Draft NIST Special Publication 800-70
Revision 4

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

Stephen D. Quinn
Murugiah Souppaya
Melanie Cook
Karen Scarfone

COMPUTER SECURITY

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-70 Revision 4

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

Stephen D. Quinn
Murugiah Souppaya
Melanie Cook
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

August 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

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

Authority

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

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

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

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

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

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

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

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

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

Reports on Computer Systems Technology

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

Abstract

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

Keywords

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

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.

Trademark Information

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

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

Table of Contents

List of Figures

List of Tables

Executive Summary

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Introduction

1.1 Purpose and Scope

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

1.2 Document Organization

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

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

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

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

Appendix A lists references for this document.

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

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

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

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

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

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

2. The NIST National Checklist Program

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

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

2.1 Security Configuration Checklists

A *security configuration checklist* (also referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark)[3] is essentially 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. The IT product may be commercial, open source, government-off-the-shelf (GOTS), etc.

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

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

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

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

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

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

2.2 Benefits of Using Security Checklists

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

- Provides a base level of security to protect against common and dangerous local and remote threats (e.g., malware, denial-of-service attacks, unauthorized access, and inappropriate usage)
- Verifies the configuration of certain technical security controls for system assessments, such as confirming compliance with certain Federal Information Security Modernization Act (FISMA) requirements or other sets of requirements, and understanding the exposure caused by misconfigurations
- Significantly reduces the time required to research and develop appropriate security configurations for installed IT products
- Allows smaller organizations to leverage outside resources to implement recommended practice security configurations
- 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)).

Although using security checklists for security compliance purposes can significantly improve overall levels of security in organizations, using a checklist cannot make a system or a product 100 percent secure. However, using checklists that emphasize hardening of systems against the hidden software flaws will typically result in greater levels of product security and protection from future threats (e.g., zero-day vulnerabilities). IT vendors that configure their products using checklists that adhere to the FISMA-associated security control requirements will provide more consistency in configuration settings within the federal agencies. This configuration will also provide a much more cost-effective method for establishing and verifying the minimum configuration settings, even if the agencies must modify the checklists to fine-tune the configuration settings for their specific applications and operational environments.

2.3 Overview of NIST National Checklist Program

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

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

- Facilitate development and sharing of checklists by providing a formal framework for vendors and other checklist developers to submit checklists to NIST
- Provide guidance to developers to help them create standardized, high-quality checklists that conform to common operational environments
- Help developers and users by providing guidelines for making checklists better documented and more usable
- Encourage software vendors and other parties to develop checklists
- Provide a managed process for the review, update, and maintenance of checklists
- Provide an easy-to-use repository of checklist information
- Provide checklist content in a standardized format
- Encourage the use of automation technologies for applying checklists.

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

2.4 Types of Checklists Listed by NCP

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

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

- **Non-Automated.** As the name implies, a non-automated checklist is one 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.

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

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

[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

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

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

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

3.1 Standalone Environment

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

3.2 Managed Environment

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

[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.

The Managed environment is more restrictive and provides less functionality than the Standalone environment. However, because of the supported and controlled[8] nature of the Managed environment, it is typically easier to use more functionally restrictive settings in Managed environments than in Standalone environments. Managed environments also tend to implement several layers of defense (e.g., firewalls, antivirus servers, IDSs, patch management systems, and email filtering), which provides greater protection for systems.

3.3 Specialized Security-Limited Functionality Custom Environment

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

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

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

3.4 Legacy Environments

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

[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.

3.5 United States Government Environment

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

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

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

4. Checklist Usage

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

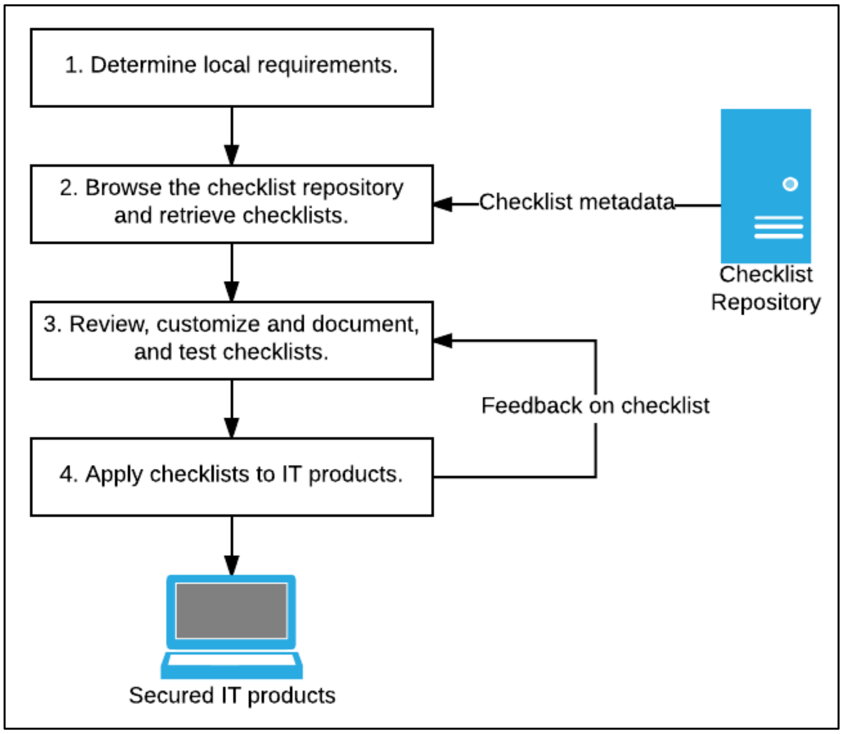
1. Determine local requirements.
2. Browse the checklist repository and retrieve checklists.
Checklist metadata
Checklist Repository
3. Review, customize and document, and test checklists.
Feedback on checklist
4. Apply checklists to IT products.
Secured IT products

Figure 1: Checklist User Process Overview

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

1. Users gather their local requirements (e.g., IT products, the operating environment, and associated security needs) and then acquire or purchase the IT product that best suits their needs.

2. Users browse the checklist repository to retrieve checklists that match the user’s operational environment and security requirements. If a product is intended to be secure by default, it is still important to check the NIST checklist repository for updates to that checklist.

3. Users review the checklists and select the checklist that best meets their requirements, then tailor and document the checklist as necessary to take into account local policies and functional requirements, test the checklist, and provide feedback to NIST and checklist developers.

4. Users prepare to deploy the checklist, such as making configuration or data backups, and then apply the checklist in production.

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

4.1 Determining Local Requirements

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

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

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

- **Identify Functional Needs.** What must the product do? Identifying upfront the end user's requirements, such as remote access for telecommuters or a web server to make internal information available to employees, is necessary to ensure that the security controls selected are appropriate; that is, that they implement an appropriate security solution and still allow the system to meet its requirements for functionality.
- **Identify Threats and Vulnerabilities.** A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. The goal of this step is to identify potential threat-sources that are applicable to the IT product or system being considered, as well as the vulnerabilities that could be exploited by the potential threat-sources.
- **Identify Security Needs.** The goal of this step is to determine the controls needed to minimize or eliminate the likelihood (or probability) of a threat exercising a product or system vulnerability. It answers the question, "What security features must the product provide?" Armed with this information, the organization can make wiser choices about which IT product best meets its needs.

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

4.2 Browsing and Retrieving Checklists

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

[9] https://nvd.nist.gov/

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

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

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

- **Prose.** Prose checklists provide narrative descriptions of how a person can manually alter a product's configuration.
- **Automated.** Automated checklists document their security settings in a machine-readable format, either standard or proprietary. An example is a product-specific configuration script. These checklists may include some elements of SCAP (for example, they may contain CCE [Common Configuration Enumeration] identifiers), but do not fully adhere to the SCAP specification.
- **SCAP Content.** SCAP content checklists adhere to the SCAP specification in NIST SP 800-126 for documenting security settings in machine-readable standardized SCAP formats. SCAP content checklists can be processed by SCAP-validated products, which have been validated by an accredited independent testing laboratory as conforming to applicable SCAP specifications and requirements. SCAP content that is available on the National Checklist Program repository has been evaluated with the NIST SCAP Content Validation Tool (SCAPVal)[10]. This evaluation ensures the checklist conforms to the SCAP specification. The SCAPVal tool does not evaluate the checklist for logic errors such as use of an "equal to" operator when "equal to or greater than" should have been used.

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

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

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

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

4.3 Reviewing, Customizing and Documenting, and Testing Checklists

Checklist users should download all documentation for the checklist and review it carefully. The documentation should explain any required preparatory activities, such as backing up a system. Because a checklist may not exactly match a user’s specific requirements, reviewing a checklist is useful in determining whether the checklist may need to be tailored[11] and whether the system or product will require further changes after applying the checklist.

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

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

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

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

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

4.4 Applying Checklists to IT Products

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

- Setting Modification
  - Even after reviewing and testing a checklist, users should handle deployment carefully to minimize any issues that might arise from applying the checklist.
  - For users who are unable to test a checklist in a non-operational environment (e.g., home users), it is important to carefully review the checklist documentation completely and to determine if an initial backup is required. The *Rollback Capability* field in the checklist description will indicate whether the results of applying the checklist can be reversed to return the product to its original configuration. Regardless of this setting, it is strongly recommended that a user back up the IT product’s configuration before installing the checklist recommendations.

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

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

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

4.5 Providing Feedback on Checklists

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

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

- Documentation
  - Does it explain the security objectives?
  - Does it contain a complete, clear, and concise description of the checklist settings?
- Recommended Practices
  - Are the checklist settings consistent with recommended practices?
  - Do the checklist settings take into account recent vulnerabilities?
- Impact of Settings
  - Has the checklist developer tested the checklist settings on the product in an operationally realistic environment and determined that the application of the checklist settings causes the product to meet the security objectives of the checklist?

[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.

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

5. Checklist Development

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

The checklist life cycle comprises the following steps:

1. **Initial Checklist Development:** The developer[14] becomes familiar with the procedures and requirements of the checklist program, and then performs the initial development of the checklist, including selection of a target environment.
2. **Checklist Testing:** The developer tests the checklist in the target environment and corrects any problems with the checklist.
3. **Checklist Documented:** The developer documents the checklist according to the guidelines of the program.
4. **Checklist Submitted to NIST:** The developer submits the checklist and documentation package to NIST for screening and public review.
5. **NIST Screening:** NIST screens the checklist package's information and confirms that any SCAP data stream content is well-formed, then addresses any issues with the developer prior to public review.
6. **Public Review and Feedback:** NIST holds a 30-day public review of the candidate checklist, then the developer addresses comments as necessary.
7. **Final Listing on Checklist Repository:** NIST lists the checklist on repository as final and announces the checklist's availability.
8. **Checklist Maintenance and Archival:** Anyone can provide feedback on the checklist throughout its life. The developer updates the checklist periodically as necessary. The checklist is archived when it is no longer being maintained or is no longer needed.

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

5.1 Developer Steps for Creating, Testing, and Submitting Checklists

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

5.1.1 Initial Checklist Development

During initial checklist development, a developer becomes familiar with the requirements of the checklist 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.

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

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

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

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

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

5.1.2 Checklist Testing

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

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

[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/.

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

5.1.3 Checklist Documented

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

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

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

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 *Authority Type*: *Authority*.
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.

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

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

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

5.1.4 Checklist Submitted to NIST

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

- Checklist and configuration files, templates, scripts, etc.
- Completed checklist description
- Checklist documentation
- Identification of the developer point of contact
- Signed participation agreement.

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

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

5.2 NIST Steps for Reviewing and Finalizing Checklists for Publication

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

5.2.1 NIST Screening of the Checklist Package

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

5.2.2 Public Review and Feedback for the Candidate Checklist

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

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

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

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

5.2.3 Final Listing on Checklist Repository

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

5.2.4 Checklist Maintenance and Archival

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

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

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

Appendix A. References

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

[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, *The Technical Specification for the Security Content Automation Protocol (SCAP)*, all versions available at http://csrc.nist.gov/publications/PubsSPs.html.
[5]	NIST Special Publication (SP) 800-27 Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), June 2004, https://doi.org/10.6028/NIST.SP.800-27rA
[6]	NIST Special Publication (SP) 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010 (updated 6/5/2014), https://doi.org/10.6028/NIST.SP.800-37r1
[7]	NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated 1/22/2015) https://doi.org/10.6028/NIST.SP.800-53r4
[8]	NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008, https://doi.org/10.6028/NIST.SP.800-115
[9]	Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, https://doi.org/10.6028/NIST.FIPS.199
[10]	Committee on National Security Systems (CNSS) Instruction No. 4009, *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015, https://www.cnss.gov/CNSS/issuances/Instructions.cfm

Appendix B. Checklist Program Operational Procedures

Operational Procedures for The NIST National Checklist Program for Information Technology Products

Version 1.4 (Draft)

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

This document is organized as follows:

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

The following terminology is used in this appendix:

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

- *Checklist* refers to a checklist for a specific product and version.
- *Checklist Developer* or *Developer* is an individual or organization that develops and owns a checklist and submits it to the National Checklist Program.
- *Independent Qualified Reviewers* are tasked by NIST with making a recommendation to NIST regarding public review or listing of the checklist. They work independently of other reviewers and are considered expert in the technology represented by the checklist.
- *Logo* refers to the NIST National Checklist Program logo.
- *National Checklist Program*, *Program*, or *NCP* is used in place of the NIST National Checklist Program for Information Technology Products.
- *NIST Checklist Repository* or *Repository* refers to the website that maintains the checklists, the descriptions of the checklists, and other information regarding the National Checklist Program.
- *Public Reviewer* is any member of the general public who reviews a candidate checklist and sends comments to NIST.
- *Operational Environments* refer to the operational environments outlined in this document.

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

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, https://doi.org/10.6028/NIST.FIPS.199
- NIST SP 800-27 Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), https://doi.org/10.6028/NIST.SP.800-27rA
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, https://doi.org/10.6028/NIST.SP.800-53r4
- Draft NIST SP 800-70 Revision 4, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, http://csrc.nist.gov/publications/PubsSPs.html

1. Overview and General Considerations

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

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

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

4. NIST forwards comments from public reviewers to the developer. The developer addresses the issues as appropriate, and the checklist is listed on the FCL, as discussed in Section 4.
5. NIST periodically reviews each final checklist to determine whether its listing should continue, be updated, or be archived, as discussed in Section 5.

(b) **Intellectual Property Rights:** Developers retain intellectual property rights to their checklists.

(c) **Confidential Information:** NIST does not anticipate the need to receive confidential information from checklist developers. If it becomes necessary to disclose confidential information to NIST, NIST and the developer must enter into a separate confidentiality agreement prior to such disclosure.

(d) **Independent Qualified Reviewers:** NIST may decide to seek technical advice from independent qualified experts who will review checklist submissions to determine whether they meet the program requirements. The reviewers are tasked with making a recommendation to NIST regarding a subsequent public review or final listing of the checklist. Typical but not exclusive of the reasons for using independent reviewers include the following:

1. NIST does not possess the expertise to determine whether issues have been addressed satisfactorily.
2. NIST disagrees with proposed issue resolutions.

(e) **Terminating Consideration of a Checklist Submission:** NIST or the developer may terminate consideration of checklist submissions at any time. If NIST terminates consideration, the points of contact are asked to respond within 10 business days. Typical but not exclusive of the reasons for terminating consideration of checklist submissions include the following:

1. The submission package does not meet the screening criteria.
2. The developer fails to address issues raised at other times.
3. The developer violates the terms and conditions of participation in the program.

2. Checklist Submission and Screening

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

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

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

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

2. The checklist, documentation, and description template.

3. The participation agreement, which must be printed, signed, and sent to NIST. NIST accepts emailed PDF copies of the participation agreement, facsimiles, or copies via regular mail.

4. Participation fees. Currently, there is no fee to checklist developers. NIST reserves the right to charge fees for participation in the future. Fees are not retroactive.

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

3. Candidate Checklist Public Review

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

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

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

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

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

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

4. Final Checklist Listing

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

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

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

(b) **Handling Comments:** NIST continues to accept comments about final checklists by maintaining a central email address on the repository, checklists@nist.gov. NIST lists the procedures to be used for contacting the developer, along with the contact information for the developer, such as an email address or URL. If at any time the point of contact changes, NIST must be notified immediately.

5. Final Checklist Update, Archival, and Delisting

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

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

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

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

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

6. Record Keeping

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

(a) **NIST Records:** During the period that a checklist has been submitted to NIST, and during the period that a checklist is listed on the FCL as a final or archived checklist, and for three years thereafter[18], NIST will maintain the following:

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

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

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

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

Appendix C. Participation and Logo Usage Agreement Form

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

NIST
National Institute of Standards and Technology

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD ™

Participation and Logo Usage Agreement Form
for
The NIST National Checklist Program for Information Technology Products

Version 1.5 (Draft)
August 1, 2017

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

1. You will follow the rules and requirements of the program as outlined in the NIST Operational Procedures for the NIST National Checklist Program (Appendix B of NIST SP 800-70 Revision 4).

2. You will respond to comments and issues raised by a public review of your checklist submission within 30 days of the end of the public review period. Any comments from reviewers and your responses may be made publicly available.

3. You agree to maintain the checklist and provide a timely response (within 10 business days) to requests from NIST for information or assistance with regard to the contents of the checklist.

4. You agree to maintain checklist-related records according to the requirements of the NIST National Checklist Program, as listed in Appendix B of NIST SP 800-70 Revision 4, item 6.b.

5. You will hold NIST harmless in any subsequent litigation involving the checklist submission.

6. You may terminate your participation in the NIST National Checklist Program at any time. You will provide two business weeks' notice to NIST of your intention to terminate participation. NIST may terminate its consideration of a checklist submission or your participation in the NIST National Checklist Program at any time. NIST will contact you two business weeks prior to its intention to terminate your participation. You may, within one business week, appeal the rejection and provide supporting evidence.

7. You may not use the name of NIST or the Department of Commerce on any advertisement, product, or service that is directly or indirectly related to this agreement. By accepting this agreement, NIST does not directly or indirectly endorse any product or service provided, or to be provided, by you, your successors, assignees, or licensees. You may not in any way imply that this agreement is an endorsement of any such product or service. You may not combine use of the logo with other Marks, phrases, or logos in such a way that would imply endorsement by NIST.

8. The phrase "NIST National Checklist Program for Information Technology Products" and the NIST National Checklist Program logo are Registered Marks of NIST, which retains exclusive rights to their use. NIST reserves the right to control the quality of the use of the phrase "NIST National Checklist Program for Information Technology Products" and the NIST National Checklist Program logo.

9. Your permission for advertising participation in the NIST National Checklist Program and use of the logo is conditional on and limited to those products and the specific product versions for which a checklist is made currently available by NIST through the NIST National Checklist Program on its Final Checklist List.

10. Your permission for advertising participation in the NIST National Checklist Program and use of the logo is conditional on and limited to those checklist developers who provide assistance and help to users of the checklist with regard to proper use of the checklist and that the warranty for the product and the specific product versions is not changed by use of the checklist.

11. Your use of the logo on product reports, letterhead, brochures, marketing material, and product packaging must be accompanied by the following: "TM: a Registered Mark of NIST, which does not imply product endorsement by NIST or the U.S. Government."

12. The dimensional requirements for the size, placement, color, and other aspects of the logo are specified in NIST SP 800-70 Revision 4.

13. NIST reserves the right to charge a participation fee in the future. No fee is required at present. No fees will be made retroactive.

14. NIST may terminate the NIST National Checklist Program at its discretion. NIST may terminate your participation in the Program for any violation of the terms and conditions of the program or for statutory or regulatory reasons.

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

Organization or company name:

Name and title of organization authorized person:

Signature:

Date:

Appendix D. Additional Requirements for USGCB Baselines

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

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

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

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

D.1.1 Initial Baseline Development

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

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

Developing a viable USGCB baseline requires expertise with the IT product and the ability to balance security and operational needs. During baseline development, discrete settings are defined, reviewed, and tested with the goal of arriving at a baseline that provides protection while allowing operational functionality. The champion agency should draw on field experience and available security configuration resources, such as government security guidelines, product security guidelines, and industry recommendations when developing baseline settings. Each baseline should be referenced to a security guide, such as a DISA STIG/checklist, an NSA security configuration guide, or a vendor security guide. Champion agencies should also engage the product vendor during the baseline creation phase to ensure supportability and applicability. After settings are selected, the champion agency considers how each setting functions (e.g., registry value or file version) and identifies available methods for assessing compliance or determining a setting's value. As the baseline is created, the developers will test the system's behavior when settings are changed (e.g., examine the registry value, daemon, or service status).

Each USGCB candidate must be expressed as SCAP content. NIST recommends producing SCAP at the current version of SCAP to take advantage of the latest specification features and SCAP product validation[19]. If the SCAP content is produced in a version other than the latest, the SCAP content must comply with the requirements of the revision of NIST SP 800-126 commensurate with the corresponding SCAP version, and the SCAP content must pass validation using the current version of the NIST SCAP Content Validation Tool (SCAPVal).

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

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

D.1.2 Baseline Testing

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

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

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

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

In addition to verifying baseline compliance with SCAP requirements, the champion agency should also test the baseline in an operational enterprise environment of considerable size that is representative of a typical Federal agency's operational enterprise environment. This testing ensures the viability of the baseline in an operational environment. NIST recommends testing the baseline for a minimum of three 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.

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

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

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

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

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

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

D.1.3 Baseline Documented

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

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

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

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

D.1.4 Baseline Submitted to NIST

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

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

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

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

D.2.1 NIST Screening of the Baseline Package

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

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

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

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

D.3 Field Testing Report Template

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

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

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

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	

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

Appendix E. Acronyms and Abbreviations

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

Appendix F. Glossary

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

Appendix G. Change Log

Revision 4 Release 0 – August 1, 2017

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

Revision 3 Release 1 – December 8, 2016

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