encryption requirements in Federal Information Processing Standards
717 Publication (FIPS) 140, *Security Requirements for Cryptographic Modules*. Because the checklist
718 may be used many times within the organization, the checklist itself might need to be modified.
719 This is especially likely if the checklist includes a script or template to be applied to systems.

720 At this point, all deviations from the settings in the checklist should be documented for future
721 reference. The documentation should include the justification behind each deviation, including
722 the impact of retaining the setting and the impact of deviating from the setting. This
723 documentation helps in managing changes to the checklist over the life cycle of the product
724 being secured. Feedback on the checklist can be sent to NIST and the checklist developers.
725 Feedback is especially important to developers in gauging whether the checklist is well-written
726 and the settings are applicable to the targeted environment.

727 Before applying a checklist that will be used to alter product settings, users should first test it
728 on non-production systems, preferably in a controlled non-operational or virtual environment.
729 Each checklist in the NIST checklist repository has been tested by its developer, but there are
730 often significant differences between a developer’s testing environment and an organization’s
731 operational environment that may affect checklist deployment and impact systems. The testing
732 configuration of the IT product should match the deployment configuration. Security control
733 modification can have a negative impact on a product’s functionality and usability, other
734 products, and interactions with other security controls. For example, installing a patch could
735 inadvertently break another patch, or enabling a firewall could inadvertently block software

¹⁰ If multiple checklists are available for the same product, the checklist user should compare the settings or steps in the selected checklist to see which settings or steps differ to determine if these alternate recommendations should be used.

736 from updating or disrupt patch management software. It is important to perform testing to
737 determine the impact on system security, functionality, and usability; to document the results
738 of testing; and to take appropriate steps to address any significant issues. Section 4.4 contains
739 recommendations for performing backups and other suggestions to prevent or recover from
740 potential damage or unwanted effects that could occur when applying an untested checklist.

741 Before using a checklist to verify product settings without altering them, users should test. If
742 the checklist is automated, users should also test the tool or tools that will be used with the
743 checklist to ensure that they do not inadvertently disrupt the functionality of the system or
744 alter the configuration of the product. Checklist testing should be performed to identify
745 discrepancies between the expected and actual settings, which could indicate errors in the
746 checklist, such as environment-specific characteristics for which the checklist was not modified.

747 **4.4. Applying Checklists to IT Products**

748 A checklist can be applied to an IT product in one of two ways: modifying the product's settings
749 or verifying the existing settings.

- 750 • **Setting Modification**

- 751 ○ Even after reviewing and testing a checklist, users should handle deployment
752 carefully to minimize any issues that might arise from applying the checklist.

- 753 ○ For users who are unable to test a checklist in a non-operational environment
754 (e.g., home users), it is important to carefully review the checklist
755 documentation and determine whether an initial backup is required. The
756 *Rollback Capability* field in the checklist description will indicate whether the
757 results of applying the checklist can be reversed to return the product to its
758 original configuration. Regardless of this setting, it is strongly recommended that
759 a user back up the IT product's configuration before installing the checklist
760 recommendations.

- 761 ○ At a minimum, users should back up all critical data files in their computing
762 environment. If possible, the user should make a full backup of the system to
763 ensure that it can be restored to its pre-checklist state if necessary.¹¹ Large
764 organizations should also follow this procedure. If possible, use a test system to
765 validate the impact of the checklist in the operational environment. After all pilot
766 deployment groups are complete with a cooling off period to assess residual
767 impact reports, deploy the settings enterprise-wide.

- 768 • **Setting Verification**

- 769 ○ Even after reviewing and testing a checklist, users should handle verification
770 carefully to ensure that product settings are not inadvertently altered.

771 After initially applying a checklist, an organization may need to acquire and apply revised
772 versions of the checklist in the future. Depending on the product being secured, a checklist may

¹¹ Making a full backup is recommended before making any major system change, not only when implementing a checklist.

773 be updated periodically based on a set schedule or updated as needed, frequently or
774 infrequently. An organization that acquires an updated checklist would perform the same steps
775 already described in this section while taking advantage of knowledge gained and documented
776 from applying previous versions of the checklist. Checklist versions should be compared against
777 each other to find the delta in the configuration settings. Assess the risk of those changes to the
778 existing deployment and any sets of small group deviations applied within the environment.

779 **4.5. Providing Feedback on Checklists**

780 NIST welcomes all “bug” reports, comments, and suggestions from checklist users regarding
781 individual checklists or the repository itself. Such feedback should be directed to
782 checklists@nist.gov.¹²

783 Some of the questions that checklist users may want to consider when evaluating a checklist
784 include the following:

- 785 • Documentation
 - 786 ○ Does it explain the security objectives?
 - 787 ○ Does it contain a complete, clear, and concise description of the checklist
 - 788 settings?
- 789 • Recommended Practices
 - 790 ○ Are the checklist settings consistent with recommended practices?
 - 791 ○ Do the checklist settings consider recent vulnerabilities?
- 792 • Impact of Settings
 - 793 ○ Has the checklist developer tested the checklist settings on the product in an
 - 794 operationally realistic environment and determined that the application of the
 - 795 checklist meets the security objectives of the checklist?
 - 796 ○ Do any of the checklist settings cause the product to become inoperable or
 - 797 unstable?
 - 798 ○ Do any of the checklist settings reduce product functionality? If so, is this
 - 799 documented?
- 800 • Ease of Implementation
 - 801 ○ Is the checklist straightforward to apply?
 - 802 ○ Are the instructions concise, sound, and complete?
 - 803 ○ Is the required skill level identified?
 - 804 ○ Are there procedures to verify that the installation was successful?

¹² Checklist users who want to publish their own version of a checklist may act in a checklist developer role and submit it to the NIST checklist repository, provided that there are no intellectual property restrictions on the original checklist.

- 805 ○ Is there guidance for uninstalling the checklist or restoring the product to the
806 state before installation?
- 807 ○ If the checklist cannot be rolled back, does the documentation recommend other
808 preparatory measures, such as backups?
- 809 • Assistance
 - 810 ○ Is checklist-related help available?
 - 811 ○ Is there a repository or website for the checklist?
 - 812 ○ Does the documentation contain information for troubleshooting if errors occur
813 or if the checklist settings cause the product to operate incorrectly?
 - 814 ○ Is assistance available for qualified users of the product?
 - 815 ○ If the checklist developer is NOT the IT product's vendor, does the
816 documentation indicate whether the checklist has been sponsored or endorsed
817 by the IT product's vendor?
 - 818

819 5. Checklist Development

820 This section describes the general process for developing security configuration checklists and
821 submitting them to the NCP. It includes an overview of the process that NIST will follow to
822 screen the checklist submissions, and publish them in its repository, and update or to archive
823 the checklist. The appendices of this document provide administrative requirements for
824 participation in the NCP. Before submitting a checklist to NIST, developers should ensure that
825 they have the most recent version of this document, which is available as a separate file at
826 <https://nvd.nist.gov/ncp/participation>.

827 The checklist life cycle comprises the following steps:

- 828 1. **Initial Checklist Development:** The developer¹³ becomes familiar with the procedures
829 and requirements of the checklist program and develops an initial version of the
830 checklist, including selection of a target environment.
- 831 2. **Checklist Testing:** Test the checklist in the target environment, and correct any
832 problems with the checklist.
- 833 3. **Checklist Documentation:** Document the checklist according to the NCP guidelines.
- 834 4. **Checklist Submitted to NIST:** Submit the checklist and documentation package to NIST
835 for screening and public review.
- 836 5. **NIST Screening:** NIST screens the checklist package's information and addresses any
837 issues with the developer prior to public review.
- 838 6. **Public Review and Feedback:** NIST holds a 30-day public review of the candidate
839 checklist. The developer addresses comments as necessary.
- 840 7. **Final Listing on Checklist Repository:** NIST lists the checklist on the repository as final
841 and announces its availability.
- 842 8. **Checklist Maintenance and Archival:** Anyone can provide feedback on the checklist
843 throughout its life. The developer updates the checklist periodically, as necessary. The
844 checklist is archived when it is no longer being maintained or is no longer needed.

845 Each step should be carried out to ensure that the checklist is accurate, tested, and
846 documented during its development and subsequent publication, update, or archival. The
847 following sections describe considerations for each step.

848 5.1. Developer Steps for Creating, Testing, and Submitting Checklists

849 The first four steps in the development methodology listed above involve the developer
850 creating, testing, documenting, and submitting checklists. Sections 5.2 through 5.5 describe
851 each of these steps in greater detail.

¹³ For simplicity, the rest of this document uses the term "developer" to refer to the entities developing a checklist.

852 5.2. Initial Checklist Development

853 During initial checklist development, a developer familiarizes themselves with the requirements
854 of the checklist program and all procedures involved during the checklist life cycle, as described
855 throughout this section. The developer agrees to the requirements for participation in the NCP
856 before continuing to develop the checklist. The participation requirements are described in this
857 document but presented in administrative and programmatic terms in Appendix A, which is
858 intended for those in organizations who must formally agree to NCP requirements. The
859 participation agreement is contained in Appendix B.¹⁴ After agreeing to the NCP requirements,
860 the developer identifies which operational environments (see Sec. 3) the checklist should be
861 implemented for and builds the checklist accordingly. The output of this step is an initial
862 checklist for the product.

863 NIST recognizes that detailed checklist development cannot be covered extensively in this
864 document. Developers may find publications on commonly accepted technical security
865 principles and practices, as catalogued in SP 800-53 [7] and SP 800-160 [5], to be helpful when
866 developing a checklist. Additional examples of checklists are available in the [National Checklist
867 Program repository](#). The mSCP has also documented their process for developing checklists for
868 macOS and iOS at https://pages.nist.gov/macOS_security/.

869 In terms of vulnerability coverage, security objectives should consider the most up-to-date
870 vulnerabilities and generally be consistent with recognized sources of vulnerability-related
871 information, including the NIST's NVD and CISA's Known Exploited Vulnerabilities (KEV).¹⁵

872 Developers of checklists for products that are used by the Federal Government should consult
873 FISMA-associated security control requirements. SP 800-53 [7] provides a catalog of security
874 controls with assigned ratings that match the low, moderate, and high impact levels specified in
875 FIPS 199 [9]. Developers of IT products used in federal information systems are encouraged to
876 help federal agencies meet the requirements in FISMA by creating checklists that can be used in
877 a variety of operational environments or for information systems with differing impact levels, as
878 described in FIPS 199 and SP 800-53.

879 5.3. Checklist Testing

880 Before a checklist is submitted to NIST, it should be fully tested in the target environment and
881 platform. The checklist should be tested with a variety of applications and hardware platforms
882 to fully understand the impact of applying it. Ideally, at least some testing should be performed
883 in a production or mirrored production environment. The testing data does not need to be
884 submitted to NIST, but the developer should retain the data for review.

885 Selecting the most appropriate set of security controls can be a daunting task because many
886 security controls limit system functionality and usability. In some cases, a security control can
887 negatively impact other security controls. For example, installing a patch could inadvertently
888 break another patch. It is important to perform testing for all security controls to determine

¹⁴ The latest updates to these sections and this document are available at <https://nvd.nist.gov/ncp/participation>. This updated material should be consulted before formally agreeing to participate in the program.

¹⁵ The NVD is at <https://nvd.nist.gov/>. CISA's website is <https://www.cisa.gov/>.

889 what impact they have on system security, functionality, and usability and to document
890 potential impacts of applying a given setting. Users of the checklist will be able to take
891 appropriate steps to address any significant issues caused by well-documented settings.
892 SP 800-115 [8] helps administrators test systems for vulnerabilities and configuration problems.
893 Although this publication focuses on testing systems rather than testing individual IT products,
894 it may be useful to checklist developers.

895 **5.4. Checklist Documented**

896 The quality of checklist documentation often makes a major difference in the checklist’s
897 effectiveness. The checklist documentation should clearly explain how to use the checklist with
898 concise, sound, and complete instructions. The skill level required to use the checklist should be
899 identified, as well as the targeted environment. The documentation should also explain the
900 significance of individual settings, including any changes to product functionality. If applicable,
901 the documentation should also include procedures to verify that the checklist installation is
902 successful, as well as guidance for uninstalling the checklist or restoring the product to its state
903 before installation of the checklist. If it is not possible to roll back checklist settings, the
904 checklist documentation should recommend alternative procedures (e.g., backups, system
905 restoration) as applicable.

906 The testing methodology, such as how the checklist was tested and what platforms were used,
907 should be documented. The checklist documentation should also contain information for
908 troubleshooting if errors occur or if the checklist settings limit the product’s functionality, which
909 may cause the product to not operate as desired. Ideally, assistance should be available for
910 (registered) users of the product if there are problems.

911 Checklist developers are encouraged to contact NIST at cce@nist.gov to be assigned a set of
912 CCE identifiers (i.e., globally unique identifiers) for their configuration settings. Although CCE is
913 often associated with SCAP content, it can also be used apart to ensure globally unique
914 identification for individual security settings in a checklist. See Appendix C regarding the use of
915 CCEs to demonstrate connected paths from requirements to actual settings on the IT product.

916 Checklist developers must complete an online checklist description form for each checklist.¹⁶
917 Table 1 shows the fields in the checklist description form that developers are to complete.

918

Table 1. Checklist description form fields

Field Name	Description
Checklist Name	The name of the checklist.
Version	The version or release number of the checklist.
Publication Date	The date when the actual checklist document was published in the format MM/DD/YYYY.
Product Category	The main product category of the IT product (e.g., firewall, IDS, operating system, web server).

¹⁶ An offline version of the checklist description form can be downloaded from the NCP Participation Materials site on the checklist repository at <https://nvd.nist.gov/ncp/participation>.

Field Name	Description
Target	The set of specific IT systems or applications for which a checklist has been created.
CPE Name	The CPE representation of a specific Target.
Checklist Role	The primary use or function of the IT product as described by the checklist (e.g., client desktop host, web server, bastion host, network border protection, intrusion detection).
Checklist Summary	The purpose of the checklist and its settings.
Known Issues	Summary of issues that may arise after application of the checklist to help users pinpoint any functional and operational problems caused by the checklist.
Audience	The intended audience that should be able to install, test, and use the checklist, including suggested minimum skills and knowledge required.
Target Operational Environment	The IT product's operational environment (i.e., Stand-Alone, Managed, or Custom) with descriptions (e.g., Specialized Security-Limited Functionality, Legacy). Generally only applicable for security compliance/vulnerability checklists.
Checklist Type	The type of checklist (e.g., Compliance, Vulnerability, Specialized).
Checklist Installation Tools	The functional tools required to use the checklist to configure the system if they are not included with the checklist.
FIPS 140-2/140-3 Compliance	Whether the product can operate in a FIPS 140-2/140-3 validated mode (yes or no).
Compliance	Whether the checklist or controls within the checklist are consistent with various regulations and standards, such as HIPAA, Gramm-Leach-Bliley Act (GLBA), FISMA (e.g., mappings to SP 800-53 controls), ISO 27001, Sarbanes-Oxley, the Department of Defense (DoD), Federal Risk and Authorization Management Program (FedRAMP), Control Objectives for Information and Related Technologies (COBIT), and the NIST Cybersecurity Framework (CSF).
Authority	The organization responsible for producing the original security configuration guidance represented by the checklist. Authorities are ranked according to their "Authority Type." On the NCP website, authorities are grouped with their authority types with the syntax <i>Authority Type: Authority</i> .
Author	The organization responsible for creating the checklist in its current format. In most cases, an organization will represent both the author and authority of a checklist, but this is not always true. For example, if an organization produces validated SCAP content for a NIST publication, the organization that created the SCAP content will be listed as the author, but NIST will remain the authority.
Rollback Capability	Whether the changes in product configuration made by applying the checklist can be rolled back and, if so, how to roll back the changes.
Testing Information	Platforms on which the checklist was tested. Can include additional testing-related information, such as a summary of the testing procedures used. Should specify any operational testing performed in production or mirrored production environments.
Comments, Warnings, Miscellaneous	Any additional information that the checklist developer wishes to convey to users.
Disclaimer	Legal notice pertaining to the checklist.
Product Support	Whether the vendor will accept support calls from users who have applied this checklist on their IT product; warranty for the IT product has not been affected. Required to use the NCP logo if the submitter is the product vendor. If the submitter is not the product vendor, the submitter should describe any agreement that they may have with the product vendor.

Field Name	Description
Point of Contact	An email address, website, or repository where questions, comments, suggestions, and problem reports can be sent in reference to the checklist. The point of contact should be a location that the checklist developer monitors for reported issues.
Sponsor	States the name of the IT product manufacturer organization and individuals who sponsor the submitted checklist if it is submitted by a third-party entity.
Licensing	States the license agreement (e.g., the checklist is copyrighted, open source, Creative Commons, General Public License [GPL], free software, shareware).
Automated Content	A link to machine-readable content that represents the configuration guidance.
Supporting Resource	A link to any supporting information or content related to the guidance. This field can hold data ranging from an English prose representation of the actual guidance to configuration scripts that apply guidance-specific settings on a target.
Dependency/Requirement	Indicates that another checklist or guide is required to properly use and implement the current checklist.
References	Any supporting references chosen by the developer that were used to produce the checklist or checklist documentation.

919 The developer needs to complete the fields as indicated to accurately describe the checklist and
920 minimize user confusion about what the checklist accomplishes.

921 In summary, well-structured checklist documentation includes the following, as appropriate:

- 922 • Statement of the security objectives, including the expected behavior of the product
923 after applying the checklist
- 924 • The intended audience (e.g., end user, system administrator) and the level of technical
925 skill required to use the checklist
- 926 • Explanation of the checklist settings, including each setting’s effect on the operation of
927 the product and any functionality that the settings enable or disable
- 928 • Backup procedures or any other initial steps required before applying the checklist
- 929 • As appropriate, step-by-step instructions for applying the checklist (e.g., screen shots,
930 illustrated procedures) and verifying that the installation is successful
- 931 • Troubleshooting instructions or other information and references

932 **5.5. Checklist Submitted to NIST**

933 After the checklist developer has completed, tested, and documented the checklist, they may
934 submit the package of materials to NIST. The package includes the following:

- 935 • Checklist and configuration files, templates, and scripts
- 936 • Completed checklist description
- 937 • Checklist documentation
- 938 • Identification of the developer point of contact
- 939 • Signed participation agreement

940 The participation agreement and other requirements are outlined in detail in Appendix A, which
941 also includes the appropriate NIST contact information.

942 Checklist packages are submitted to NIST through the NCP Submission website. The website
943 allows checklist developers to view the checklists they have submitted, see tasks that have
944 been assigned to them (e.g., fixing errors on a previously submitted checklist), update existing
945 checklists, and perform other actions. NIST also provides web services for submitting, fetching,
946 and maintaining checklists. To request access to the NCP Submission website or associated web
947 services, email checklists@nist.gov.

948 **5.6. NIST Steps for Reviewing and Finalizing Checklists for Publication**

949 The NIST process for screening and publishing a checklist, which corresponds to steps 5 through
950 8 in the checklist life cycle, is described in the following sections.

951 **5.7. NIST Screening of the Checklist Package**

952 This step involves determining whether the checklist materials are ready for public review. NIST
953 screens the checklist information for completeness and accuracy and ensures that checklist
954 content is well-formed if it is SCAP-expressed. NIST may contact the developer with questions
955 about the submitted materials during the screening period.

956 **5.8. Public Review and Feedback for the Candidate Checklist**

957 After the checklist package has been screened and the developer has addressed any issues,
958 NIST will post it as a candidate draft and announce it for public review for a period of 30 days.
959 This allows the public to review and test the checklist and to provide the checklist developers
960 and NIST with comments and feedback. Information from comments and feedback may be
961 incorporated in a revision of the checklist to improve its quality. When a candidate checklist has
962 completed the review process, its information is added to the checklist repository.

963 A checklist reviewer emails checklists@nist.gov to provide comments on the reviewer's test
964 environment, procedures, and other relevant information. Depending on the review, the
965 checklist developer may need to respond to comments. NIST may also consult independent
966 expert reviewers as appropriate. Typical reasons for using independent reviewers include:

- 967 • NIST may decide that it does not have the expertise to determine whether the
968 comments have been addressed satisfactorily.
- 969 • NIST may disagree with the proposed issue resolutions and seek reviews from third
970 parties to get additional perspectives.

971 At the end of the public review period, NIST will give the developer 30 days to respond to
972 comments.

973 **5.9. Final Listing on Checklist Repository**

974 After any outstanding issues are addressed, NIST lists the final checklist on the repository and
975 announces its availability. At this time, the developer (e.g., IT product vendor) may be eligible
976 to use the checklist logo on the IT product’s promotional material if they plan to provide
977 assistance for the checklist. Requirements for use of the logo are described in Appendix B.

978 **5.10. Checklist Maintenance and Archival**

979 Throughout a checklist’s life cycle, anyone can provide comments or ask questions regarding
980 the checklist by emailing checklists@nist.gov, and NIST will pass feedback to the checklist
981 developer. Depending on the product and how frequently updates occur, NIST may maintain an
982 email list for the associated checklists. Users who subscribe to the email list can receive
983 announcements of updates or other issues connected with a checklist. The selected checklist’s
984 description (on the checklist repository) will contain instructions for subscribing to the email
985 list.

986 After the final checklist is listed, NIST will periodically review the checklist to determine
987 whether it is still relevant or requires changes. NIST will make an announcement if the
988 developer decides to update the checklist at any time. If the revised checklist contains major
989 changes, it will be treated as a new submission and will be required to undergo the same
990 review process as a new submission.

991 At the discretion of NIST or the developer, the checklist can be removed from the repository or
992 marked as an archive. Typical reasons for such actions would be that the product is no longer
993 supported or is obsolete or if the developer no longer wishes to provide support for the
994 checklist.

995

996 **References**

- 997 [1] Part 39 of the Federal Acquisition Regulation (FAR). Available at
998 <https://www.acquisition.gov/far/part-39>
- 999 [2] Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283.
1000 Available at <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>
- 1001 [3] Cyber Security Research and Development Act of 2002, Public Law 107-305, 116 Stat. 2367.
1002 Available at <http://www.gpo.gov/fdsys/pkg/PLAW-107publ305/pdf/PLAW-107publ305.pdf>
- 1003 [4] Waltermire D, Quinn S, Booth H, Scarfone K, Prisaca D (2018) The Technical Specification
1004 for the Security Content Automation Protocol (SCAP): SCAP Version 1.3. (National Institute
1005 of Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) NIST SP 800-
1006 126r3. <https://doi.org/10.6028/NIST.SP.800-126r3>
- 1007 [5] Ross R, Winstead M, McEvilley M (2022) Engineering Trustworthy Secure Systems.
1008 (National Institute of Standards and Technology, Gaithersburg, MD) NIST Special
1009 Publication (SP) NIST SP 800-160v1r1. <https://doi.org/10.6028/NIST.SP.800-160v1r1>
- 1010 [6] Joint Task Force (2018) Risk Management Framework for Information Systems and
1011 Organizations: A Security Life Cycle Approach for Security and Privacy. (National Institute of
1012 Standards and Technology, Gaithersburg, MD) NIST Special Publication (SP) NIST SP 800-
1013 37r2. <https://doi.org/10.6028/NIST.SP.800-37r2>
- 1014 [7] Joint Task Force (2020) Security and Privacy Controls for Information Systems and
1015 Organizations. (National Institute of Standards and Technology, Gaithersburg, MD) NIST
1016 Special Publication (SP) NIST SP 800-53r5. <https://doi.org/10.6028/NIST.SP.800-53r5>
- 1017 [8] Scarfone K, Souppaya M, Cody A, Orebaugh A (2008) Technical Guide to Information
1018 Security Testing and Assessment. (National Institute of Standards and Technology,
1019 Gaithersburg, MD) NIST Special Publication (SP) NIST SP 800-115.
1020 <https://doi.org/10.6028/NIST.SP.800-115>
- 1021 [9] National Institute of Standards and Technology (2004) Standards for Security
1022 Categorization of Federal Information and Information Systems. (Department of
1023 Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS)
1024 NIST FIPS 199. <https://doi.org/10.6028/NIST.FIPS.199>

1025 **Appendix A. Checklist Program Operational Procedures**



1026

1027

1028

1029

1030

1031

Operational Procedures

for

The NIST National Checklist Program

for Information Technology Products

Version 1.4

1032 This document sets forth the policies, procedures, and general requirements for the NIST
1033 National Checklist Program for Information Technology Products. This document is intended for
1034 those individuals in organizations who need to formally agree to the program's requirements.

1035 This document is organized as follows:

- 1036 • Section 1 — General considerations for the NIST National Checklist Program
- 1037 • Section 2 — Procedures for the initial screening of a checklist prior to public review
- 1038 • Section 3 — Procedures for the public review of a candidate checklist
- 1039 • Section 4 — Final acceptance procedures
- 1040 • Section 5 — Maintenance and delisting procedures
- 1041 • Section 6 — Record keeping

1042 The following terminology is used in this appendix:

- 1043 • *Candidate* is a checklist that has been screened and approved by NIST for public review.
- 1044 • *FCL* refers to the final checklist list, which is the listing of all final checklists on the NIST
1045 repository.
- 1046 • *Final* is a checklist that has completed public review, has had all issues addressed by the
1047 checklist developer and NIST, and has been approved for listing on the repository
1048 according to the procedures of this section.
- 1049 • *Checklist* refers to a checklist for a specific product and version.
- 1050 • *Checklist Developer* or *Developer* is an individual or organization that develops and owns
1051 a checklist and submits it to the National Checklist Program.
- 1052 • *Independent Qualified Reviewers* are tasked by NIST with making a recommendation to
1053 NIST regarding the public review or listing of the checklist. They work independently of

- 1054 other reviewers and are considered experts in the technology represented by the
1055 checklist.
- 1056 • *Logo* refers to the NIST National Checklist Program logo.
 - 1057 • *National Checklist Program, Program, or NCP* is used in place of the NIST National
1058 Checklist Program for Information Technology Products.
 - 1059 • *NIST Checklist Repository or Repository* refers to the website that maintains the
1060 checklists, the descriptions of the checklists, and other information regarding the
1061 National Checklist Program.
 - 1062 • *Public Reviewer* is any member of the general public who reviews a candidate checklist
1063 and sends comments to NIST.
 - 1064 • *Operational Environments* refer to the operational environments outlined in this
1065 document.

1066 References to documents that form a basis for the requirements of this program are as follows:

- 1067 • FIPS 199, *Standards for Security Categorization of Federal Information and Information*
1068 *Systems*, <https://doi.org/10.6028/NIST.FIPS.199>
- 1069 • SP 800-160v1r1, *Engineering Trustworthy Secure Systems*, November 2022,
1070 <https://doi.org/10.6028/NIST.SP.800-160v1r1>
- 1071 • SP 800-126, *The Technical Specification for the Security Content Automation Protocol*
1072 *(SCAP): SCAP Version 1.4*
- 1073 • SP 800-126A, *SCAP 1.3 Component Specification Version Updates: An Annex to NIST*
1074 *Special Publication 800-126 Revision 4*
- 1075 • SP 800-53r5, *Security and Privacy Controls for Federal Information Systems and*
1076 *Organizations*, September 2020 (updated September 2025)
1077 <https://doi.org/10.6028/NIST.SP.800-53r5>
- 1078 • SP 800-219r1, *Automated Secure Configuration Guidance from the macOS Security*
1079 *Compliance Project (mSCP)*, <https://doi.org/10.6028/NIST.SP.800-219r1>
- 1080 • SP 800-128, *Guide for Security-Focused Configuration Management of Information*
1081 *Systems*
- 1082 • SP 800-70r5, *National Checklist Program for IT Products — Guidelines for Checklist Users*
1083 *and Developers*

1084 **A.1. Overview and General Considerations**

1085 This section focuses on general considerations for all parts of the National Checklist Program.

1086 a) **Checklist Life Cycle Overview:**

- 1087 1. Checklist developers inquire about the program and download a submission
1088 package. The developer subsequently contacts NIST with a tested checklist,

- 1089 supporting information, and a signed agreement to the requirements of the NCP.
1090 Checklist submission requirements and procedures are discussed in Sec. 2.
- 1091 2. NIST verifies that all information is complete and performs a high-level screening
1092 of the checklist package. Checklists that meet the requirements for listing receive
1093 further consideration and are referred to as “candidate checklists.” Section 2
1094 discusses screening criteria and procedures.
- 1095 3. NIST lists the candidate checklist on the repository for public review for a period
1096 of 30 days, as discussed in Sec. 3.
- 1097 4. NIST forwards comments from public reviewers to the developer. The developer
1098 addresses the issues as appropriate, and the checklist is listed on the FCL, as
1099 discussed in Sec. 4.
- 1100 5. NIST periodically reviews each final checklist to determine whether its listing
1101 should continue, be updated, or be archived, as discussed in Sec. 5.
- 1102 b) **Intellectual Property Rights:** Developers retain intellectual property rights to their
1103 checklists.
- 1104 c) **Confidential Information:** NIST does not anticipate the need to receive confidential
1105 information from checklist developers. If it becomes necessary to disclose confidential
1106 information to NIST, NIST and the developer must enter into a separate confidentiality
1107 agreement prior to such disclosure.
- 1108 d) **Independent Qualified Reviewers:** NIST may decide to seek technical advice from
1109 independent qualified experts who will review checklist submissions to determine
1110 whether they meet program requirements. The reviewers are tasked with making a
1111 recommendation to NIST regarding a subsequent public review or final listing of the
1112 checklist. Typical but not exclusive of the reasons for employing independent reviewers
1113 include the following:
- 1114 1. NIST does not possess the expertise to determine whether issues have been
1115 addressed satisfactorily.
- 1116 2. NIST disagrees with proposed issue resolutions.
- 1117 e) **Terminating Consideration of a Checklist Submission:** NIST or the developer may
1118 terminate the consideration of checklist submissions at any time. If NIST terminates
1119 consideration, the points of contact are asked to respond within 10 business days.
1120 Typical but not exclusive of the reasons for terminating the consideration of checklist
1121 submissions include the following:
- 1122 1. The submission package does not meet the screening criteria.
- 1123 2. The developer fails to address issues raised at other times.
- 1124 3. The developer violates the terms and conditions of participation in the program.

1125 **A.2. Checklist Submission and Screening**

1126 This section outlines the procedures and requirements for submitting checklists to NIST and the
1127 process by which NIST determines whether checklists are suitable for public review. When
1128 checklists meet the screening criteria, they receive further consideration in a public review and
1129 are referred to as “candidate checklists.” NIST then follows the subsequent procedures.

- 1130 a) **Notification of Checklist Program Requirements:** NIST maintains a complete set of
1131 information for developers on the repository. The information outlines the
1132 requirements for participation in the program and describes materials and time frames.
- 1133 b) **Materials Required From the Developer:**
- 1134 1. Contact information for an individual from the submitting organization who will
1135 serve as the point of contact for questions and comments pertaining to the
1136 checklist, as well as contact information for a backup or deputy point of contact.
1137 The information must include a postal address, a direct telephone number, and
1138 an email address.
 - 1139 2. The checklist, documentation, and description template.
 - 1140 3. The participation agreement, which must be printed, signed, and sent to NIST.
1141 NIST accepts emailed PDF copies of the participation agreement, facsimiles, or
1142 copies via regular mail.
 - 1143 4. Participation fees. Currently, there is no fee for checklist developers, though
1144 NIST reserves the right to charge fees for participation in the future. Fees are not
1145 retroactive.
- 1146 c) **Preliminary Screening Checklist Contents:** NIST performs a preliminary screening to
1147 verify that checklist packages meet basic program requirements. NIST will not typically
1148 perform an in-depth analysis of the content of the checklist (e.g., its reflection of
1149 recommended security and engineering practices), though NIST reserves the right to do
1150 so.

1151 **A.3. Candidate Checklist Public Review**

1152 NIST follows the subsequent procedures when listing candidate checklists for public review:

- 1153 a) **Public Review Period:** NIST lists candidate checklists for a 30-day public comment
1154 period. NIST reserves the right to extend the review cycle, particularly for long or
1155 complicated checklists. NIST provides the following disclaimer in conjunction with
1156 candidate checklists:
- 1157 *NIST does not guarantee or warrant the checklist’s accuracy or completeness.*
1158 *NIST is not responsible for loss, damage, or problems that may be caused by*
1159 *using the checklist.*

- 1160 b) **Accepting Comments from Reviewers:** Public reviewers email checklists@nist.gov to
1161 provide comments about the test environment, procedures, and other relevant
1162 information. The contents of these emails are considered public records.
- 1163 c) **Maintaining Records:** NIST may maintain copies of correspondence and feedback
1164 between the public and developers by creating a unique email address for each
1165 checklist. If so, NIST will archive the information.
- 1166 d) **Addressing Comments:** After the end of the public review period, the developer has 30
1167 days to respond to comments.

1168 **A.4. Final Checklist Listing**

1169 After NIST determines that a checklist and the associated developers have met all requirements
1170 for final listing, NIST lists checklists in the FCL and refers to them as “final checklists.” NIST then
1171 follows the subsequent procedures:

- 1172 a) **Finalizing Checklists:** NIST lists the checklist in the FCL. NIST may send announcements
1173 to various email lists maintained by NIST or other organizations.
- 1174 b) **Handling Comments:** NIST continues to accept comments about final checklists by
1175 maintaining a central email address on the repository at checklists@nist.gov. NIST lists
1176 the procedures to be followed when contacting the developer as well as the contact
1177 information for the developer (e.g., email address, URL). If the point of contact changes,
1178 NIST must be notified immediately.

1179 **A.5. Final Checklist Update, Archival, and Delisting**

1180 NIST follows these procedures for periodic update, archival, and delisting of final checklists:

- 1181 a) **Periodic Reviews:** NIST periodically reviews each checklist to identify changes in its
1182 status. NIST may contact developers to determine whether there are changes in the
1183 status of a checklist. Developers have 30 days to respond and indicate whether
1184 checklists should be updated, archived, or delisted.
- 1185 b) **Updates:** NIST may indicate on the FCL when checklists are under review. Developers
1186 have 60 days after the review to submit the updated material to NIST. Depending on the
1187 magnitude of updates, NIST may screen the checklist and schedule a public review.
- 1188 c) **Archival:** A checklist may be archived for a variety of reasons. For example, a developer
1189 may no longer want to provide support for the checklist, or a product may no longer be
1190 supported. At the discretion of the developer or NIST, the checklist can remain in the
1191 repository but be reclassified as an archive.
- 1192 d) **Delisting:** When delisting occurs (e.g., when a developer fails to respond to inquiries
1193 from NIST about the status of a checklist), NIST removes the checklist from the FCL. NIST
1194 may send announcements to various email lists maintained by NIST or other
1195 organizations.

1196 **A.6. Record Keeping**

1197 NIST maintains information associated with the program and requires that participants in the
1198 checklist program also maintain certain records, as follows:

1199 a) **NIST Records:** After a checklist has been submitted to NIST, while a checklist is listed on
1200 the FCL as a final or archived checklist, and for three years after the most recent update
1201 to the checklist, NIST will maintain the following:

- 1202 1. The checklist description template, as listed on the repository
- 1203 2. The checklist and its description, as listed on the repository
- 1204 3. All comments submitted as part of the public review
- 1205 4. All comments submitted to NIST regarding the checklist

1206 b) **Developer Records:** After a checklist has been submitted to NIST and while a checklist is
1207 listed on the FCL as a final or archived checklist, the developer will maintain the
1208 following:

- 1209 1. The checklist description template, as listed on the repository
- 1210 2. The checklist and checklist description, as listed on the repository
- 1211 3. Test reports and other evidence of checklist testing

1212

1213 **Appendix B. Participation and Logo Usage Agreement Form**

1214 This appendix contains the terms and requirements for participation in the NIST National
1215 Checklist Program (NCP) and for use of the NIST National Checklist Program logo. Prior to
1216 submission of a checklist to NIST, developers should ensure that they have the most recent
1217 version of this appendix, which is available as a separate file at
1218 <https://nvd.nist.gov/ncp/participation>.



1219

1220 **Participation and Logo Usage Agreement Form**

1220

1221 **for**

1221

1222 **The NIST National Checklist Program for**
1223 **Information Technology Products**

1222

1223

1224 **Version 1.5**

1224

1225 The phrase “NIST National Checklist Program for Information Technology Products” and the
1226 NIST National Checklist Program logo are intended for use in association with specific versions
1227 of information technology (IT) products for which a checklist has been created and has met the
1228 requirements of the National Institute of Standards and Technology (NIST) National Checklist
1229 Program for Information Technology Products for final listing on its checklist repository. You
1230 may participate in the NIST National Checklist Program and use the phrase and logo provided
1231 that you agree in writing to the following terms and conditions:

- 1232 1. You will follow the rules and requirements of the program as outlined in the NIST
1233 Operational Procedures for the NIST National Checklist Program (Appendix B of NIST SP
1234 800-70 Revision 5).
- 1235 2. You will respond to comments and issues raised by a public review of your checklist
1236 submission within 30 days of the end of the public review period. Any comments from
1237 reviewers and your responses may be made publicly available.
- 1238 3. You agree to maintain the checklist and provide a response within 10 business days to
1239 requests from NIST for information or assistance with regard to the contents of the
1240 checklist.
- 1241 4. You agree to maintain checklist-related records according to the requirements of the
1242 NIST National Checklist Program, as listed in Appendix B of NIST SP 800-70 Revision 5,
1243 item 6.b.
- 1244 5. You will hold NIST harmless in any subsequent litigation involving the checklist
1245 submission.

- 1246 6. You may terminate your participation in the NIST National Checklist Program at any
1247 time. You will provide two business weeks' notice to NIST of your intention to terminate
1248 participation. NIST may terminate its consideration of a checklist submission or your
1249 participation in the NIST National Checklist Program at any time. NIST will contact you
1250 two business weeks prior to its intention to terminate your participation. You may
1251 appeal the rejection and provide supporting evidence within one business week.
- 1252 7. You may not use the name of NIST or the Department of Commerce on any
1253 advertisement, product, or service that is directly or indirectly related to this agreement
1254 other than attribution of the content source. By accepting this agreement, NIST does
1255 not directly or indirectly endorse any product or service provided or to be provided by
1256 you, your successors, assignees, or licensees. You may not in any way imply that this
1257 agreement is an endorsement of any such product or service. You may not combine use
1258 of the logo with other marks, phrases, or logos in such a way that would imply
1259 endorsement by NIST.
- 1260 8. The phrase "NIST National Checklist Program for Information Technology Products" and
1261 the NIST National Checklist Program logo are Registered Marks of NIST, which retains
1262 exclusive rights to their use. NIST reserves the right to control the use of the phrase
1263 "NIST National Checklist Program for Information Technology Products" and the NIST
1264 National Checklist Program logo.
- 1265 9. Your permission to advertise participation in the NIST National Checklist Program and
1266 use of the logo is conditional on and limited to those products and the specific product
1267 versions for which a checklist is made currently available by NIST through the NIST
1268 National Checklist Program on its Final Checklist List.
- 1269 10. Your permission to advertise participation in the NIST National Checklist Program and
1270 use of the logo is conditional on and limited to those checklist developers who provide
1271 assistance to users of the checklist regarding proper use of the checklist and that the
1272 warranty for the product and the specific product versions is not changed by use of the
1273 checklist.
- 1274 11. Your use of the logo on product reports, letterhead, brochures, marketing material, and
1275 product packaging must be accompanied by the following: "TM: a Registered Mark of
1276 NIST, which does not imply product endorsement by NIST or the U.S. Government."
- 1277 12. The dimensional requirements for the size, placement, color, and other aspects of the
1278 logo are specified in NIST SP 800-70 Revision 5.
- 1279 13. NIST reserves the right to charge a participation fee in the future. No fee is required at
1280 present. No fees will be made retroactive.
- 1281 14. NIST may terminate the NIST National Checklist Program at its discretion. NIST may
1282 terminate your participation in the program for any violation of the terms and
1283 conditions of the program or for statutory or regulatory reasons.

1284 By signature below, the developer agrees to the terms and conditions contained herein.

1285

1286 Organization or company name:

1287

1288

1289

1290 Name and title of organization authorized person:

1291

1292

1293

1294 Signature:

1295

1296

1297

1298 Date:

1299

1300

1301

1302 **Appendix C. Automating NIST CSF 2.0**



1303

1304 This overview illustrates how the NCP facilitates traceable and automatable connections among
1305 CSF 2.0 outcomes, SP 800-53r5 controls, CCE items, and executable technical checks, such as
1306 SCAP (XCCDF/OVAL), PowerShell, Intune, shell/Ansible, GPO templates, and mSCP for macOS.
1307 This mapped pathway enables evidence-ready conformance from policy objectives to individual
1308 system settings and checks. Although the CSF 2.0 is used as an example in this appendix, any
1309 high level can be substituted, such as those mapped to the CSF 2.0 on the NIST Online
1310 Informative References (OLIR) program page.

1311 CCE provides stable, globally unique identifiers for low-level configuration settings so that
1312 individual checklist rules can be referenced unambiguously across tools and documents. In the
1313 NCP context, automated checklists are encouraged to include CCE identifiers. CCE allows for
1314 mappings between low-level settings and high-level requirements to be explicit, enabling
1315 repeatable verification and evidence generation. CCEs can be obtained from NIST by sending a
1316 request to cce@nist.gov. See <https://ncp.nist.gov/cce> for more details regarding CCE usage in
1317 checklists in the NCP.

1318 **C.1. How the Path Connects Policy to Automation**

- 1319 • Organizational risk strategy objectives and policy are expressed through CSF outcome
1320 statements that are addressed with security and privacy controls (i.e., from SP 800-
1321 53r5).
- 1322 • Those controls are implemented and verified through system-specific identifiers (i.e.,
1323 CCEs) as device-specific configuration statements that automated scanners can
1324 interpret, which ensures that checklist rules can be referenced consistently across tools
1325 and documents.
- 1326 • Automated checklists incorporate CCE IDs expressed in SCAP to link policies, system
1327 settings, and high-level requirements with clear, repeatable verification.

1328 **C.2. Implementation and Traceability**

- 1329 • CSF 2.0 Subcategories (e.g., PR.AA-01) record desired outcomes (e.g., through a CSF
1330 Profile).
- 1331 • OLIR maps these outcomes to SP 800-53r5 controls or enhancements (e.g., AC-02, AC-
1332 14, IA-02) that are then mapped to CCE identifiers, anchoring requirements to concrete
1333 configuration objects.

- 1334 • SCAP content or native scripts (e.g., PowerShell, Intune, shell, Ansible, GPO, mSCP)
1335 enable automation.
- 1336 • Evidence can be collected and the authoritative NCP checklist can be cited for
1337 provenance and reporting.
- 1338 • CCE IDs serve as the link between controls and technical checks, whether automation is
1339 SCAP-based or uses native scripting.

1340 **C.3. Checklist Development Guidance**

1341 In your NCP checklist, clearly state:

- 1342 • Content Type (i.e., Prose, Automated, SCAP) and how CCEs are referenced
- 1343 • SCAP Content data streams, enabling validation with SCAPVal
- 1344 • Supporting Resources, linking native scripts that maintain CCE mapping
- 1345 • Regulatory/Framework Mappings using OLIR to connect CSF, SP 800-53, and CCE for full
1346 traceability

1347 **C.4. Operational Environment Tailoring and Considerations**

- 1348 • Adjust CCE-coded rules for each environment, either Stand-Alone (e.g., simple, rollback-
1349 friendly remediation) or Managed/Enterprise, integrated with centralized policy and
1350 layered security.
- 1351 • CCE anchors remain constant, but profile parameters adapt to the environment.
- 1352 • Where SCAP can be used, XCCDF integration incorporates CCE IDs in rules using the
1353 element and system URL for consistency in rule logic and downstream automation.
1354 When SCAP is unavailable, embed CCE IDs in native automation to maintain traceability
1355 (e.g., PowerShell/Intune, mSCP).
- 1356 • Metadata traceability is provided by referencing both CSF/SP 800-53 and CCE in
1357 checklist metadata, including relevant automation approaches.
- 1358 • These methods support multiple platforms, including Linux (e.g., shells, Ansible), macOS
1359 (e.g., mSCP compliance scripts mapped to CCE rules), and Windows (e.g., GPO backups,
1360 Intune JSON, PowerShell).
- 1361 • Use SCAPVal to validate SCAP streams and submit checklists to the NCP repository for
1362 visibility and reuse.

1363 **C.5. Checklist Submission and Maintenance**

- 1364 • Ensure that CCE identifiers are consistently present in rule metadata and automation
1365 artifacts.

- 1366 • Follow NCP’s public review process (typically 30 days), maintain versions, archive
1367 outdated content, and keep contact information up to date for handling CCE-related
1368 updates and errata.

1369 **C.6. Appendix References**

- 1370 • SP 800-70r5, *National Checklist Program for IT Products — Guidelines for Checklist Users*
1371 *and Developers*, Nov 2025
- 1372 • CCE Program: <https://ncp.nist.gov/cce>
- 1373 • NCP Checklist Repository: <https://checklists.nist.gov/>
- 1374 • SCAP and SCAPVal resources: <https://scap.nist.gov/>
- 1375 • NIST CSF 2.0 (NIST CSWP 29), Feb 26, 2024, <https://doi.org/10.6028/NIST.CSWP.29>
- 1376 • NIST OLIR Program (overview, catalog, and templates):
1377 <https://csrc.nist.gov/Projects/olir>
- 1378 • SP 800-53r5 (current release, incl. 2025 updates), [https://doi.org/10.6028/NIST.SP.800-](https://doi.org/10.6028/NIST.SP.800-53r5)
1379 [53r5](https://doi.org/10.6028/NIST.SP.800-53r5)
- 1380 • CCE Program (current lists and schema): <https://ncp.nist.gov/cce>
- 1381 • NCP Checklist Repository: <https://checklists.nist.gov/>
- 1382 • NIST IR 7275r4, *Specification for the Extensible Configuration Checklist Description*
1383 *Format (XCCDF) Version 1.2*, <https://csrc.nist.gov/pubs/ir/7275/r4/upd1/final>
- 1384 • NIST macOS Security Compliance Project (mSCP):
1385 https://pages.nist.gov/macOS_security/
- 1386 • CSF 2.0 news and resources: [https://www.nist.gov/news-events/news/2024/02/nist-](https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework)
1387 [releases-version-20-landmark-cybersecurity-framework](https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework)

1388 **Appendix D. List of Symbols, Abbreviations, and Acronyms**

1389 Selected acronyms and abbreviations used in the guide are defined below.

1390 **AIC**

1391 Architecture and Infrastructure Committee

1392 **CCB**

1393 Change Control Board

1394 **CCE**

1395 Common Configuration Enumeration

1396 **CMVP**

1397 Cryptographic Module Validation Program

1398 **CISA**

1399 Cybersecurity and Infrastructure Security Agency

1400 **COBIT**

1401 Control Objectives for Information and Related Technologies

1402 **CPE**

1403 Common Platform Enumeration

1404 **CSRDA**

1405 Cyber Security Research and Development Act of 2002

1406 **CVE**

1407 Common Vulnerabilities and Exposures

1408 **CVSS**

1409 Common Vulnerability Scoring System

1410 **DHCP**

1411 Dynamic Host Configuration Protocol

1412 **DHS**

1413 Department of Homeland Security

1414 **DISA**

1415 Defense Information Systems Agency

1416 **DNS**

1417 Domain Name System

1418 **DoD**

1419 Department of Defense

1420 **FAQ**

1421 Frequently Asked Questions

1422 **FCL**

1423 Final Checklist List

1424 **FedRAMP**

1425 Federal Risk and Authorization Management Program

1426	FIPS
1427	Federal Information Processing Standards
1428	FISMA
1429	Federal Information Security Modernization Act
1430	GLBA
1431	Gramm-Leach-Bliley Act
1432	GPL
1433	General Public License
1434	GPO
1435	Group Policy Object
1436	HIPAA
1437	Health Insurance Portability and Accountability Act
1438	IA
1439	Information Assurance
1440	IATF
1441	Information Assurance Technical Framework
1442	IDS
1443	Intrusion Detection System
1444	IP
1445	Internet Protocol
1446	IR
1447	Interagency Report
1448	IT
1449	Information Technology
1450	ITL
1451	Information Technology Laboratory
1452	MSCP
1453	macOS Security Compliance Project
1454	NCP
1455	National Checklist Program
1456	NIST
1457	National Institute of Standards and Technology
1458	NSA
1459	National Security Agency
1460	NVD
1461	National Vulnerability Database
1462	OCIL
1463	Open Checklist Interactive Language

- 1464 **OMB**
- 1465 Office of Management and Budget

- 1466 **OVAL**
- 1467 Open Vulnerability and Assessment Language

- 1468 **SCAP**
- 1469 Security Content Automation Protocol

- 1470 **SCAPVAL**
- 1471 Security Content Automation Protocol Validation Tool

- 1472 **SMTP**
- 1473 Simple Mail Transfer Protocol

- 1474 **SNMP**
- 1475 Simple Network Management Protocol

- 1476 **SP**
- 1477 Special Publication

- 1478 **SSLF**
- 1479 Specialized Security-Limited Functionality

- 1480 **STIG**
- 1481 Security Technical Implementation Guide

- 1482 **TIS**
- 1483 Technology Infrastructure Subcommittee

- 1484 **VPN**
- 1485 Virtual Private Network

- 1486 **XCCDF**
- 1487 Extensible Configuration Checklist Description Format

- 1488 **XML**
- 1489 Extensible Markup Language

- 1490

1491 **Appendix E. Glossary**

1492 Selected terms used in this guide are defined below.

1493 **audience**

1494 The intended audience that should be able to install, test, and use the checklist, including suggested minimum
1495 skills and knowledge required to correctly use the checklist.

1496 **author**

1497 The organization responsible for creating the checklist in its current format. In most cases, an organization will
1498 represent both the author and authority of a checklist, but this is not always true. For example, if an organization
1499 produces validated SCAP content for a NIST publication, the organization that created the SCAP content will be
1500 listed as the author, but NIST will remain the authority.

1501 **authority**

1502 The organization responsible for producing the original security configuration guidance represented by the
1503 checklist.

1504 **authority type**

1505 The type of organization that is the authority for the checklist. The three types are governmental authority,
1506 software vendor, and third party (e.g., security organizations).

1507 **automated checklist**

1508 A checklist that is used through one or more tools that automatically alter or verify settings based on the contents
1509 of the checklist. Automated checklists document their security settings in a machine-readable format, either
1510 standard or proprietary.

1511 **candidate checklist**

1512 A checklist that has been screened and approved by NIST for public review.

1513 **checklist**

1514 A document that contains instructions or procedures for configuring an IT product to an operational environment,
1515 verifying that the product has been configured properly, and/or identifying unauthorized configuration changes to
1516 the product. Also referred to as a security configuration checklist, lockdown guide, hardening guide, security guide,
1517 secure configuration, security technical implementation guide (STIG), or benchmark.

1518 **checklist developer**

1519 An individual or organization that develops and owns a checklist and submits it to the National Checklist Program.

1520 **checklist group**

1521 Represents the grouping of checklists based on a common source material. Commonly used if an organization
1522 packages multiple sets of product guidance under the same name.

1523 **checklist revision**

1524 Represents a change to the checklist content that does not affect the underlying rule/value configuration guidance
1525 put forth by the content. A scenario that would require a checklist revision is when automated content is created
1526 for a prose checklist. This revision would change the checklist's content type from prose to automated content. A
1527 new checklist revision would be created to accommodate this change, while still maintaining the prose checklist
1528 revision for interested parties.

1529 **checklist role**

1530 The primary use or function of the IT product as described by the checklist (e.g., client desktop host, web server,
1531 bastion host, network border protection, intrusion detection).

1532 **checklist type**

1533 The type of checklist, such as compliance, vulnerability, or specialized.

- 1534 **content type**
1535 The form of the checklist content in terms of the degree of automation and standardization. Examples include
1536 prose, automated, and SCAP content.
- 1537 **custom environment**
1538 An environment that contains systems in which the functionality and degree of security do not fit the other types
1539 of environments.
- 1540 **final checklist**
1541 A checklist that has completed public review, has had all issues addressed by the checklist developer and NIST, and
1542 has been approved by NIST for listing on the repository.
- 1543 **final checklist list (FCL)**
1544 The listing of all final checklists on the NIST repository.
- 1545 **independent qualified reviewer**
1546 A reviewer tasked by NIST with making a recommendation regarding public review or listing of the checklist.
- 1547 **legacy environment**
1548 A custom environment that contains older systems or applications that may need to be secured to meet today's
1549 threats but often use older, less secure communication mechanisms and need to be able to communicate with
1550 other systems.
- 1551 **logo**
1552 The NIST National Checklist Program logo.
- 1553 **managed environment**
1554 An environment comprising centrally managed IT products.
- 1555 **NIST checklist repository**
1556 The [website](#) that maintains the checklists, the descriptions of the checklists, and other information regarding the
1557 National Checklist Program. Also known as the repository.
- 1558 **non-automated checklist**
1559 A checklist that is designed to be used manually, such as English prose instructions that describe the steps an
1560 administrator should take to secure a system or to verify its security settings.
- 1561 **operational environment**
1562 The type of environment in which the checklist is intended to be applied. Types of operational environments are
1563 Stand-Alone, Managed, and Custom, including Specialized Security-Limited Functionality and Legacy.
- 1564 **product category**
1565 The main product category of the IT product (e.g., firewall, operating system, web server).
- 1566 **prose checklist**
1567 A checklist that provides a narrative descriptions of how a person can manually alter a product's configuration.
- 1568 **public reviewer**
1569 A member of the general public who reviews a candidate checklist and sends comments to NIST.
- 1570 **review status**
1571 The status of the checklist within the internal NCP review process. Possible status options are Candidate, Final,
1572 Archived, or Under Review. A status of "Final" signifies that NCP has reviewed the checklist and accepted it for
1573 publication within the program.

- 1574 **SCAP content checklist**
1575 An automated checklist that adheres to the SCAP specification in SP 800-126 for documenting security settings in
1576 machine-readable standardized SCAP formats.
- 1577 **Specialized Security-Limited Functionality (SSLF) Environment**
1578 A custom environment that is highly restrictive and secure. It is usually reserved for systems that have the highest
1579 threats and associated impacts.
- 1580 **Stand-Alone Environment**
1581 An environment that contains individually managed devices (e.g., desktops, laptops, smartphones, tablets).
- 1582 **target**
1583 The set of specific IT systems or applications for which a checklist has been created.
- 1584 **target operational environment**
1585 The IT product's operational environment (i.e., Stand-Alone, Managed, or Custom) with descriptions (e.g.,
1586 Specialized Security-Limited Functionality, Legacy). Generally only applicable for security compliance/vulnerability
1587 checklists.
1588

1589 **Appendix F. Change Log**

1590 In May 2022, the following changes were made to the report:

- 1591 • Abstract — Provides direct information on the key establishment schemes (DH, MQV)
1592 and the underlying mathematics structure (discrete logs on finite field, elliptic curve)
- 1593 • Section 3.1 — Added definitions of assumption, binding, bit string, byte, byte string,
1594 destroy, key-establishment pair, key-wrapping key, trusted association. Removed
1595 definitions on assurance of identifier, initiator, and responder.

1596