
**National Checklist Program for IT
Products – Guidelines for Checklist
Users and Developers**

Stephen D. Quinn
Murugiah Souppaya
Melanie Cook
Karen Scarfone

C O M P U T E R S E C U R I T Y

23 **Draft NIST Special Publication 800-70**
24 **Revision 4**

25 **National Checklist Program for IT**
26 **Products – Guidelines for Checklist**
27 **Users and Developers**
28

29 Stephen D. Quinn
30 Murugiah Souppaya
31 Melanie Cook
32 *Computer Security Division*
33 *Information Technology Laboratory*
34

35 Karen Scarfone
36 *Scarfone Cybersecurity*
37 *Clifton, VA*
38

39
40
41
42 August 2017
43
44



45
46
47
48 U.S. Department of Commerce
49 *Wilbur L. Ross, Jr., Secretary*
50

51 National Institute of Standards and Technology
52 *Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology*

53

Authority

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

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

67 National Institute of Standards and Technology Special Publication 800-70 Revision 4
68 Natl. Inst. Stand. Technol. Spec. Publ. 800-70 Rev. 4, 53 pages (August 2017)
69 CODEN: NSPUE2
70

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

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

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

84

85 **Public comment period: August 1, 2017 through August 30, 2017**

86 National Institute of Standards and Technology
87 Attn: Computer Security Division, Information Technology Laboratory
88 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
89 Email: checklists@nist.gov
90

91

92 All comments are subject to release under the Freedom of Information Act (FOIA).
93
94

95

Reports on Computer Systems Technology

96 The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology
97 (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's
98 measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of
99 concept implementations, and technical analyses to advance the development and productive use of
100 information technology. ITL's responsibilities include the development of management, administrative,
101 technical, and physical standards and guidelines for the cost-effective security and privacy of other than
102 national security-related information in federal information systems. The Special Publication 800-series
103 reports on ITL's research, guidelines, and outreach efforts in information system security, and its
104 collaborative activities with industry, government, and academic organizations.
105

106

Abstract

107 A security configuration checklist is a document that contains instructions or procedures for configuring
108 an information technology (IT) product to an operational environment, for verifying that the product has
109 been configured properly, and/or for identifying unauthorized changes to the product. Using these
110 checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks,
111 and identify changes that might otherwise go undetected. To facilitate development of checklists and to
112 make checklists more organized and usable, NIST established the National Checklist Program (NCP).
113 This publication explains how to use the NCP to find and retrieve checklists, and it also describes the
114 policies, procedures, and general requirements for participation in the NCP.

115

116

Keywords

117 change detection; checklist; information security; National Checklist Program (NCP); security
118 configuration checklist; Security Content Automation Protocol (SCAP); software configuration;
119 vulnerability

120

Acknowledgments

The authors, Stephen Quinn, Murugiah Souppaya, and Melanie Cook of the National Institute of Standards and Technology (NIST), and Karen Scarfone of Scarfone Cybersecurity wish to thank all individuals and organizations who have contributed to this revision of SP 800-70. Contributors include Harold Booth, Bob Byers, and David Waltermire of NIST; Harold Owen, Christopher Turner, and Chuck Wergin of CocoaSystems Inc.; and Tim Lusby and Dragos Prisaca of G2, Inc.

The authors acknowledge the following individuals and organizations that assisted in the development of earlier revisions of SP 800-70:

- Apple
- Booz Allen Hamilton: Paul Cichonski, Anthony Harris, and Paul M. Johnson
- Center for Internet Security (CIS): Clint Kreitner
- Centers for Disease Control and Prevention (CDC)
- Defense Information Systems Agency (DISA): Terry Sherald
- Department of Energy (DOE)
- G2, Inc.: Greg Witte
- Microsoft Corporation: Chase Carpenter, Kurt Dillard, and Jesper Johansson
- National Security Agency (NSA): Paul Bartock, Trent Pitsenbarger, and Neal Ziring
- NIST: John Banghart, Matt Barrett, Harold Booth, David Ferraiolo, Timothy Grance, Blair Heiserman, Jeffrey Horlick, Arnold Johnson, Suzanne Lightman, Mark Madsen, Edward Roback, Ron Ross, Michael Rubin, Carolyn Schmidt, Matt Scholl, and John Wack (co-author of the original version)
- Sun Microsystems: Glenn Brunette
- Symantec Corporation

NIST would also like to express appreciation and thanks to the Department of Homeland Security for its sponsorship and support of the NIST National Checklist Program for IT Products.

Audience

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

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

Note to Reviewers

In previous revisions of NIST SP 800-70, the contents of Appendix B and Appendix C have been duplicated in separate standalone files at <https://nvd.nist.gov/ncp/participation>. Section 5 of NIST SP 800-70 advises readers to check that website for the latest version of each file. To eliminate duplication of efforts, the authors are considering removing Appendix B and/or Appendix C from the final release of NIST SP 800-70 Revision 4 and only making them available as separate files on the website. The authors would especially appreciate any feedback on the advantages and disadvantages of making such a change.

166

Trademark Information

167 Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the
168 United States and other countries.

169 All other names are registered trademarks or trademarks of their respective companies.

170

171

172
173

Table of Contents

174 **Executive Summaryvii**

175 **1. Introduction 1**

176 1.1 Purpose and Scope 1

177 1.2 Document Organization 1

178 **2. The NIST National Checklist Program.....2**

179 2.1 Security Configuration Checklists2

180 2.2 Benefits of Using Security Checklists 3

181 2.3 Overview of NIST National Checklist Program4

182 2.4 Types of Checklists Listed by NCP4

183 **3. Operational Environments for Checklists 6**

184 3.1 Standalone Environment.....6

185 3.2 Managed Environment.....6

186 3.3 Specialized Security-Limited Functionality Custom Environment 7

187 3.4 Legacy Environments 7

188 3.5 United States Government Environment 8

189 **4. Checklist Usage9**

190 4.1 Determining Local Requirements..... 10

191 4.2 Browsing and Retrieving Checklists..... 10

192 4.3 Reviewing, Customizing and Documenting, and Testing Checklists 12

193 4.4 Applying Checklists to IT Products 13

194 4.5 Providing Feedback on Checklists..... 14

195 **5. Checklist Development..... 16**

196 5.1 Developer Steps for Creating, Testing, and Submitting Checklists 16

197 5.1.1 Initial Checklist Development16

198 5.1.2 Checklist Testing 17

199 5.1.3 Checklist Documented.....18

200 5.1.4 Checklist Submitted to NIST.....20

201 5.2 NIST Steps for Reviewing and Finalizing Checklists for Publication..... 20

202 5.2.1 NIST Screening of the Checklist Package.....21

203 5.2.2 Public Review and Feedback for the Candidate Checklist21

204 5.2.3 Final Listing on Checklist Repository.....21

205 5.2.4 Checklist Maintenance and Archival.....21

206 **Appendix A. References23**

207 **Appendix B. Checklist Program Operational Procedures.....24**

208 1. Overview and General Considerations 25

209 2. Checklist Submission and Screening.....26

210 3. Candidate Checklist Public Review 27

211 4. Final Checklist Listing 27

212 5. Final Checklist Update, Archival, and Delisting.....28

213 6. Record Keeping 28

214 **Appendix C. Participation and Logo Usage Agreement Form.....29**

215 **Appendix D. Additional Requirements for USGCB Baselines32**
216 D.1 Developer Steps for Creating, Testing, and Submitting USGCB Baselines 32
217 D.2 NIST Steps for Reviewing and Finalizing USGCB Baselines for Publication..... 35
218 D.3 Field Testing Report Template..... 35
219 **Appendix E. Acronyms and Abbreviations37**
220 **Appendix F. Glossary.....39**
221 **Appendix G. Change Log42**

222
223
224

List of Figures

225 Figure 1: Checklist User Process Overview.....9

226
227

List of Tables

229 Table 1: Checklist Description Form Fields 18

230
231
232

233 **Executive Summary**

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

238 Checklists can comprise templates or automated scripts, patch information, Extensible Markup Language
239 (XML) files, and other procedures. Checklists are intended to be tailored by each organization to meet its
240 particular security and operational requirements. Typically, checklists are created by IT vendors for their
241 own products; however, checklists are also created by other organizations, such as academia, consortia,
242 and government agencies. The use of well-written, standardized checklists can markedly reduce the
243 vulnerability exposure of IT products. Checklists can be particularly helpful to small organizations and to
244 individuals with limited resources for securing their systems.

245 NIST maintains the National Checklist Repository, which is a publicly available resource that contains
246 information on a variety of security configuration checklists for specific IT products or categories of IT
247 products. The repository, which is located at <https://checklists.nist.gov/>, contains information that
248 describes each checklist. The repository also hosts copies of some checklists, primarily those developed
249 by the federal government, and has links to the location of other checklists. Users can browse and search
250 the repository to locate a particular checklist using a variety of criteria. Having a centralized checklist
251 repository makes it easier for organizations to find the current, authoritative versions of security
252 checklists and to determine which ones best meet their needs.

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

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

259 **Organizations should apply checklists to operating systems and applications to reduce the number**
260 **of vulnerabilities that attackers can attempt to exploit and to lessen the impact of successful attacks.**

261 There is no checklist that can make a system or product 100 percent secure, and using checklists does not
262 eliminate the need for ongoing security maintenance, such as patch installation. However, using checklists
263 that emphasize both hardening of systems against software flaws (e.g., by applying patches and
264 eliminating unnecessary functionality) and configuring systems securely will typically reduce the number
265 of ways in which the systems can be attacked, resulting in greater levels of product security and
266 protection from future threats. Checklists can also be used to verify the configuration of some types of
267 security controls for system assessments, such as confirming compliance with certain Federal Information
268 Security Modernization Act (FISMA) requirements or other sets of security requirements.

269 Federal agencies are required to use appropriate security configuration checklists from the NCP when
270 available. In January 2017, Part 39 of the Federal Acquisition Regulation (FAR) was updated. Paragraph
271 (c) of section 39.101 states, “In acquiring information technology, agencies shall include the appropriate
272 information technology security policies and requirements, including use of common security
273 configurations available from the National Institute of Standards and Technology’s website at
274 <https://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure
275 the appropriate standards are incorporated.” [1] Also, FISMA requires each Federal agency to determine

276 minimally acceptable system configuration requirements and to ensure compliance with them [2].
277 Accordingly, Federal agencies, as well as vendors of products for the Federal government, should acquire
278 or implement and share such checklists using the NIST repository. NIST encourages checklist developers
279 to assert mappings to the security controls delineated in NIST Special Publication (SP) 800-53 to
280 facilitate FISMA compliance checking for Federal agencies.¹

281 Organizations should consider the availability of security configuration checklists during their IT product
282 selection processes.

283 **When selecting checklists, checklist users should carefully consider each checklist's degree of**
284 **automation, source, use of standards, and other relevant characteristics.**

285 NIST recognizes that some checklists are more automated and standards-based than others. For example,
286 non-automated checklists provide prose-based descriptions of how a person can manually alter a
287 product's configuration. Automated checklists are machine-readable. Automated checklists that fully
288 adhere to the Security Content Automation Protocol (SCAP), which are also known as SCAP content,
289 have all security settings documented in standardized SCAP formats; have undergone syntactic testing
290 using the NIST SCAP Content Validation Tool (SCAPVal)² for compliance to the SCAP-related
291 specifications; and include mappings between low-level security settings and high-level security
292 requirements.

293 When multiple checklists are available for a particular product, organizations should take into
294 consideration the degree of automation and use of standards of each checklist. Generally, SCAP
295 checklists can be used more consistently and efficiently than others. There may be other significant
296 differences among checklists; for example, one checklist may include software bundled with an operating
297 system (e.g., web browser and email client) while another checklist addresses that operating system only.
298 Another example is the assumptions on which the checklists are based (e.g., operational environment). A
299 checklist user should identify such differences and determine which checklist(s) seem appropriate and
300 merit further analysis.

301 Checklist source is particularly important for users from Federal civilian agencies, who should first search
302 for government-authorized or mandated checklists (e.g., mandated by Part 39 of the FAR [1]). In general,
303 these users should search for NIST-produced checklists, which are tailored for civilian agency use. If no
304 NIST-produced checklist is available, then agency-produced checklists from the Defense Information
305 Systems Agency (DISA) or the National Security Agency (NSA) should be used if available. If formal
306 government-authorized checklists do not exist, organizations are encouraged to use vendor-produced
307 checklists. If vendor-produced checklists are not available, other checklists that are posted on the NCP
308 website may be used.

309 **Checklist users should customize and test checklists before applying them to production systems.**

310 A checklist that is not mandatory for an organization to adopt should be considered a starting point for an
311 organization to customize. Although the settings are based on sound knowledge of security threats and
312 vulnerabilities, they cannot take into account organization-specific security and operational requirements,
313 existing security controls, and other factors that may necessitate changes. Organizations should carefully
314 evaluate the checklist settings and give them considerable weight, then make any changes necessary to
315 adapt the settings to the organization's environment, requirements, policies, and security objectives. This

¹ Organizations are also encouraged to include information in their checklists that supports mapping to other sets of requirements, such as HIPAA.

² SCAPVal is available for download for each SCAP version on the SCAP specification website at <https://scap.nist.gov/revision/index.html>.

316 is particularly true for checklists intended for an environment with significantly different security needs.
317 All deviations from the checklist settings should be documented for future reference, and include the
318 reason behind each deviation and the impact of deviating from the setting.

319 Before applying a checklist that will be used to alter product settings, users should first test it on non-
320 critical systems, preferably in a controlled non-operational environment. Each checklist in the NIST
321 repository has been tested by its developer, but there are often significant differences between a
322 developer's testing environment and an organization's operational environment, and some of these
323 differences may affect checklist deployment. In some cases, a security control modification can have a
324 negative impact on a product's functionality and usability, or on other products or security controls.
325 Consequently, it is important to perform testing to determine the impact on system security, functionality,
326 and usability; to document the results of testing; and to take appropriate steps to address any significant
327 issues.

328 **Checklist users should take their operational environments into account when selecting checklists,**
329 **and checklist developers should target their checklists to one or more operational environments.**

330 Checklists are significantly more useful when they can run in common operational environments. The
331 NCP has identified several broad and specialized operational environments, such as Standalone and
332 Managed, and at least one of the environments should be common to most of the audiences. Thoroughly
333 identifying and describing these environments will make it easier for users to select the security checklists
334 that are most appropriate for their particular operating environments, and will allow developers to better
335 target their checklists to the general security characteristics associated with their operating environments.

336 **NIST strongly encourages IT product vendors to develop security configuration checklists for their**
337 **products and contribute them to the NIST National Checklist Repository.**

338 NIST encourages IT product vendors to develop security configuration checklists for their products, since
339 the vendors have the most expertise on the possible security configuration settings and the best
340 understanding of how the settings relate to and affect each other.

341 Vendors that create security configuration checklists should submit them for inclusion in the National
342 Checklist Repository through the NCP. The NCP provides a process and guidance for developing
343 checklists in a consistent fashion. For checklist developers, steps include initial development of the
344 checklist, checklist testing, documenting the checklist according to the guidelines of the NCP, and
345 submitting a checklist package to NIST. NIST screens the checklist according to program requirements
346 and then releases the checklist for public review, which lasts 30 days. After the public review period and
347 subsequent resolution of issues, the checklist is listed on the NIST checklist repository with its
348 information. Checklist maintenance may potentially be performed by the vendor, resulting in the release
349 of updated checklists. NIST retires or archives checklists as they become outdated or incorrect.

350

351 **1. Introduction**

352 **1.1 Purpose and Scope**

353 This document describes the use, benefits, and management of checklists, and explains how to use the
354 NIST National Checklist Program (NCP) to find and retrieve checklists. The document also describes the
355 policies, procedures, and general requirements for participation in the NCP.

356 **1.2 Document Organization**

357 Section 2 contains an overview of checklists and describes the advantages of the NIST NCP and how it
358 works.

359 Section 3 provides additional details on pre-defined checklist operational environments that are used in
360 the NCP to help developers create checklists that are consistent with security practices. The material
361 presented in Section 3 can also help checklist users select the checklists that best match their own
362 operational environments.

363 Section 4 contains information for potential checklist users. It describes how to use the NCP to find and
364 retrieve checklists that best match the identified needs. It also contains guidance on how to implement
365 checklists, including how to analyze the specific operating environment and then tailor checklists as
366 applicable.

367 Section 5 provides guidance for current and prospective checklist developers. This guidance contains
368 information on the procedures for preparing and submitting a checklist to NIST for inclusion in the
369 checklist repository.

370 Appendix A lists references for this document.

371 Appendix B contains the programmatic and legal requirements that must be satisfied to participate in the
372 NCP.

373 Appendix C contains the NCP participation and logo usage agreement form.

374 Appendix D details additional requirements that United States Government Configuration Baseline
375 (USGCB) checklists must meet.

376 Appendix E contains a list of acronyms used in this document.

377 Appendix F presents a glossary of the terms used in this document.

378 Appendix G provides the change log for the most recent release of the document.

2. The NIST National Checklist Program

380 There are many threats to users' computers, and new vulnerabilities in IT products (e.g., operating
381 systems and applications) are discovered daily. Patches may not be immediately available for new
382 vulnerabilities, causing the need to rapidly deploy temporary mitigation through reconfiguration until
383 patches are available. Also, because IT products often are intended for a wide variety of audiences,
384 restrictive security settings are usually not enabled by default, which means that many IT products are
385 immediately vulnerable in their default configuration. It is a complicated, arduous, and time-consuming
386 task even for experienced system administrators to know what a reasonable set of security settings is for
387 many different IT products.

388
389 Although the solutions to IT security are complex, one simple yet effective tool is the security
390 configuration checklist. To facilitate development of security configuration checklists and to meet the
391 requirements of the Cyber Security Research and Development Act of 2002 (Public Law 107-305)
392 (CSRDA) [3], NIST developed the National Checklist Program (NCP) for IT Products. This section
393 contains an overview of the NCP. It begins by describing the contents of checklists and giving examples
394 of the types of IT products for which checklists are often created. It next explains the benefits of using
395 security configuration checklists, such as improving the base level of security for an organization. It also
396 explains the goals and benefits of the NCP, which include increasing the quality, usability, and
397 availability of checklists.

2.1 Security Configuration Checklists

400 A *security configuration checklist* (also referred to as a lockdown guide, hardening guide, security guide,
401 security technical implementation guide [STIG], or benchmark)³ is essentially a document that contains
402 instructions or procedures for configuring an IT product to an operational environment, for verifying that
403 the product has been configured properly, and/or for identifying unauthorized configuration changes to
404 the product. The IT product may be commercial, open source, government-off-the-shelf (GOTS), etc.

405
406 Using well-written, standardized configuration checklists can reduce the vulnerability exposure of IT
407 products and be particularly helpful to small organizations and individuals in securing their systems.
408 Checklists can be developed not only by IT vendors, but also by other organizations with technical
409 competence in IT product security. A security configuration checklist might include any of the following:

- 410
411 ■ Configuration files that automatically set or verify various security-related settings (e.g., executables,
412 security templates that modify settings, Security Content Automation Protocol (SCAP) XML
413 (Extensible Markup Language) files, and scripts).⁴
- 414 ■ Documentation (e.g., text file) that guides the checklist user to manually configure an IT product
- 415 ■ Documents that explain the recommended methods to securely install and configure a device
- 416 ■ Policy and programmatic documents that set forth guidelines for such things as auditing,
417 authentication mechanisms (e.g., passwords), and perimeter security.

³ From this point on in this document, the term *checklist* (used according to CSRDA terminology) is used to describe a security configuration checklist.

⁴ More information about SCAP can be found at <https://scap.nist.gov/> and all versions of NIST Special Publication (SP) 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP)* [4].

418 Not all instructions in a security configuration checklist need to strictly address security settings.
419 Checklists can also include specialized security functions, such as looking for artifacts of an attack on a
420 host, or administrative practices such as enabling energy saving features.

421
422 Typically, a system administrator or end user follows the instructions in the checklist to configure a
423 product or system to the level of security implemented in the checklist, or to verify that a product or
424 system is already configured properly. The system administrator may need to modify the checklist to
425 incorporate the local security policy.

426
427 Examples of the types of devices and software for which security checklists are intended are as follows:

- 428
429 ■ General-purpose operating systems and mobile operating systems
- 430
431 ■ Common applications such as email clients, web browsers, word processors, personal firewalls, and
antivirus software
- 432
433 ■ Infrastructure devices such as routers, firewalls, virtual private network (VPN) gateways, intrusion
detection systems (IDS), wireless access points, and telecommunication systems
- 434
435 ■ Application servers such as Domain Name System (DNS), Dynamic Host Configuration Protocol
(DHCP), web, Simple Mail Transfer Protocol (SMTP), and database servers
- 436
437 ■ Other network devices such as scanners, printers, and copiers.

437 **2.2 Benefits of Using Security Checklists**

438 Security checklists, when developed correctly, can help users configure IT products so that they have
439 more protection than the defaults provide. Applying checklists to operating systems and applications can
440 reduce the number of vulnerabilities that attackers can attempt to exploit and lessen the impact of
441 successful attacks. Using checklists improves the consistency and predictability of system security,
442 particularly in conjunction with user training and awareness activities and other supporting security
443 controls. Additional benefits associated with using checklists include the following:

- 444
445 ■ Provides a base level of security to protect against common and dangerous local and remote threats
446 (e.g., malware, denial-of-service attacks, unauthorized access, and inappropriate usage)
- 447
448 ■ Verifies the configuration of certain technical security controls for system assessments, such as
449 confirming compliance with certain Federal Information Security Modernization Act (FISMA)
450 requirements or other sets of requirements, and understanding the exposure caused by
misconfigurations
- 451
452 ■ Significantly reduces the time required to research and develop appropriate security configurations
for installed IT products
- 453
454 ■ Allows smaller organizations to leverage outside resources to implement recommended practice
security configurations
- 455
456 ■ Reduces the likelihood of public loss of confidence or embarrassment resulting from a compromise of
systems (for example, a major breach of personally identifiable information (PII)).

457 Although using security checklists for security compliance purposes can significantly improve overall
458 levels of security in organizations, using a checklist cannot make a system or a product 100 percent
459 secure. However, using checklists that emphasize hardening of systems against the hidden software flaws
460 will typically result in greater levels of product security and protection from future threats (e.g., zero-day

461 vulnerabilities). IT vendors that configure their products using checklists that adhere to the FISMA-
 462 associated security control requirements will provide more consistency in configuration settings within
 463 the federal agencies. This configuration will also provide a much more cost-effective method for
 464 establishing and verifying the minimum configuration settings, even if the agencies must modify the
 465 checklists to fine-tune the configuration settings for their specific applications and operational
 466 environments.

467

468 **2.3 Overview of NIST National Checklist Program**

469 Many organizations have created checklists; however, these checklists vary widely in terms of quality and
 470 usability, and they may become outdated as software updates and upgrades are released. Without a central
 471 checklist repository, finding security checklists can be difficult. In addition, checklists may differ
 472 significantly from one another in terms of the purpose of the checklist or the level of security provided.
 473 Also, it may be difficult to determine if the checklist is current or how the checklist should be
 474 implemented.

475

476 To facilitate development of security checklists for IT products and to make checklists more organized
 477 and usable, NIST established the NCP. The goals of the NCP are to—

478

479 ■ Facilitate development and sharing of checklists by providing a formal framework for vendors and
 480 other checklist developers to submit checklists to NIST

481 ■ Provide guidance to developers to help them create standardized, high-quality checklists that conform
 482 to common operational environments

483 ■ Help developers and users by providing guidelines for making checklists better documented and more
 484 usable

485 ■ Encourage software vendors and other parties to develop checklists

486 ■ Provide a managed process for the review, update, and maintenance of checklists

487 ■ Provide an easy-to-use repository of checklist information

488 ■ Provide checklist content in a standardized format

489 ■ Encourage the use of automation technologies for applying checklists.

490 Federal agencies are required to use appropriate security configuration checklists from the NCP when
 491 available. In January 2017, Part 39 of the Federal Acquisition Regulation (FAR) was updated. Paragraph
 492 (c) of section 39.101 states, “In acquiring information technology, agencies shall include the appropriate
 493 information technology security policies and requirements, including use of common security
 494 configurations available from the National Institute of Standards and Technology’s website at
 495 <https://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure
 496 the appropriate standards are incorporated.” [1]

497 **2.4 Types of Checklists Listed by NCP**

498 The NCP deals with checklists that are tied to *specific* IT products, such as a checklist for a specific brand
 499 and model of a router. Some checklists may guide a user to other checklists. For example, a checklist for a
 500 database product may reference the checklist for the operating system on which the database product runs.
 501 The NCP includes two major groups of checklists:
 502

503 ■ **Automated.** An automated checklist is one that is used through one or more tools that automatically
504 alter or verify settings based on the contents of the checklist. Many checklists are written in
505 Extensible Markup Language (XML), and there are special tools that can use the contents of the XML
506 files to check and alter system settings.⁵ For example, the Security Content Automation Protocol
507 (SCAP) is commonly used to express checklist content in a standardized way that can be processed
508 by tools that support SCAP.⁶

509 ■ **Non-Automated.** As the name implies, a non-automated checklist is one that is designed to be used
510 manually, such as English prose instructions that describe the steps an administrator should take to
511 secure a system or to verify its security settings.

512 Security configuration checklists in the NCP can help organizations meet FISMA requirements. FISMA
513 requires each agency to determine minimally acceptable system configuration requirements and to ensure
514 compliance with them. Checklists can also map specific technical control settings to the corresponding
515 NIST Special Publication (SP) 800-53 controls, which can make the verification of compliance more
516 consistent and efficient. Accordingly, federal agencies, as well as vendors of products for the federal
517 government, are encouraged to acquire or develop and to share such checklists using the NIST repository.
518 The development and sharing of checklists can reduce what would otherwise be a “reinvention of the
519 wheel” for IT products that are widely used in the federal government, such as common operating
520 systems, servers, and client applications.

521 The NIST checklist repository (located at <https://checklists.nist.gov/>) contains information on automated
522 and non-automated checklists that have been developed and screened to meet the requirements of the
523 NCP. The repository also hosts copies of some checklists, primarily those developed by the federal
524 government, and has pointers to the other checklists’ locations. Users can browse checklist descriptions to
525 locate and retrieve a particular checklist using a variety of different fields. A mailing list for the checklist
526 program is available at <https://nvd.nist.gov/general/email-list>.
527

⁵ The Extensible Checklist Configuration Description Format (XCCDF) is an XML-based format for automating tool usage and eliminating interpretation issues. The XCCDF XML format can be used for both technical checklists (e.g., operating systems, software applications, and hardware configurations) and non-technical checklists (e.g., physical security for IT systems). More information on XCCDF is available from NIST Interagency Report (IR) 7275 Revision 4, *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2*, which is available for download at <https://doi.org/10.6028/NIST.IR.7275r4>. Another XML-based format for checklists is the Open Vulnerability and Assessment Language (OVAL), which is used to exchange technical details about how to check for the presence of vulnerabilities and configuration issues on systems. More information on OVAL is available at <https://oval.cisecurity.org>.

⁶ For more information on the validation of products’ SCAP support and a list of SCAP-validated products, see <https://scap.nist.gov/validation/index.html>.

3. Operational Environments for Checklists

529 To ensure that as many users as possible receive value from checklists, it is recommended that checklist
530 authors create checklists for a broad operational environment unless there is a compelling reason to focus
531 on a specialized operational environment. The NCP identifies several broad and specialized operational
532 environments, at least one of which should be common to most audiences. Identifying and describing
533 these environments allows developers to better target their checklists to the general security requirements
534 associated with the environments, and allows end users to more easily select the checklists that are most
535 appropriate for their environments.

536
537 This section describes the operational environments defined for the NCP, and the general threat
538 description and fundamental technical security practice for each environment. The two broad operational
539 environments are referred to as **Standalone** (or Small Office/Home Office [SOHO]) and **Managed** (or
540 Enterprise). Three typical **Custom** environments, which could be subsets of the broader environments, are
541 **Specialized Security-Limited Functionality (SSLF)**, **Legacy**, and **United States Government**.

542
543 Users of IT products may find it useful to consult this section of the document when initially identifying
544 their own security requirements and needs (outlined in detail in Section 4). Developers may find this
545 section useful when building checklists because tailoring checklist development to these environments
546 and their policies will enable developers to create security compliance checklists for diverse products but
547 still adhere to the general uniform technical security practices and settings associated with the
548 environments. This is discussed in detail in Section 5. Before submitting a checklist to NIST, developers
549 should ensure they have the most recent version of this document because updates to the criteria for
550 operational environments may occur periodically. The most recent version is available as a separate file at
551 <https://checklists.nist.gov/>.⁷

3.1 Standalone Environment

554 The **Standalone** environment describes individually managed devices (e.g., desktops, laptops,
555 smartphones, tablets), as opposed to Managed environments (see Section 3.2), which are based on
556 centrally managed devices (i.e., many devices managed by a single organization). Standalone
557 environments are typically the least secured. The individuals who perform system administrator duties on
558 Standalone systems are assumed to be less knowledgeable about security than average administrators,
559 which often results in environments that are less secure than they should be because the focus is on
560 functionality. Accordingly, Standalone checklists should be relatively simple to understand and
561 implement by home users or novice system administrators.

3.2 Managed Environment

564 The **Managed** environment, also referred to as **Enterprise**, comprises centrally managed IT products,
565 everything ranging from servers and printers to desktops, laptops, smartphones, and tablets. Managed
566 checklists are intended for advanced end users and system administrators. The managed nature of typical
567 Managed environments gives administrators centralized control over various settings on devices.
568 Authentication, account, and policy management can also be administered centrally to maintain a
569 consistent security posture across an organization.

570

⁷ NIST may, as new information becomes available, update the criteria and information for the operational environments as well as other criteria contained in this document.

571 The Managed environment is more restrictive and provides less functionality than the Standalone
572 environment. However, because of the supported and controlled⁸ nature of the Managed environment, it
573 is typically easier to use more functionally restrictive settings in Managed environments than in
574 Standalone environments. Managed environments also tend to implement several layers of defense (e.g.,
575 firewalls, antivirus servers, IDSs, patch management systems, and email filtering), which provides greater
576 protection for systems.

577

578 **3.3 Specialized Security-Limited Functionality Custom Environment**

579 A **Custom** environment contains systems in which the functionality and degree of security do not fit the
580 other types of environments. **Specialized Security-Limited Functionality (SSLF)** is a typical Custom
581 environment that is highly restrictive and secure; it is usually reserved for systems that have the highest
582 threats and associated impacts. Typical examples of such systems are outward-facing web, email, and
583 DNS servers, other publicly accessed systems, and firewalls. It also encompasses computers that contain
584 confidential information (e.g., central repository of personnel records, medical records, and financial
585 information) or that perform vital organizational functions (e.g., accounting, payroll processing, and air
586 traffic control). These systems might be targeted by third parties for exploitation, but also might be
587 targeted by trusted parties inside the organization. Because systems in an SSLF environment are at high
588 risk of attack or data exposure, security takes precedence over functionality. The systems' data content or
589 mission purpose is of such value that aggressive tradeoffs in favor of security outweigh the potential
590 negative consequences to other useful system attributes such as legacy applications or interoperability
591 with other systems.

592

593 An SSLF environment could be a subset of another environment. For example, three desktops in a
594 Managed environment that hold the organization's confidential employee data could be thought of as an
595 SSLF environment within a Managed environment. In addition, a laptop used by a mobile worker (e.g.,
596 organization management) might be an SSLF environment in a Standalone environment. An SSLF
597 environment might also be a self-contained environment outside any other environment, such as a
598 government security installation processing sensitive data.

599

600 SSLF checklists are intended for experienced security specialists and seasoned system administrators who
601 understand the impact of implementing strict technical security practices. If home users and other users
602 who do not have security expertise attempt to apply SSLF checklists to their systems, they typically
603 experience unwanted limitations on system functionality and cause possibly irreparable system damage.

604

605 **3.4 Legacy Environments**

606 A Legacy environment is another example of a Custom environment. A Legacy environment contains
607 older systems or applications that may need to be secured to meet today's threats, but they often use older,
608 less secure communication mechanisms and need to be able to communicate with other systems. Non-
609 legacy systems operating in a Legacy environment may need less restrictive security settings so that they
610 can communicate with legacy systems and applications. Legacy environments are often subsets of other
611 environments.

612

⁸ This is not meant to imply that checklists should not be customized within Managed environments. For example, it may be prudent to make exceptions for groups of users with a specific need to deviate from a particular checklist setting, rather than either have the entire enterprise deviate from the setting because of the needs of a subset of users, or prevent the subset of users from performing their duties.

613 3.5 United States Government Environment

614 A United States Government environment is another example of a Custom environment. This
615 environment contains federal government systems. These systems need to be secured according to
616 prescribed configurations as mandated by policy. For example, the Federal Desktop Core Configuration
617 (FDCC) is a security configuration policy mandated by the Office of Management and Budget (OMB).
618 The original checklists developed in support of the FDCC policy exist for multiple versions of Microsoft
619 Windows, Windows Firewall, and Internet Explorer. These checklists are broader than previous
620 checklists, incorporating settings for Web browsers, personal firewalls, and other software. The
621 configuration settings also include non security-related settings aimed at improving performance, energy
622 efficiency, compatibility, and interoperability. The settings are largely based on the configuration settings
623 recommended by Microsoft in its security guides, but they have been customized to take into account
624 federal government security requirements. Many federal systems have been required to use these
625 checklists by OMB's FDCC mandate.

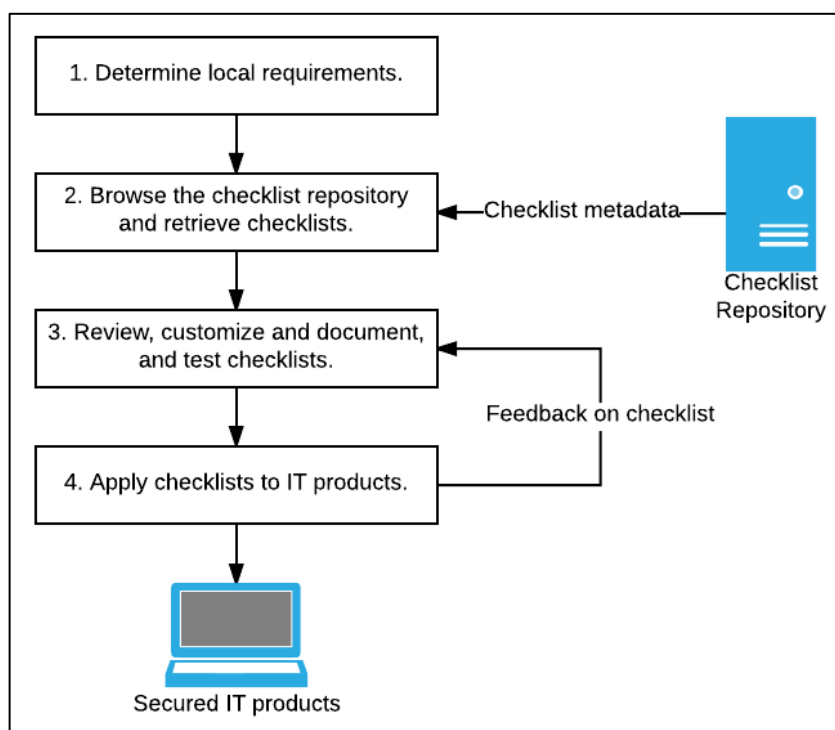
626
627 Since that time, the US government has focused on developing a new set of security configuration
628 checklists to augment the existing checklists in support of the FDCC policy. These new checklists are
629 known as the United States Government Configuration Baseline (USGCB). Like the original checklists,
630 the USGCB checklists also support the FDCC policy, and the USGCB checklists address a wide variety
631 of security and non-security settings that are largely based on settings recommended by product vendors
632 but customized to meet federal requirements. The USGCB initiative was created in 2010 by the
633 Technology Infrastructure Subcommittee (TIS) of the CIO Council Architecture and Infrastructure
634 Committee (AIC) as an evolution of the FDCC policy. The USGCB checklists are referred to as
635 "baselines" because they define minimum sets of configurations that must be implemented. New USGCB
636 baselines were released to replace the original FDCC checklists (Windows XP, Windows Vista, and
637 Internet Explorer 7), and the original FDCC checklists were deprecated at that time. USGCB checklists
638 have also been created for other platforms, namely Red Hat Enterprise Linux Desktop.

639
640 The USGCB configuration settings are intended to be deployed primarily to managed systems. The
641 original checklists in support of the FDCC policy and USGCB baselines are intended to be applied to
642 systems primarily through automated tools. Organizations should thoroughly test all checklists and
643 baselines before deploying them in operational environments because a number of their settings, such as
644 cryptographic algorithm options and wireless services, may impact system functionality. After
645 deployment, settings may also be checked through automated means for compliance with checklists and
646 baselines.

647

648 4. Checklist Usage

649 This section describes a high-level process for checklist users to follow when retrieving and using
 650 checklists. Although all checklist users, ranging from home users to system administrators, have their
 651 own specific requirements, the process described will apply to most situations. This section includes
 652 guidance on conducting an initial analysis of local environment threats and risks, and lists the potential
 653 impacts of such attacks. It then describes a process for selecting and retrieving checklists through the
 654 NIST checklist repository, and recommends steps for analyzing, tailoring, and applying the checklist.



655 **Figure 1: Checklist User Process Overview**

656 Figure 1 shows the general process for using checklists. The general steps involved in acquiring and using
 657 checklists are simple and straightforward—

- 658 1. Users gather their local requirements (e.g., IT products, the operating environment, and
 659 associated security needs) and then acquire or purchase the IT product that best suits their needs.
 660
- 661 2. Users browse the checklist repository to retrieve checklists that match the user's operational
 662 environment and security requirements. If a product is intended to be secure by default, it is still
 663 important to check the NIST checklist repository for updates to that checklist.
- 664 3. Users review the checklists and select the checklist that best meets their requirements, then tailor
 665 and document the checklist as necessary to take into account local policies and functional
 666 requirements, test the checklist, and provide feedback to NIST and checklist developers.
- 667 4. Users prepare to deploy the checklist, such as making configuration or data backups, and then
 668 apply the checklist in production.

669 The following sections describe the details of the activities included in each of these steps.

670

671 4.1 Determining Local Requirements

672 Organizations usually conduct a requirements analysis before actually selecting and purchasing a
673 particular IT product. Such an analysis would include identifying the needs of the organization (what the
674 product must do) and the security requirements for the product (e.g., relevant security policies). Individual
675 end users can conduct the same process, although it could be quite informal. Because it is difficult to add
676 security later, it is best to assess requirements upfront when incorporating security into IT operations, big
677 or small.

678
679 When planning security, it is essential to first define the threats that must be mitigated. Organizations that
680 use checklists should conduct risk assessments to identify the specific threats against their systems and
681 determine the effectiveness of existing security controls in counteracting the threats; they then should
682 perform risk mitigation to decide what additional measures (if any) should be implemented, as discussed
683 in NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal*
684 *Information Systems: A Security Life Cycle Approach* [6]. Performing risk assessments and mitigation
685 helps organizations better understand their needs and decide whether or not they need to modify or
686 enhance selected checklists.

687
688 The risk mitigation methodology includes steps that are straightforward and simple, even for an
689 individual home user who may not be especially savvy with regard to IT security. Important steps include
690 the following:

691
692 ■ **Identify Functional Needs.** What must the product do? Identifying upfront the end user's
693 requirements, such as remote access for telecommuters or a web server to make internal information
694 available to employees, is necessary to ensure that the security controls selected are appropriate; that
695 is, that they implement an appropriate security solution and still allow the system to meet its
696 requirements for functionality.

697 ■ **Identify Threats and Vulnerabilities.** A threat is the potential for a particular threat-source to
698 successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally
699 triggered or intentionally exploited. The goal of this step is to identify potential threat-sources that are
700 applicable to the IT product or system being considered, as well as the vulnerabilities that could be
701 exploited by the potential threat-sources.

702 ■ **Identify Security Needs.** The goal of this step is to determine the controls needed to minimize or
703 eliminate the likelihood (or probability) of a threat exercising a product or system vulnerability. It
704 answers the question, "What security features must the product provide?" Armed with this
705 information, the organization can make wiser choices about which IT product best meets its needs.

706 NIST has also written several documents and guides to help federal agencies when selecting information
707 security products and when acquiring and using tested/evaluated products. Another key resource available
708 at NIST for identifying vulnerability-related information about IT products is the National Vulnerability
709 Database (NVD).⁹ This website provides a search engine for identified system vulnerabilities and
710 information on patches that are available to correct the vulnerabilities.

711 4.2 Browsing and Retrieving Checklists

713 After determining local requirements and identifying an IT product, a checklist user is ready to browse
714 the NIST checklist repository. To help users obtain checklists that can be processed by SCAP-validated
715 products, the checklists are categorized by content type (degree of automation and standardization) and

⁹ <https://nvd.nist.gov/>

716 authority (the organization responsible for producing the original security configuration guidance
 717 represented by the checklist). Users can browse the checklists based on the content type, IT product, or
 718 authority and through a keyword search that searches the checklist name and summary for user-specified
 719 terms. The search results show the detailed checklist information and a link to any SCAP content for the
 720 checklist, as well as links to any supporting resources associated with the checklist. Selecting a particular
 721 checklist will show a description template that includes extensive information to help users decide
 722 whether the checklist will suit their specific purposes. Depending on a user's needs, role, and skills (e.g.,
 723 home user versus enterprise administrator), some fields in the description will be more important than
 724 others.

725
 726 Some checklists address more than one application or operating system, such as several products from a
 727 single organization. To help users navigate the site from the checklist detail page, a Checklist Group link
 728 is available; it represents the grouping of checklists based on a common source material. For example, the
 729 DISA (Defense Information Systems Agency) Desktop Checklist contains configuration settings for
 730 multiple products including browsers and antivirus products. The NCP decomposes the checklist
 731 information according to these individual targets, but keeps them conveniently linked to the same source
 732 document via the Checklist Group.

733 In some cases, multiple checklists are available for a particular version of a product. Such checklists are
 734 often similar, but they have important differences, such as the degree of automation provided, the
 735 intended audience (e.g., providing general recommendations versus complying with Federal agency-
 736 specific requirements), and the checklist purpose (reconfiguring a product versus identifying a successful
 737 compromise of the product). To assist checklist users in being able to readily identify the major
 738 differences among checklists, NIST categorized checklists by content type, such as:

739 ■ **Prose.** Prose checklists provide narrative descriptions of how a person can manually alter a product's
 740 configuration.

741 ■ **Automated.** Automated checklists document their security settings in a machine-readable format,
 742 either standard or proprietary. An example is a product-specific configuration script. These checklists
 743 may include some elements of SCAP (for example, they may contain CCE [Common Configuration
 744 Enumeration] identifiers), but do not fully adhere to the SCAP specification.

745 ■ **SCAP Content.** SCAP content checklists adhere to the SCAP specification in NIST SP 800-126 for
 746 documenting security settings in machine-readable standardized SCAP formats. SCAP content
 747 checklists can be processed by SCAP-validated products, which have been validated by an accredited
 748 independent testing laboratory as conforming to applicable SCAP specifications and requirements.
 749 SCAP content that is available on the National Checklist Program repository has been evaluated with
 750 the NIST SCAP Content Validation Tool (SCAPVal)¹⁰. This evaluation ensures the checklist
 751 conforms to the SCAP specification. The SCAPVal tool does not evaluate the checklist for logic
 752 errors such as use of an "equal to" operator when "equal to or greater than" should have been used.

753 Some SCAP content checklists have been vetted with at least one governance organization authority.
 754 These SCAP checklists are known to run on SCAP-enabled tools and include low-level security
 755 setting mappings (for example, standardized identifiers for individual security configuration issues)
 756 that can be externally mapped to high-level security requirements as represented in various security
 757 frameworks (e.g., SP 800-53 controls for FISMA). The USGCB checklists described in Section 3.5
 758 are examples of vetted SCAP content checklists.

¹⁰ 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].

759 When multiple checklists are available for a particular product, organizations should take into
760 consideration the degree of automation and use of standards of each checklist. Generally, SCAP-
761 expressed checklists can be used more consistently and efficiently than others. There may be other
762 significant differences among checklists; for example, one checklist may include software bundled with
763 an operating system (e.g., web browser and email client) while another checklist addresses that operating
764 system only. Another example is the assumptions on which the checklists are based (e.g., operational
765 environment). A checklist user should identify such differences and determine which checklist(s) seem
766 appropriate and merit further analysis.

767 Checklist source is particularly important for users from Federal civilian agencies, who should first search
768 for government-authorized or mandated checklists. In general, these users should search for NIST-
769 produced checklists, which are tailored for civilian agency use. If no NIST-produced checklist is
770 available, then agency-produced checklists from the Defense Information Systems Agency (DISA) or the
771 National Security Agency (NSA) should be used if available. If formal government-authorized checklists
772 do not exist, organizations are encouraged to use vendor-produced checklists. If vendor-produced
773 checklists are not available, other checklists that are posted on the NCP website may be used.

774 Organizations often submit checklists with associated alphanumeric version identifiers (e.g., R1.2.0).
775 Unfortunately, these identifiers do not have universal meanings. Some organizations may change the
776 version number when new checks are added, old technology is deleted, patches are added, or simply
777 based on a review date. Conversely, other organizations may update their checklist and not change the
778 version numbers. To clarify updates to checklists, NCP uses the concept of a “Checklist Revision.” A
779 Checklist Revision indicates that something has changed even if the version identifier did not change.
780 For example, if the organization does not change the version number on the document, but the content has
781 been updated (e.g., patches were added for a given month), the current checklist will be listed as archived
782 and the checklist with the updated patch content will show as the current checklist. Likewise, if the
783 submitting organization updates the version identifier, then the NCP will list the current checklist as
784 archived and link to the new checklist. From the checklist detail page, a user can navigate to the checklist
785 history via the “Archived Revisions” link.

786

787 **4.3 Reviewing, Customizing and Documenting, and Testing Checklists**

788 Checklist users should download all documentation for the checklist and review it carefully. The
789 documentation should explain any required preparatory activities, such as backing up a system. Because a
790 checklist may not exactly match a user’s specific requirements, reviewing a checklist is useful in
791 determining whether the checklist may need to be tailored¹¹ and whether the system or product will
792 require further changes after applying the checklist.

793 The user’s review can identify the impact on an organization’s current policies and practices if a given
794 security checklist is used. An organization may determine that some aspects of the checklist do not
795 conform to certain organization-specific security and operational needs and requirements. Organizations
796 should carefully evaluate the checklist settings and give them considerable weight, then make any
797 changes necessary to adapt the settings to the organization’s environment, requirements, policies, and
798 security objectives.¹² This is particularly true for checklists intended for an environment with significantly
799 different security needs. Organizations should tailor the checklists to reflect local rules, regulations, and
800 mandates; for example, federal civilian agencies would need to ensure that checklists reflect compliance
801 with Federal Information Processing Standard (FIPS) 140 encryption requirements. Because the checklist

¹¹ If multiple checklists are available for the same product, the checklist user may wish to compare the settings or steps in the selected checklist to the other checklists to see which settings or steps differ and determine if any of these alternate recommendations should be used.

¹² This may not be applicable to checklists that are mandatory for an organization to adopt.

802 may be used many times within the organization, the checklist itself might need to be modified. This is
803 especially likely if the checklist includes a script or template to be applied to systems.

804 At this point, all deviations from the settings in the checklist should be documented for future reference.
805 The documentation should include the reason behind each deviation, including the impact of retaining the
806 setting and the impact of deviating from the setting. This documentation helps in managing changes to the
807 checklist over the life cycle of the product being secured. Feedback on the checklist can be sent to NIST
808 as well as to the checklist developers. Feedback is especially important to developers in gauging whether
809 the checklist is well written and the settings are applicable to the targeted environment.

810 Before applying a checklist that will be used to alter product settings, users should first test it on non-
811 critical systems, preferably in a controlled non-operational environment. Such testing may be difficult for
812 home or small business users who do not have extra systems and networks for testing purposes. Each
813 checklist in the NIST checklist repository has been tested by its developer, but there are often significant
814 differences between a developer's testing environment and an organization's operational environment,
815 and some of these differences may affect checklist deployment. The testing configuration of the IT
816 product should match the deployment configuration. In some cases, a security control modification can
817 have a negative impact on a product's functionality and usability, or on other products or security
818 controls. For example, installing a patch could inadvertently break another patch, or enabling a firewall
819 could inadvertently block antivirus software from updating its signatures or disrupt patch management
820 software. Consequently, it is important to perform testing to determine the impact on system security,
821 functionality, and usability; to document the results of testing; and to take appropriate steps to address any
822 significant issues. Section 4.4 contains recommendations for performing backups and other suggestions to
823 prevent or recover from potential damage or unwanted effects that could occur if applying an untested
824 checklist.

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

831 **4.4 Applying Checklists to IT Products**

832 A checklist can be applied to an IT product in one of two ways: modifying the product's settings or
833 verifying the existing settings. The following provides recommendations for both ways of applying
834 checklists:

835 ■ Setting Modification

837 – Even after reviewing and testing a checklist, users should handle deployment carefully to
838 minimize any issues that might arise from applying the checklist.

839 – For users who are unable to test a checklist in a non-operational environment (e.g., home users), it
840 is important to carefully review the checklist documentation completely and to determine if an
841 initial backup is required. The *Rollback Capability* field in the checklist description will indicate
842 whether the results of applying the checklist can be reversed to return the product to its original
843 configuration. Regardless of this setting, it is strongly recommended that a user back up the IT
844 product's configuration before installing the checklist recommendations.

845 – At a minimum, users should back up all critical data files in their computing environment. If
846 possible, the user should make a full backup of the system to ensure that the system can be
847 restored to its pre-checklist state if necessary. (Making a full backup is recommended before
848 making any major system change; it does not apply only to implementing a checklist.) Large
849 organizations should also follow this procedure and, if possible, first select several operational
850 systems as pilots to provide “real-world” testing for the checklist before enterprise-wide
851 deployment.

852 ■ Setting Verification

853 – Even after reviewing and testing a checklist, users should handle verification carefully to ensure
854 that product settings are not inadvertently altered.

855 After initially applying a checklist, an organization may need to acquire and apply revised versions of the
856 checklist in the future. Depending on the product being secured, a checklist may be updated periodically
857 based on a set schedule or updated as needed, frequently or infrequently. For selected checklists, NIST
858 may maintain a mailing address list of users, and users who subscribe to the list will receive
859 announcements of updates or other issues connected with the checklist. Instructions for subscribing to the
860 mailing address list will be included in the selected checklist’s description on the checklist repository. An
861 organization that acquires an updated checklist would perform the same steps already described in this
862 section while taking advantage of knowledge gained and documented from applying previous versions of
863 the checklist.

864 **4.5 Providing Feedback on Checklists**

866 NIST welcomes all “bug” reports, comments, and suggestions from checklist users in regard to individual
867 checklists or the repository itself. Such feedback should be directed to checklists@nist.gov.¹³

868
869 Some of the questions that checklist users may want to consider when evaluating a checklist include the
870 following:

871 ■ Documentation

872 – Does it explain the security objectives?

873 – Does it contain a complete, clear, and concise description of the checklist settings?

874 ■ Recommended Practices

875 – Are the checklist settings consistent with recommended practices?

876 – Do the checklist settings take into account recent vulnerabilities?

877 ■ Impact of Settings

878 – Has the checklist developer tested the checklist settings on the product in an operationally
879 realistic environment and determined that the application of the checklist settings causes the
880 product to meet the security objectives of the checklist?
881

¹³ 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 that would prohibit doing so.

- 882 – Do any of the checklist settings cause the product to become inoperable or unstable?
- 883 – Do any of the checklist settings reduce product functionality? If so, is this documented?
- 884 ■ Ease of Implementation
- 885 – Is the checklist straightforward to apply?
- 886 – Are the instructions concise, sound, and complete?
- 887 – Is the required skill level identified?
- 888 – Are procedures to verify that the installation is successful included?
- 889 – Is there guidance for uninstalling the checklist or restoring the product to the state before
890 installation?
- 891 – If the checklist cannot be rolled back, does the documentation recommend other preparatory
892 measures such as backups?
- 893 ■ Assistance
- 894 – Is checklist-related help available?
- 895 – Does the documentation contain information for troubleshooting if errors occur or if the checklist
896 settings cause the product to operate incorrectly?
- 897 – Is there assistance available for qualified users of the product?
- 898 ■ If the checklist developer is NOT the IT product's vendor, does the documentation indicate whether
899 the checklist has been sponsored or endorsed by the IT product's vendor?
- 900

901 5. Checklist Development

902 This section describes the general process for developing security configuration checklists and submitting
903 them to the NCP. It includes an overview of the process NIST will follow to screen the checklist
904 submissions and publish them in its repository, and the process NIST and developers will follow to
905 update the checklist or to archive the checklist. Individual developers and organizations that want to
906 submit checklists to NIST should review the appendices of this document, which contain the
907 administrative requirements for participation in the NCP. Before submitting a checklist to NIST,
908 developers should ensure they have the most recent version of this document. The most recent version is
909 available as a separate file at <https://nvd.nist.gov/ncp/participation>.

910
911 The checklist life cycle comprises the following steps:

- 912 1. **Initial Checklist Development:** The developer¹⁴ becomes familiar with the procedures and
913 requirements of the checklist program, and then performs the initial development of the checklist,
914 including selection of a target environment.
- 915 2. **Checklist Testing:** The developer tests the checklist in the target environment and corrects any
916 problems with the checklist.
- 917 3. **Checklist Documented:** The developer documents the checklist according to the guidelines of
918 the program.
- 919 4. **Checklist Submitted to NIST:** The developer submits the checklist and documentation package
920 to NIST for screening and public review.
- 921 5. **NIST Screening:** NIST screens the checklist package's information and confirms that any SCAP
922 data stream content is well-formed, then addresses any issues with the developer prior to public
923 review.
- 924 6. **Public Review and Feedback:** NIST holds a 30-day public review of the candidate checklist,
925 then the developer addresses comments as necessary.
- 926 7. **Final Listing on Checklist Repository:** NIST lists the checklist on repository as final and
927 announces the checklist's availability.
- 928 8. **Checklist Maintenance and Archival:** Anyone can provide feedback on the checklist
929 throughout its life. The developer updates the checklist periodically as necessary. The checklist is
930 archived when it is no longer being maintained or is no longer needed.

931
932 Each step should be carried out to ensure the checklist is accurate, tested, and documented during its
933 development and subsequent publication, update, or archival. The following sections describe
934 considerations for each step. USGCB checklists for the US Government environment follow the steps in
935 this section, but they must meet additional requirements as detailed in Appendix D.

936 5.1 Developer Steps for Creating, Testing, and Submitting Checklists

938 The first four steps in the development methodology listed above involve the developer creating, testing,
939 documenting and submitting checklists. Sections 5.1.1 through 5.1.4 describe each of these steps in
940 greater detail.

941 5.1.1 Initial Checklist Development

943 During initial checklist development, a developer becomes familiar with the requirements of the checklist
944 program and all procedures involved during the checklist life cycle (as described throughout this section).

¹⁴ For simplicity, the rest of this document uses the term "developer" to refer to the individual, individuals, or institution that is developing a checklist.

945 At this point, a developer would presumably agree to the requirements for participation in the NCP before
946 continuing to develop the checklist. The participation requirements are described in this document, but are
947 presented in administrative and programmatic terms in Appendix B, which is intended less for technical
948 developers and more for those in developer organizations who must formally agree to NCP requirements.
949 The participation agreement is contained in Appendix C.¹⁵

950

951 After agreeing to NCP requirements, the developer decides in which operational environment (see
952 Section 3) the checklist should be implemented, and builds the checklist accordingly. The output of this
953 step is an initial checklist for the product.

954

955 NIST recognizes that detailed checklist development cannot be covered extensively in this document.
956 Developers may find publications on commonly accepted technical security principles and practices, as
957 catalogued in NIST SP 800-53 [7] and NIST SP 800-27, *Engineering Principles for Information*
958 *Technology Security (A Baseline for Achieving Security)* [5], to be helpful when developing a checklist.
959 There are also many publications related to SCAP available at <https://scap.nist.gov/>.

960

961 In terms of vulnerability coverage, the security objectives should take into account the most up-to-date
962 vulnerabilities and generally be consistent with recognized sources of vulnerability-related information,
963 including the Department of Homeland Security's (DHS) United States Computer Emergency Readiness
964 Team (US-CERT), the Computer Emergency Response Team/Coordination Center (CERT/CC), and
965 NIST's NVD.¹⁶

966

967 Developers of checklists for products that are used by the federal government should consult the FISMA-
968 associated security control requirements. NIST SP 800-53 [7] provides a catalog of security controls,
969 using groups of the controls to create three minimum security control sets for federal information
970 systems—low, moderate, and high impact as specified in FIPS 199 [9]. Developers of IT products that
971 will be used in federal information systems are encouraged to help federal agencies meet the mandatory
972 requirements in FISMA by creating checklists that provide recommended configuration settings in a
973 variety of operational environments or for information systems of differing impact levels, as described in
974 FIPS 199 and SP 800-53. Developers are also encouraged to consider requirements imposed by HIPAA
975 and other sources.

976

977 **5.1.2 Checklist Testing**

978 Before a checklist is submitted to NIST, it should be fully tested in a configuration that meets the target
979 environment and platform. The checklist should be tested with a variety of applications and hardware
980 platforms, if applicable. Ideally, at least some testing should be performed in a production or mirrored
981 production environment. The testing data does not need to be submitted to NIST; however, the developer
982 should retain the data for review as appropriate.

983

984 Selecting the most appropriate set of security controls can be a daunting task because many security
985 controls have limited system functionality and usability. In some cases, a security control can have a
986 negative impact on other security controls. For example, installing a patch could inadvertently break
987 another patch. Therefore, it is important to perform testing for all security controls to determine what
988 impact they have on system security, functionality, and usability, and to take appropriate steps to address
989 any significant issues.

990

¹⁵ The latest updates to these sections and to 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.

¹⁶ US-CERT website is <https://www.us-cert.gov/>. CERT/CC website is <https://www.cert.org/>. NVD is at <https://nvd.nist.gov/>.

991 NIST has produced SP 800-115, *Technical Guide to Information Security Testing and Assessment* [8], to
 992 help administrators in testing systems for vulnerabilities and configuration problems. Although this
 993 publication is focused more on testing systems than testing individual IT products, it may be useful to
 994 checklist developers.

995

996 **5.1.3 Checklist Documented**

997 The quality of checklist documentation often makes a major difference in the checklist's effectiveness.
 998 The checklist documentation should clearly explain how to use the checklist, with concise, sound, and
 999 complete instructions. The skill level required to use the checklist should be identified, as well as the
 1000 targeted environment. The documentation should also explain the significance of individual settings,
 1001 including any changes to product functionality. If applicable, the documentation should also include
 1002 procedures to verify that the checklist installation is successful, as well as guidance for uninstalling the
 1003 checklist or restoring the product to its state before installation of the checklist. In some cases, it may not
 1004 be possible to roll back checklist settings, in which case the checklist documentation should recommend
 1005 procedures such as backups and system restoration as applicable.

1006

1007 The testing methodology, such as how the checklist was tested and what platforms were used, should be
 1008 documented. The checklist documentation should also contain information for troubleshooting if errors
 1009 occur or if the checklist settings cause the product to operate incorrectly. Ideally, assistance is available
 1010 for (registered) users of the product if there are problems.

1011

1012 Checklist developers must complete an online checklist description form for each checklist.¹⁷ Table 1
 1013 shows the fields in the checklist description form that developers are to complete.

1014

1015

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	States 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).
Target	The set of specific IT systems or applications that the checklist provides guidance for.
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	Summarizes the purpose of the checklist and its settings.
Known Issues	Summarizes 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 to correctly use the checklist.

¹⁷ 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 Operational Environment	The IT product’s operational environment, such as Standalone, Managed, or Custom (with description, such as Specialized Security-Limited Functionality, Legacy, or United States Government). Generally only applicable for security compliance/vulnerability checklists.
Checklist Type	The type of checklist, such as Compliance, Vulnerability, and Specialized.
Checklist Installation Tools	Describes the functional tools required to use the checklist to configure the system, if they are not included with the checklist.
FIPS 140-2 Compliance	Whether the product can operate in a FIPS 140-2 validated mode (yes or no).
Regulatory Compliance	Whether the checklist is consistent with various regulations and standards (e.g., Health information Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley Act [GLBA], FISMA [such as mappings to NIST SP 800-53 controls], ISO 27001, Sarbanes-Oxley, Department of Defense [DoD] 8500, Federal Risk and Authorization Management Program [FedRAMP], Committee on National Security Systems Instruction [CNSSI] 1253, Control Objectives for Information and Related Technologies [COBIT] 5, the NIST Cybersecurity Framework, the Center for Internet Security [CIS] Controls).
Authority	The organization responsible for producing the original security configuration guidance represented by the checklist. Authorities are ranked according to their “Authority Type.” Within the NCP website, authorities are grouped with their authority types through the syntax of <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 any additional testing-related information such as summary of 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	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 for usage of 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.
Point of Contact	An email address where questions, comments, suggestions, and problem reports can be sent in reference to the checklist. The point of contact should be an email address that the checklist developer monitors for checklist problem reports.
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, General Public License [GPL], free software, shareware).
SCAP Content	A link to the machine-readable content representing the configuration guidance. This guidance is expressed using SCAP.
Supporting Resource	A link to any supporting information, or content, relating 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	Indicate 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.

1016
1017 The developer needs to complete the fields as indicated to describe the checklist accurately and minimize
1018 user confusion as to what the checklist accomplishes.

1019
1020 In summary, well-structured checklist documentation includes the following, as appropriate:

1021
1022 ■ Statement of the security objectives, including the expected behavior of the product after applying the
1023 checklist

1024 ■ The intended audience (e.g., end user, system administrator) and the level of technical skill required
1025 to use the checklist

1026 ■ Explanation of the checklist settings, including each setting's effect on operation of the product and
1027 any functionality the settings enable or disable

1028 ■ Backup procedures or any other initial steps required before applying the checklist

1029 ■ As appropriate, step-by-step instructions for applying the checklist (e.g., screen shots, illustrated
1030 procedures) and verifying that the installation is successful

1031 ■ Troubleshooting instructions or other information and references.

1032 **5.1.4 Checklist Submitted to NIST**

1033 At this point, the checklist developer has completed, tested, and documented the checklist. The developer
1034 now submits the package of materials to NIST. The package includes the following:

1035
1036 ■ Checklist and configuration files, templates, scripts, etc.

1037 ■ Completed checklist description

1038 ■ Checklist documentation

1039 ■ Identification of the developer point of contact

1040 ■ Signed participation agreement.

1041 The participation agreement and other requirements are outlined in detail in Appendix B, which also
1042 includes the appropriate NIST contact information.

1043
1044 Checklist packages are submitted to NIST through the NCP Submission website. The website walks the
1045 checklist developer through a series of screens that collect all of the information and materials needed for
1046 checklist submission. In addition, the website allows checklist developers to view the checklists they have
1047 submitted, see tasks that have been assigned to them (such as fixing errors on a previously submitted
1048 checklist), update existing checklists, and perform other actions. NIST also provides web services for
1049 submitting, fetching, and maintaining checklists. To request access to the NCP Submission website or
1050 associated web services, email checklists@nist.gov.

1051 1052 **5.2 NIST Steps for Reviewing and Finalizing Checklists for Publication**

1053 The NIST process for screening and publishing a checklist, which corresponds to steps 5 through 8 in the
1054 checklist life cycle, is described in the following sections.

1055

1056 **5.2.1 NIST Screening of the Checklist Package**

1057 This step involves determining if the appropriate checklist materials are sufficiently accurate and
1058 complete to be publicly reviewed. NIST screens the checklist information for completeness and accuracy,
1059 and ensures that checklist content is well-formed if it is SCAP-expressed. NIST may contact the
1060 developer with questions about the submitted materials during the screening period.

1061 **5.2.2 Public Review and Feedback for the Candidate Checklist**

1063 After the checklist package has been screened and the developer has addressed any issues, NIST will post
1064 it as a candidate draft and announce it for public review for a period of 30 days. This allows the public to
1065 review and test the checklist, and to provide the checklist developers and NIST with comments and
1066 feedback. Information from comments and feedback may be incorporated in a revision of the checklist to
1067 improve its quality. When a candidate checklist has completed the review process, its information is
1068 added to the checklist repository.

1069 A checklist reviewer emails checklists@nist.gov to provide comments as well as other information about
1070 the reviewer's test environment, procedures, and other relevant information. Depending on the review, the
1071 checklist developer may need to respond to comments. NIST may also consult independent expert
1072 reviewers as appropriate. Typical reasons for using independent reviewers include the following:

1073

- 1074 ■ NIST may decide that it does not have the expertise to determine whether the comments have been
1075 addressed satisfactorily.

1076

- 1077 ■ NIST may disagree with the proposed issue resolutions and seek reviews from third parties to get
1078 additional perspectives.

1079 At the end of the public review period, NIST will give the developer 30 days to respond to comments.

1080 **5.2.3 Final Listing on Checklist Repository**

1082 After any outstanding issues are addressed, NIST lists the final checklist and announces that the checklist
1083 is now listed on the repository. At this time, the developer (e.g., IT product vendor) may be eligible to use
1084 the checklist logo on the IT product's promotional material if the developer provides assistance for the
1085 checklist. Requirements for use of the logo are described in Appendix C.

1086 **5.2.4 Checklist Maintenance and Archival**

1087 Throughout a checklist's life cycle, anyone can provide comments or ask questions regarding the
1088 checklist by mailing checklists@nist.gov; NIST will pass feedback to the checklist developer. Depending
1089 on the product and how frequently updates occur, NIST may maintain a mailing address for the associated
1090 checklists. Users who subscribe to the mailing list can receive announcements of updates or other issues
1091 connected with a checklist. The selected checklist's description (on the checklist repository) will contain
1092 instructions for subscribing to the mailing address list.

1093 After the final checklist is listed, NIST will periodically review the checklist to determine if it is still
1094 relevant or if changes need to be made to it. If the developer decides to update the checklist at any time,
1095 NIST will announce that the checklist is in the process of being updated. If the revised checklist contains
1096 major changes, it will be accepted as if it were a new submission, and will be required to undergo the
1097 same review process as a new submission.

1100

- 1101 At NIST's or the developer's discretion, the checklist can be removed from the repository or marked as an
1102 archive. Typical reasons for such actions would be that the product is no longer supported or is obsolete,
1103 or that the developer no longer wishes to provide support for the checklist.

1104 **Appendix A. References**

1105 This appendix contains a list of documents referenced by this publication.

1106

[1]	Part 39 of the Federal Acquisition Regulation (FAR), https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP39.html
[2]	Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[3]	Cyber Security Research and Development Act of 2002, Public Law 107-305, 116 Stat. 2367, http://www.gpo.gov/fdsys/pkg/PLAW-107publ305/pdf/PLAW-107publ305.pdf
[4]	NIST Special Publication (SP) 800-126, <i>The Technical Specification for the Security Content Automation Protocol (SCAP)</i> , all versions available at http://csrc.nist.gov/publications/PubsSPs.html .
[5]	NIST Special Publication (SP) 800-27 Revision A, <i>Engineering Principles for Information Technology Security (A Baseline for Achieving Security)</i> , June 2004, https://doi.org/10.6028/NIST.SP.800-27rA
[6]	NIST Special Publication (SP) 800-37 Revision 1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i> , February 2010 (updated 6/5/2014), https://doi.org/10.6028/NIST.SP.800-37r1
[7]	NIST Special Publication (SP) 800-53 Revision 4, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i> , April 2013 (updated 1/22/2015) https://doi.org/10.6028/NIST.SP.800-53r4
[8]	NIST Special Publication (SP) 800-115, <i>Technical Guide to Information Security Testing and Assessment</i> , September 2008, https://doi.org/10.6028/NIST.SP.800-115
[9]	Federal Information Processing Standard (FIPS) 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , February 2004, https://doi.org/10.6028/NIST.FIPS.199
[10]	Committee on National Security Systems (CNSS) Instruction No. 4009, <i>Committee on National Security Systems (CNSS) Glossary</i> , April 6, 2015, https://www.cnss.gov/CNSS/issuances/Instructions.cfm

1107

1108 Appendix B. Checklist Program Operational Procedures



1119 Operational Procedures
1120 for
1121 The NIST National Checklist Program
1122 for Information Technology Products

1123
1124 Version 1.4 (Draft)

1125
1126
1127
1128 This document sets forth the policies, procedures and general requirements for the NIST National
1129 Checklist Program for Information Technology Products. This document is intended for those individuals
1130 in developer organizations who would need to formally agree to the program's requirements.

1131
1132 This document is organized as follows:

- 1133 ■ Section 1 – general considerations for the NIST National Checklist Program
- 1134 ■ Section 2 – procedures for initial screening of a checklist prior to public review
- 1135 ■ Section 3 – procedures for the public review of a candidate checklist
- 1136 ■ Section 4 – final acceptance procedures
- 1137 ■ Section 5 – maintenance and delisting procedures
- 1138 ■ Section 6 – record keeping

1139
1140 The following terminology is used in this appendix:

- 1141 ■ *Candidate* is a checklist that has been screened and approved by NIST for public review.
- 1142 ■ *FCL* refers to the final checklist list—the listing of all final checklists on the NIST repository.
- 1143 ■ *Final* is a checklist that has completed public review, has had all issues addressed by the checklist
1144 developer and NIST, and has been approved for listing on the repository according to the procedures
1145 of this section.
1146

- 1147 ■ *Checklist* refers to a checklist for a specific product and version.
- 1148 ■ *Checklist Developer* or *Developer* is an individual or organization that develops and owns a checklist
1149 and submits it to the National Checklist Program.
- 1150 ■ *Independent Qualified Reviewers* are tasked by NIST with making a recommendation to NIST
1151 regarding public review or listing of the checklist. They work independently of other reviewers and
1152 are considered expert in the technology represented by the checklist.
- 1153 ■ *Logo* refers to the NIST National Checklist Program logo.
- 1154 ■ *National Checklist Program, Program, or NCP* is used in place of the NIST National Checklist
1155 Program for Information Technology Products.
- 1156 ■ *NIST Checklist Repository* or *Repository* refers to the website that maintains the checklists, the
1157 descriptions of the checklists, and other information regarding the National Checklist Program.
- 1158 ■ *Public Reviewer* is any member of the general public who reviews a candidate checklist and sends
1159 comments to NIST.
- 1160 ■ *Operational Environments* refer to the operational environments outlined in this document.
- 1161 References to documents that form a basis for the requirements of this program are as follows:
1162
- 1163 ■ FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*,
1164 <https://doi.org/10.6028/NIST.FIPS.199>
- 1165 ■ NIST SP 800-27 Revision A, *Engineering Principles for Information Technology Security (A*
1166 *Baseline for Achieving Security)*, <https://doi.org/10.6028/NIST.SP.800-27rA>
- 1167 ■ NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and*
1168 *Organizations*, <https://doi.org/10.6028/NIST.SP.800-53r4>
- 1169 ■ Draft NIST SP 800-70 Revision 4, *National Checklist Program for IT Products—Guidelines for*
1170 *Checklist Users and Developers*, <http://csrc.nist.gov/publications/PubsSPs.html>

1171

1172 **1. Overview and General Considerations**

1173 This section focuses on general considerations for all parts of the National Checklist Program.

1174

1175 (a) **Checklist Lifecycle Overview:** Checklists typically have the following lifecycle:

1176

- 1177 1. Checklist developers inquire about the program and download a submission package. The
1178 developer subsequently contacts NIST with a tested checklist, supporting information, and a
1179 signed agreement to the requirements of the NCP. Checklist submission requirements and
1180 procedures are discussed in Section 2.
- 1181 2. NIST verifies that all information is complete and performs a high-level screening on the
1182 checklist package. Checklists meeting the requirements for listing receive further
1183 consideration and are referred to as “candidate checklists.” Section 2 discusses screening
1184 criteria and procedures.
- 1185 3. NIST lists the candidate checklist on the repository for public review for a period of 30 days,
1186 as discussed in Section 3.

- 1187 4. NIST forwards comments from public reviewers to the developer. The developer addresses
1188 the issues as appropriate, and the checklist is listed on the FCL, as discussed in Section 4.
1189 5. NIST periodically reviews each final checklist to determine whether its listing should
1190 continue, be updated, or be archived, as discussed in Section 5.
1191
- 1192 (b) **Intellectual Property Rights:** Developers retain intellectual property rights to their checklists.
1193
- 1194 (c) **Confidential Information:** NIST does not anticipate the need to receive confidential information
1195 from checklist developers. If it becomes necessary to disclose confidential information to NIST, NIST
1196 and the developer must enter into a separate confidentiality agreement prior to such disclosure.
1197
- 1198 (d) **Independent Qualified Reviewers:** NIST may decide to seek technical advice from independent
1199 qualified experts who will review checklist submissions to determine whether they meet the program
1200 requirements. The reviewers are tasked with making a recommendation to NIST regarding a
1201 subsequent public review or final listing of the checklist. Typical but not exclusive of the reasons for
1202 using independent reviewers include the following:
1203
- 1204 1. NIST does not possess the expertise to determine whether issues have been addressed
1205 satisfactorily.
 - 1206 2. NIST disagrees with proposed issue resolutions.
- 1207 (e) **Terminating Consideration of a Checklist Submission:** NIST or the developer may terminate
1208 consideration of checklist submissions at any time. If NIST terminates consideration, the points of
1209 contact are asked to respond within 10 business days. Typical but not exclusive of the reasons for
1210 terminating consideration of checklist submissions include the following:
1211
- 1212 1. The submission package does not meet the screening criteria.
 - 1213 2. The developer fails to address issues raised at other times.
 - 1214 3. The developer violates the terms and conditions of participation in the program.

1215

1216 2. Checklist Submission and Screening

1217 This section outlines the procedures and requirements for submitting checklists to NIST and the process
1218 by which NIST determines if checklists are suitable for public review. When checklists meet the
1219 screening criteria, they receive further consideration in a public review and are referred to as “candidate
1220 checklists.” NIST then follows the subsequent procedures.
1221

1222 (a) **Notification of Checklist Program Requirements:** NIST maintains on the repository a complete set
1223 of information for developers. The information outlines the requirements for participation in the
1224 program and describes materials and timeframes.
1225

1226 (b) **Materials Required From the Developer:** Developers provide the following information:
1227

- 1228 1. Contact information for an individual from the submitting organization who will serve as the
1229 point of contact for questions and comments pertaining to the checklist, and contact
1230 information for a backup or deputy point of contact. The information must include postal
1231 address, direct telephone number, and email address.

- 1232 2. The checklist, documentation, and description template.
- 1233 3. The participation agreement, which must be printed, signed, and sent to NIST. NIST accepts
1234 emailed PDF copies of the participation agreement, facsimiles, or copies via regular mail.
- 1235 4. Participation fees. Currently, there is no fee to checklist developers. NIST reserves the right
1236 to charge fees for participation in the future. Fees are not retroactive.

- 1237 (c) **Preliminary Screening Checklist Contents:** NIST performs a preliminary screening to verify that
1238 checklist packages meet the basic program requirements. NIST will not typically perform an in-depth
1239 analysis of the content of the checklist, such as its reflection of recommended security and
1240 engineering practices, although NIST reserves the right to do so.

1241

1242 3. Candidate Checklist Public Review

1243 NIST follows the subsequent procedures when listing candidate checklists for public review.

1244

- 1245 (a) **Public Review Period:** NIST lists candidate checklists for a 30-day comment period. NIST reserves
1246 the right to extend the review cycle, particularly for long or complicated checklists. NIST uses the
1247 following disclaimer (or very similar words) in conjunction with candidate checklists:

1248

1249 *NIST does not guarantee or warrant the checklist's accuracy or completeness. NIST is not*
1250 *responsible for loss, damage, or problems that may be caused by using the checklist.*

1251

- 1252 (b) **Accepting Comments from Reviewers:** Public reviewers email checklists@nist.gov to provide their
1253 comments as well as information about their test environment, procedures, and other relevant
1254 information. The contents of these emails are considered public records.

1255

- 1256 (c) **Maintaining Records:** NIST may maintain copies of correspondence and feedback between the
1257 public and developers by creating a unique email address for each checklist. If so, NIST will archive
1258 the information.

1259

- 1260 (d) **Addressing Comments:** After the end of the public review period, the developer has 30 days to
1261 respond to comments.

1262

1263 4. Final Checklist Listing

1264 After NIST determines that a checklist and the associated developers have met all requirements for final
1265 listing, NIST lists checklists in the FCL and refers to them as "final checklists." NIST then follows the
1266 subsequent procedures.

1267

- 1268 (a) **Finalizing Checklists:** NIST lists the checklist in the FCL. NIST may send announcements to
1269 various email lists maintained by NIST or other organizations. NIST uses the following disclaimer (or
1270 very similar words) for final checklists:

1271

1272 *NIST does not guarantee or warrant the checklist's accuracy or completeness. NIST is not*
1273 *responsible for loss, damage, or problems that may be caused by using the checklist.*

1273

- 1274 (b) **Handling Comments:** NIST continues to accept comments about final checklists by maintaining a
1275 central email address on the repository, checklists@nist.gov. NIST lists the procedures to be used for

1276 contacting the developer, along with the contact information for the developer, such as an email
 1277 address or URL. If at any time the point of contact changes, NIST must be notified immediately.

1278

1279 **5. Final Checklist Update, Archival, and Delisting**

1280 NIST follows the subsequent procedures for periodic update, archival, and delisting of final checklists.

1281

1282 (a) **Periodic Reviews:** NIST periodically reviews each checklist to identify changes in its status. NIST
 1283 may contact developers, as appropriate, to determine if there are changes in the status of a checklist,
 1284 in which case developers have 30 days to respond and indicate whether checklists should be updated,
 1285 archived, or delisted.

1286

1287 (b) **Updates:** NIST may indicate on the FCL when checklists are under review. Developers have 60 days
 1288 after the review to submit the updated material to NIST. Depending on the magnitude of updates,
 1289 NIST may screen the checklist and schedule a public review.

1290

1291 (c) **Archival:** A developer may no longer want to provide support for the checklist, a product may no
 1292 longer be supported, or there may be another reason to archive a checklist. At the developer or
 1293 NIST's discretion, the checklist can remain in the repository, but it will be reclassified as an archive.

1294

1295 (d) **Delisting:** When delisting occurs, such as when a developer fails to respond to inquiries from NIST
 1296 about the status of a checklist, NIST removes the checklist from the FCL. NIST may send
 1297 announcements to various email lists maintained by NIST or other organizations.

1298

1299 **6. Record Keeping**

1300 NIST maintains information associated with the program and requires that participants in the checklist
 1301 program also maintain certain records, as follows.

1302

1303 (a) **NIST Records:** During the period that a checklist has been submitted to NIST, and during the period
 1304 that a checklist is listed on the FCL as a final or archived checklist, and for three years thereafter¹⁸,
 1305 NIST will maintain the following:

1306

1. The checklist description template, as listed on the repository

1307

2. The checklist and checklist description, as listed on the repository

1308

3. All comments submitted as part of the public review

1309

4. All comments submitted to NIST regarding the checklist.

1310

(b) **Developer Records:** During the period that a checklist has been submitted to NIST, and during the
 1311 period that a checklist is listed on the FCL as a final or archived checklist, the developer will maintain
 1312 the following:

1313

1. The checklist description template, as listed on the repository

1314

2. The checklist and checklist description, as listed on the repository

1315

3. Test reports and other evidence of checklist testing.

¹⁸ This is for three years after the most recent update to the checklist.

1316 Appendix C. Participation and Logo Usage Agreement Form

1317 This appendix contains the terms and requirements for participation in the NIST National Checklist
1318 Program (NCP) and for use of the NIST National Checklist Program logo. Prior to submission of a
1319 checklist to NIST, developers should ensure they have the most recent version of this appendix. The most
1320 recent version is available as a separate file at <https://nvd.nist.gov/ncp/participation>.



1322
1323
1324
1325
1326
1327
1328
1329
1330
1331 Participation and Logo Usage Agreement Form
1332 for
1333 The NIST National Checklist Program for
1334 Information Technology Products

1335
1336 Version 1.5 (Draft)
1337 August 1, 2017
1338
1339
1340

1341 The phrase “NIST National Checklist Program for Information Technology Products” and the NIST
1342 National Checklist Program logo are intended for use in association with specific versions of information
1343 technology (IT) products for which a checklist has been created and has met the requirements of the
1344 National Institute of Standards and Technology (NIST) National Checklist Program for Information
1345 Technology Products for final listing on its checklist repository. You may participate in the NIST
1346 National Checklist Program and use the phrase and logo provided that you agree in writing to the
1347 following terms and conditions:

- 1348
1349 1. You will follow the rules and requirements of the program as outlined in the NIST Operational
1350 Procedures for the NIST National Checklist Program (Appendix B of NIST SP 800-70
1351 Revision 4).
1352
- 1353 2. You will respond to comments and issues raised by a public review of your checklist submission
1354 within 30 days of the end of the public review period. Any comments from reviewers and your
1355 responses may be made publicly available.
1356
- 1357 3. You agree to maintain the checklist and provide a timely response (within 10 business days) to
1358 requests from NIST for information or assistance with regard to the contents of the checklist.
1359

- 1360 4. You agree to maintain checklist-related records according to the requirements of the NIST
1361 National Checklist Program, as listed in Appendix B of NIST SP 800-70 Revision 4, item 6.b.
1362
- 1363 5. You will hold NIST harmless in any subsequent litigation involving the checklist submission.
1364
- 1365 6. You may terminate your participation in the NIST National Checklist Program at any time. You
1366 will provide two business weeks' notice to NIST of your intention to terminate participation.
1367 NIST may terminate its consideration of a checklist submission or your participation in the NIST
1368 National Checklist Program at any time. NIST will contact you two business weeks prior to its
1369 intention to terminate your participation. You may, within one business week, appeal the rejection
1370 and provide supporting evidence.
1371
- 1372 7. You may not use the name of NIST or the Department of Commerce on any advertisement,
1373 product, or service that is directly or indirectly related to this agreement. By accepting this
1374 agreement, NIST does not directly or indirectly endorse any product or service provided, or to be
1375 provided, by you, your successors, assignees, or licensees. You may not in any way imply that
1376 this agreement is an endorsement of any such product or service. You may not combine use of the
1377 logo with other Marks, phrases, or logos in such a way that would imply endorsement by NIST.
1378
- 1379 8. The phrase "NIST National Checklist Program for Information Technology Products" and the
1380 NIST National Checklist Program logo are Registered Marks of NIST, which retains exclusive
1381 rights to their use. NIST reserves the right to control the quality of the use of the phrase "NIST
1382 National Checklist Program for Information Technology Products" and the NIST National
1383 Checklist Program logo.
1384
- 1385 9. Your permission for advertising participation in the NIST National Checklist Program and use of
1386 the logo is conditional on and limited to those products and the specific product versions for
1387 which a checklist is made currently available by NIST through the NIST National Checklist
1388 Program on its Final Checklist List.
1389
- 1390 10. Your permission for advertising participation in the NIST National Checklist Program and use of
1391 the logo is conditional on and limited to those checklist developers who provide assistance and
1392 help to users of the checklist with regard to proper use of the checklist and that the warranty for
1393 the product and the specific product versions is not changed by use of the checklist.
1394
- 1395 11. Your use of the logo on product reports, letterhead, brochures, marketing material, and product
1396 packaging must be accompanied by the following: "TM: a Registered Mark of NIST, which does
1397 not imply product endorsement by NIST or the U.S. Government."
1398
- 1399 12. The dimensional requirements for the size, placement, color, and other aspects of the logo are
1400 specified in NIST SP 800-70 Revision 4.
1401
- 1402 13. NIST reserves the right to charge a participation fee in the future. No fee is required at present.
1403 No fees will be made retroactive.
1404
- 1405 14. NIST may terminate the NIST National Checklist Program at its discretion. NIST may terminate
1406 your participation in the Program for any violation of the terms and conditions of the program or
1407 for statutory or regulatory reasons.
1408
1409

1410 By signature below, the developer agrees to the terms and conditions contained herein.

1411
1412
1413

1414 Organization or company name:

1415
1416
1417

1418 Name and title of organization authorized person:

1419
1420
1421

1422 Signature:

1423
1424
1425

1426 Date:

1427
1428

1429 **Appendix D. Additional Requirements for USGCB Baselines**

1430 As mentioned in the Section 5 introduction, USGCB baselines have additional requirements that
1431 supplement those presented in Section 5. This appendix details these additional requirements and presents
1432 them based on the NCP Checklist Development Steps from Sections 5.1 and 5.2.

1433

1434 **D.1 Developer Steps for Creating, Testing, and Submitting USGCB Baselines**

1435 A new USGCB baseline's development is led by any US federal agency, which is referred to in this
1436 appendix as the *champion agency*.

1437

1438 This portion of the appendix lists additional requirements related to creating, testing, and submitting
1439 USGCB baselines that the champion agency must follow. See Section 5.1 for the base requirements.

1440

1441 **D.1.1 Initial Baseline Development**

1442 Each baseline originates from existing SCAP compliance and vulnerability final checklist posted on the
1443 National Checklist Program (NCP) website. Based on this checklist, an agency may tailor these settings to
1444 its enterprise environment. If the settings may be applicable to a broad range of federal systems, the
1445 agency should consider sending a representative to the Federal CIO Governance Committee for USGCB
1446 to discuss promotion of the settings to a USGCB baseline. USGCB baselines should be consistent with
1447 the guidance from NIST SP 800-53 Revision 4, which states that a baseline is "chosen based on the
1448 security category and associated impact level of information systems determined in accordance with FIPS
1449 Publication 199 and FIPS Publication 200, respectively."

1450

1451 USGCB settings are compiled by platform; a single platform may include one or more versions (e.g.,
1452 Windows 7 32-bit and Windows 7 64-bit). The champion agency must ensure that a discrete setting is
1453 defined for each baseline configuration. Providing general guidance does not meet the settings
1454 requirement for a USGCB candidate. NIST recognizes that some configurations may be site specific and
1455 defining discrete settings that could be mandated for all Federal agencies is not a trivial task. During the
1456 creation of the candidate settings, the champion agency should remember that these settings are intended
1457 to be used by all Federal agencies; therefore, the USGCB settings may be considered a common subset
1458 applicable to all. USGCB candidates should reflect the minimum or core set of configurations that are
1459 applicable for all Federal agencies. Agencies using a USGCB baseline may customize it, making the
1460 settings more restrictive or appending additional settings. In the case of configurations applicable to a
1461 broad number of environments but not appropriate for all, USGCB introduces the notion of "Conditional"
1462 status. For example, the use of wireless technologies may be allowed at some sites, but not at others. The
1463 baseline would provide discrete wireless configurations applicable only to sites where wireless
1464 technology is allowed.

1465

1466 Developing a viable USGCB baseline requires expertise with the IT product and the ability to balance
1467 security and operational needs. During baseline development, discrete settings are defined, reviewed, and
1468 tested with the goal of arriving at a baseline that provides protection while allowing operational
1469 functionality. The champion agency should draw on field experience and available security configuration
1470 resources, such as government security guidelines, product security guidelines, and industry
1471 recommendations when developing baseline settings. Each baseline should be referenced to a security
1472 guide, such as a DISA STIG/checklist, an NSA security configuration guide, or a vendor security guide.
1473 Champion agencies should also engage the product vendor during the baseline creation phase to ensure
1474 supportability and applicability. After settings are selected, the champion agency considers how each
1475 setting functions (e.g., registry value or file version) and identifies available methods for assessing

1476 compliance or determining a setting's value. As the baseline is created, the developers will test the
1477 system's behavior when settings are changed (e.g., examine the registry value, daemon, or service status).
1478

1479 Each USGCB candidate must be expressed as SCAP content. NIST recommends producing SCAP at the
1480 current version of SCAP to take advantage of the latest specification features and SCAP product
1481 validation¹⁹. If the SCAP content is produced in a version other than the latest, the SCAP content must
1482 comply with the requirements of the revision of NIST SP 800-126 commensurate with the corresponding
1483 SCAP version, and the SCAP content must pass validation using the current version of the NIST SCAP
1484 Content Validation Tool (SCAPVal).
1485

1486 Using the latest version of SCAP is generally advantageous because the baseline can take advantage of
1487 newer specifications for more accurate checking, but it is not mandatory to use the latest SCAP version.
1488 The champion agency should identify all baseline settings that do not have Open Vulnerability and
1489 Assessment Language (OVAL) checks, and then work with the product vendor to ensure that future
1490 versions of OVAL support these checks. Similarly, the champion agency should identify all
1491 configurations that do not have CCE identifiers and work with NIST and the content provider to ensure
1492 each configuration setting has a populated CCE.²⁰ Where automated OVAL checks are not possible or
1493 CCE identifiers cannot reasonably be supplied, each instance should be noted by the champion agency in
1494 the known issues document that is included with the USGCB candidate submission.
1495

1496 In addition to configuration checks, the champion agency should include up-to-date patch content, and the
1497 champion agency should continue to update the patch content before, during, and after baseline
1498 submission.
1499

1500 **D.1.2 Baseline Testing**

1501 There are two major aspects to USGCB candidate testing: verifying that the SCAP content is compliant
1502 with SCAP technical requirements, and evaluating the baseline settings in an operational environment.

1503 The champion agency should validate and test all SCAP content using the NIST SCAP Content
1504 Validation Tool (SCAPVal). SCAPVal is revised periodically as the SCAP specifications are updated.
1505 SCAP content testing must also include at least one validated SCAP validated product; the product
1506 chosen is at the discretion of the champion agency. If possible, validated product testing should simulate
1507 the environment that USGCB consumers will experience. A list of current SCAP Validation products can
1508 be found at <https://scap.nist.gov/validation/index.html>.

1509 Testing with SCAP validated products should include assessing a system in three configurations:

- 1510 ▪ Exact compliance: The configuration settings are equal to the discrete settings defined in the baseline.
- 1511 ▪ Reduced compliance: The configuration settings are less restrictive than those defined in the baseline.
- 1512 ▪ Enhanced compliance: The configuration settings are more restrictive than those defined in the
1513 baseline.

1514 In addition to verifying baseline compliance with SCAP requirements, the champion agency should also
1515 test the baseline in an operational enterprise environment of considerable size that is representative of a
1516 typical Federal agency's operational enterprise environment. This testing ensures the viability of the
1517 baseline in an operational environment. NIST recommends testing the baseline for a minimum of three
1518 months. Evidence of field testing should be documented and include information about the location,

¹⁹ For additional information on SCAP product validation, see the Frequently Asked Questions at <https://scap.nist.gov/validation/faq.html>.

²⁰ For more information about CCE, visit <https://nvd.nist.gov/cce/index.cfm>.

1519 duration, number of systems, issues identified, and successful resolution to known issues. The Field
1520 Testing Report template is provided in Appendix D.3.

1521 During the testing period, the baseline will be refined, arriving at a viable USGCB candidate baseline that
1522 is secure while accommodating operational requirements. The concept of leveraging a field tested
1523 configuration that provides security benefit without negative impact in an operational environment is
1524 paramount to the USGCB process. If baseline adjustments are needed to accommodate mission needs, the
1525 baseline should be updated and redeployed to the same group of operational systems for additional field
1526 testing.

1527 The configuration methods and materials are to be used for automating the configuration of test systems.
1528 The intended use of the configuration materials is facilitating lab setup for USGCB end users who test the
1529 baseline prior to deploying on operational systems. The format of these configuration materials may vary
1530 between products. For example, Microsoft provides Group Policy Objects (GPOs), whereas Red Hat may
1531 provide kickstart scripts.

1532 The champion agency should work with the vendor and the author of the content during baseline
1533 development and ensure the configuration automation materials produce a system that is USGCB
1534 compliant. NIST recommends the vendor choose the method and materials for configuration support. All
1535 configuration methods and materials in the USGCB candidate package should be fully tested, if possible
1536 during the field testing activities, and include end user instructions. At a minimum, test cases should
1537 ensure the methods and materials function as expected and produce a system that is compliant with the
1538 USGCB candidate. It is preferable that these materials be supported by the product vendor.

1539 The USGCB candidate settings should be reviewed and the results documented in the Field Testing
1540 Report template located in D.3. During this review, the tester determines whether the baseline will have
1541 operational impact, addresses known issues discovered during field testing, and determines how to assess
1542 each setting with OVAL. If the product vendor participates in the settings review and SCAP content
1543 refinement, the vendor is encouraged to do the following:

- 1544 ▪ Highlight settings that may have operational impact on systems
- 1545 ▪ Determine how each configuration setting can most accurately be assessed using an SCAP checking
1546 language (e.g., OVAL, OCIL)

1547 **D.1.3 Baseline Documented**

1549 In addition to the baseline documentation already mentioned, such as the SCAP content and the
1550 automated configuration materials, other documentation is required for USGCB baselines.

1551 Each baseline must be documented in a human-readable format, such as a settings spreadsheet, which lists
1552 a discrete setting for every configuration in the baseline. NIST recognizes that inherent differences in
1553 products will dictate variations in the settings documentation; however, the following fields are required:

- 1555 ▪ CCE Identifier – List the CCE identifier corresponding to this setting, if available
- 1556 ▪ Description of the setting – Include information needed to manually configure or assess. This will
1557 vary between products. For example, Windows documents define the Policy Path and Policy Setting
1558 Name, whereas Red Hat documents define the Technical Mechanism and Configuration Details.
- 1559 ▪ Setting – List the discrete setting recommended for the baseline
- 1560 ▪ Category – Use this column to indicate “Conditional” settings if appropriate

1561 Additional information may be included in the settings spreadsheet to provide explanation or technical
1562 details about the setting. Refer to <https://usgcb.nist.gov> for complete settings spreadsheets.

1563

1564 **D.1.4 Baseline Submitted to NIST**

1565 Once the configuration baseline is defined, SCAP content is developed, and field testing is complete, the
 1566 champion agency will submit the USGCB candidate package to the NIST checklist repository. A
 1567 complete USGCB candidate submission must include the following:

- 1568 ▪ Baseline settings spreadsheet
- 1569 ▪ SCAP content: automated checklist with validated SCAP data streams
- 1570 ▪ Known issues spreadsheet, which lists all issues with the settings or SCAP data streams
- 1571 ▪ Frequently Asked Questions (FAQ) document that addresses the questions that baseline consumers
 1572 are most likely to have
- 1573 ▪ Automated configuration materials (discussed below)
- 1574 ▪ Field testing report

1575

1576 **D.2 NIST Steps for Reviewing and Finalizing USGCB Baselines for Publication**

1577 This portion of the appendix lists additional requirements related to NIST screening and publishing
 1578 USGCB baselines. See Section 5.2 for the base requirements.

1579

1580 **D.2.1 NIST Screening of the Baseline Package**

1581 NIST reviews the USGCB candidate submission and determines whether the submission meets all
 1582 requirements for candidacy, namely the elements required for all NCP submissions plus the required
 1583 USGCB elements, as listed in Appendix D.1.4. If the submission meets the requirements, NIST will post
 1584 the USGCB candidate according to the NIST open document vetting process, which is analogous to
 1585 posting other content on CSRC (csrc.nist.gov). After the public comment period, NIST will conduct
 1586 comment adjudication and then provide the candidate USGCB baseline along with the adjudicated
 1587 comments to the Federal CIO Governance Committee for final consideration. Follow the steps defined in
 1588 Section 5.2.

1589 **D.2.2 Final Listing on Checklist Repository, Maintenance, and Archival**

1590 After the Federal CIO Governance Committee CCB approves the final configuration, OMB, the ISIMC,
 1591 and the CIO Council formally release the USGCB final version and may provide a date for mandated
 1592 implementation. The final USGCB is posted to <https://usgcb.nist.gov>. This final package includes the
 1593 requisite settings documentation, SCAP content, automated configuration scripts or virtual disk images,
 1594 an FAQ document, and a known issues document.

1595 During maintenance, NIST coordinates with the product vendor, ensuring all automated configuration
 1596 files are kept current in accordance with the vendor's update cycle as per Appendix B, item 5a.

1597

1598 **D.3 Field Testing Report Template**

1599 The following is the Field Testing Report template required for all USGCB candidate submissions.

1600



National Institute of Standards and Technology

U.S. Department of Commerce

1601 This Field Testing Report verifies successful testing of a USGCB candidate configuration in an
 1602 operational environment. This report must be included with the USGCB candidate package submitted to
 1603 the NIST National Checklist Program.
 1604

Champion Agency	
Champion Agency Point of Contact Name	
POC Email	
POC Phone	
Field Testing Site Location (Organization and location)	
Field Testing Technical Point of Contact Name	
POC Email	
POC Phone	
Dates of field testing	
Number of systems tested at field site	
Issue identified with the baseline ²¹	
Resolution to issue	

1605

²¹ Extend this template as needed in order to report all issues and the corresponding resolution.

1606 **Appendix E. Acronyms and Abbreviations**

1607 Selected acronyms and abbreviations used in the guide are defined below.

AIC	Architecture and Infrastructure Committee
CCB	Change Control Board
CCE	Common Configuration Enumeration
CERT/CC	Computer Emergency Response Team/Coordination Center
CMVP	Cryptographic Module Validation Program
CNSSI	Committee on National Security Systems Instruction
COBIT	Control Objectives for Information and Related Technologies
CPE	Common Platform Enumeration
CSRDA	Cyber Security Research and Development Act of 2002
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DNS	Domain Name System
DoD	Department of Defense
FAQ	Frequently Asked Questions
FCL	Final Checklist List
FDCC	Federal Desktop Core Configuration
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GLBA	Gramm-Leach-Bliley Act
GPL	General Public License
GPO	Group Policy Object
HIPAA	Health Information Portability and Accountability Act
IA	Information Assurance
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System
IP	Internet Protocol
IR	Interagency Report
IT	Information Technology
ITL	Information Technology Laboratory
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVD	National Vulnerability Database
OCIL	Open Checklist Interactive Language
OMB	Office of Management and Budget
OVAL	Open Vulnerability and Assessment Language
SCAP	Security Content Automation Protocol
SCAPVAL	Security Content Automation Protocol Validation Tool
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SSLF	Specialized Security-Limited Functionality
STIG	Security Technical Implementation Guide

TIS	Technology Infrastructure Subcommittee
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
VPN	Virtual Private Network
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

1608

1609

1610 **Appendix F. Glossary**

1611 Selected terms used in this guide are defined below. Definitions for some terms have been adapted from
1612 [10].

Audience	The intended audience that should be able to install, test, and use the checklist, including suggested minimum skills and knowledge required to correctly use the checklist.
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.
Authority	The organization responsible for producing the original security configuration guidance represented by the checklist.
Authority Type	The type of organization that is the authority for the checklist. The three types are Governmental Authority, Software Vendor, and Third Party (e.g., security organizations).
Automated Checklist	A checklist that is used through one or more tools that automatically alter or verify settings based on the contents of the checklist. Automated checklists document their security settings in a machine-readable format, either standard or proprietary.
Candidate Checklist	Checklist that has been screened and approved by NIST for public review.
Checklist	A document that contains instructions or procedures for configuring an IT product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized configuration changes to the product. Also referred to as a security configuration checklist, lockdown guide, hardening guide, security guide, security technical implementation guide (STIG), or benchmark.
Checklist Developer	An individual or organization that develops and owns a checklist and submits it to the National Checklist Program.
Checklist Group	Represents the grouping of checklists based on a common source material. Commonly used if an organization packages multiple sets of product guidance under the same name.
Checklist Revision	Represents a change to the checklist content that does not affect the underlying rule/value configuration guidance put forth by the content. A scenario that would require a new checklist revision is when SCAP content is created for a prose checklist. This revision would change the checklist's content type from Prose to SCAP Content. A new checklist revision would be created to accommodate this change, while still maintaining the Prose checklist revision for interested parties.
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 Type	The type of checklist, such as Compliance, Vulnerability, and Specialized.
Content Type	The form of the checklist content in terms of the degree of automation and standardization. Examples include Prose, Automated, and SCAP Content.
Custom Environment	An environment containing systems in which the functionality and degree of security do not fit the other types of environments.
Final Checklist	A checklist that has completed public review, has had all issues addressed by the checklist developer and NIST, and has been approved by NIST for listing on the repository.
Final Checklist List (FCL)	The listing of all final checklists on the NIST repository.
Independent Qualified Reviewer	A Reviewer tasked by NIST with making a recommendation to NIST regarding public review or listing of the checklist.
Legacy Environment	A Custom environment containing older systems or applications that may need to be secured to meet today's threats, but often use older, less secure communication mechanisms and need to be able to communicate with other systems.
Logo	The NIST National Checklist Program logo.
Managed Environment	Environment comprising centrally managed IT products, everything ranging from servers and printers to desktops, laptops, smartphones, and tablets.
NIST Checklist Repository	The website that maintains the checklists, the descriptions of the checklists, and other information regarding the National Checklist Program. Also known as the repository. https://checklists.nist.gov
Non-Automated Checklist	A checklist that is designed to be used manually, such as English prose instructions that describe the steps an administrator should take to secure a system or to verify its security settings.
Operational Environment	The type of environment in which the checklist is intended to be applied. Types of operational environments are Standalone, Managed, and Custom (including Specialized Security-Limited Functionality, Legacy, and United States Government).
Product Category	The main product category of the IT product (e.g., firewall, IDS, operating system, web server).
Prose Checklist	A checklist that provides a narrative descriptions of how a person can manually alter a product's configuration.
Public Reviewer	A member of the general public who reviews a candidate checklist and sends comments to NIST.
Review Status	The status of the checklist within the internal NCP review process. Possible status options are: Candidate, Final, Archived, or Under Review. A status of "Final" signifies that NCP has reviewed the checklist and has accepted it for publication within the program.
SCAP Content Checklist	An automated checklist that adheres to the SCAP specification in NIST SP 800-126 for documenting security settings in machine-readable standardized SCAP formats.

Specialized Security-Limited Functionality (SSLF) Environment	A Custom environment that is highly restrictive and secure; it is usually reserved for systems that have the highest threats and associated impacts.
Standalone Environment	Environment containing individually managed devices (e.g., desktops, laptops, smartphones, tablets).
Target	The set of specific IT systems or applications that the checklist provides guidance for.
Target Operational Environment	The IT product's operational environment, such as Standalone, Managed, or Custom (with description, such as Specialized Security-Limited Functionality, Legacy, or United States Government). Generally only applicable for security compliance/vulnerability checklists.
United States Government Environment	A Custom environment that contains federal government systems to be secured according to prescribed configurations as mandated by policy.

1614 **Appendix G. Change Log**1615 **Revision 4 Release 0 – August 1, 2017**

- 1616 • Revised front matter for the document.
- 1617 • Made minor editorial changes throughout the document.
- 1618 • Removed the checklist “tier” and “SCAP Expressed” concepts throughout the document.
- 1619 • Included removing several fields from Table 1 in Section 5.1.3, which lists the checklist
- 1620 description form fields that developers are to complete.
- 1621 • Revised the descriptions of checklist content types in Section 4.2 (examples are Prose,
- 1622 Automated, and SCAP Content).
- 1623 • Renamed the “Target Product” checklist description form field to “Target”, and renamed “Target
- 1624 Audience” to “Audience” in Table 1 in Section 5.1.3.
- 1625 • Updated Appendix B to reference NIST SP 800-70 Revision 4 instead of Revision 3, use updated
- 1626 URLs, and loosen the requirement in 5(c).
- 1627 • Updated Appendix C to reference NIST SP 800-70 Revision 4 instead of Revision 3.
- 1628 • Recompiled the glossary.
- 1629

1630 **Revision 3 Release 1 – December 8, 2016**

- 1631 • Revised the Executive Summary and Section 4.2 to reflect that federal civilian agencies should
- 1632 use government-authorized or mandated checklists if they are available.
- 1633 • Replaced the description in Section 3.5 of the Sector-Specific environment with the United States
- 1634 Government environment description. Changed the name of this environment throughout the
- 1635 publication.
- 1636 • Selected reference URLs have been updated in Appendix A and throughout the publication.
- 1637