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

Special Publication 800-70
(DRAFT)

Sponsored by the Department of Homeland Security

Security Configuration Checklists Program for IT Products

Guidance for Checklist Users and Developers

Murugiah Souppaya
John P. Wack
Anthony Harris
Paul M. Johnson
Karen Kent

NIST Special Publication 800-70 (DRAFT)

Security Configuration Checklists Program for IT Products

National Institute of Standards and Technology

Murugiah Souppaya
John P. Wack
Anthony Harris
Paul M. Johnson
Karen Kent

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

U.S. Department of Commerce

Donald L. Evans, Secretary

Technology Administration

Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology

Arden L. Bement, Jr., Director

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 technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

This document is available for download at http://checklists.nist.gov.

Comments may be submitted to the Computer Security Division,
Information Technology Laboratory, NIST,
via electronic mail at checklists@nist.gov
Or via regular mail at

100 Bureau Drive (Mail Stop 8930)
Gaithersburg, MD 20899-8930

Acknowledgements

The authors, Murugiah Souppaya and John Wack of the National Institute of Standards and Technology, and Anthony Harris, Paul Johnson, and Karen Kent of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Timothy Grance, Jeffrey Horlick, Arnold Johnson, Mark Madsen, Edward Roback, Michael Rubin, and Ron Ross of NIST for their keen and insightful assistance throughout the development of its content. The authors would also like to express their thanks to Clint Kreitner of the Center for Internet Security, Chase Carpenter, Kurt Dillard, and Jesper Johansson of the Microsoft Corporation, Paul Bartock, Trent Pitsenbarger, and Neal Ziring of the National Security Agency, and Terry Sherald of the Defense Information Systems Agency (DISA).

The National Institute of Standards and Technology would also like to express its appreciation and thanks to the Department of Homeland Security for its sponsorship and support of the NIST Security Configuration Checklists Program for IT Products.

Table of Contents

List of Figures

List of Tables

Executive Summary

The National Institute of Standards and Technology (NIST), with sponsorship from the Department of Homeland Security (DHS), has produced *Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers* to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products.

A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular security level (or baseline). It could also include templates or automated scripts and other procedures. Typically, checklists are created by IT vendors for their own products; however, checklists are also created by other organizations such as consortia, academia, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems.

This publication is intended for users and developers of IT product security configuration checklists. For checklist users, this document gives an overview of the NIST Checklist Program, explains how to retrieve checklists from NIST's repository, and provides general information about threat models and baseline technical security policies for associated operational environments. For checklist developers, the document sets forth the policies, procedures, and general requirements for participation in the NIST Checklist Program.

The Cyber Security Research and Development Act of 2002 (Public Law 107-305) tasks NIST to "*develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government*." In addition, the Common Configuration Working Group Report of the Technical Standards and Common Criteria Task Force[1], formed at the Department of Homeland Security's first National Cyber Security Summit in 2003, recommended government promotion of the use of a NIST central repository for IT security configuration checklists. In response, this document has been developed by NIST in furtherance of its statutory responsibilities under the Cyber Security Act as well as the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347).[2]

WHY USE SECURITY CONFIGURATION CHECKLISTS?

There are many threats to users' computers, ranging from remotely launched network service exploits to malicious code spread through e-mails, malicious web sites, and file downloads. Vulnerabilities in IT products are discovered on an almost daily basis, and many ready-to-use exploits are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default, so many IT products are immediately vulnerable out-of-the-box. It is a complicated, arduous, and time-consuming task for even experienced system administrators to identify a reasonable set of security settings for many IT products.

[1] The final report of the Technical Standards and Common Criteria Task Force is available at http://www.cyberpartnership.org/TF4TechSummary.pdf.

[2] The full texts of the Cyber Security Act and the FISMA are available at http://csrc.nist.gov/policies/HR3394-final.pdf and http://csrc.nist.gov/policies/FISMA-final.pdf respectfully.

While the solutions to IT security are complex, one basic yet effective tool is the security configuration checklist. To facilitate the development of security configuration checklists and to meet the requirements of the Cyber Security Act, NIST has developed a program to (a) provide vendors and other groups with guidance for developing standardized, high-quality checklists to secure IT products, (b) establish a formal framework for the submission of checklists to NIST, and (c) assist users by making available a checklist repository.

Some of the benefits that organizations and individuals can achieve by using checklists are as follows:

- Providing a baseline level of security to protect against common and dangerous local and remote threats and a consistent approach to securing systems
- Significantly reducing the time required to research and develop appropriate security configurations for installed IT products
- Allowing smaller organizations to leverage outside resources to implement recommended practice security configurations
- Preventing public loss of confidence or embarrassment due to compromise of publicly accessible systems.

While the use of security configuration checklists can greatly improve overall levels of security in organizations, no checklist can permit a system or a product to become 100% secure. However, use of checklists that emphasize hardening of systems against flaws or bugs inherent in software will typically result in greater levels of product security and protection from future threats.

WHAT IS THE MOTIVATION BEHIND THE NIST PROGRAM?

Many organizations have created various checklists; however, these checklists may vary widely in terms of quality and usability, and may have become outdated as software updates and upgrades have been released. Because there is no central checklist repository, they can be difficult to find. They may not be well documented with the result being that one checklist may differ significantly from another in terms of the level of security provided. It may be difficult to determine if the checklist is current, or how the checklist should be implemented. While many existing checklists are of high quality and quite usable[3], the majority of checklists aren't accessible or directly usable by most audiences.

The goals of the NIST program are:

- To facilitate the development and sharing of security configuration checklists by providing a framework for developers to submit checklists to NIST
- To assist developers in making checklists that conform to common baseline levels of security
- To assist developers and users by providing guidelines for making checklists better documented and more usable

[1] [3] In addition to NIST, the National Security Agency (NSA), the Defense Information System's Agency (DISA) and the Center for Internet Security (CIS) produce high-quality checklists. The NSA's checklists are available at http://www.nsa.gov/ia/. The Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) are available for .mil and .gov domains at https://iase.disa.mil/techguid/stigs.html and, for other domains, at http://csrc.nist.gov/pcig/cig.html. CIS's site is http://www.cisecurity.org.

- To provide a managed process for the review, update, and maintenance of checklists
- To provide an easy-to-use repository of checklists.

NIST's program also serves to assist vendors in the process of making their checklists available to users out-of-the-box. In such cases, it will still be advisable for product users to consult the NIST checklist repository for updates to pre-installed checklists.

HOW DO USERS ACCESS THE CHECKLISTS?

NIST maintains a checklist repository containing the descriptions of the checklists, located at http://checklists.nist.gov. Users can search on the descriptions to locate a particular checklist using a variety of different criteria, including the product name, vendor name, and operational environment/category. This document contains procedures for checklist users to follow when retrieving checklists and applying them to IT products.

WHAT ARE THE COMMON SECURITY BASELINES?

NIST recognizes that checklists are significantly more useful when they follow common security baselines. The NIST Checklist Program identifies several broad and specialized operational environments, any one of which should be common to most audiences. By identifying and describing these environments, users can better select the checklists that are most appropriate for their operating environments and developers can better target their checklists to the general security baselines associated with the environments. The operational environments are:

- **Small Office/Home Office (**SOHO), sometimes called **Standalone**, describes small, informal computer installations that are used for home or business purposes. SOHO encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems located on broadband networks, to small businesses and small branch offices of a company.
- **Enterprise.** Enterprises are typically managed environments that are structured in terms of hardware and software configurations, usually consisting of centrally-managed workstations and servers protected from the Internet by firewalls and other network security devices. This environment is sometimes referred to as **Managed**.
- **High Security.** A High Security environment is at high risk of attack or data exposure, and therefore security takes precedence over usability. This environment encompasses computers that are usually limited in their functionality to specific specialized purposes. They may contain highly confidential information (e.g., personnel records, medical records, financial information) or perform vital organizational functions (e.g., accounting, payroll processing, web servers, and firewalls). A High Security environment could be a subset of another environment. Checklists for this environment are not recommended for home users.
- **Custom.** Custom environments contain specialized systems in which the functionality and degree of security do not fit the other environments. **Legacy** is a typical Custom environment; a Legacy environment contains older systems or applications that may use older, less-secure communication mechanisms. Other machines operating in a Legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. A Custom environment could be a subset of a SOHO or Enterprise environment.

HOW DO CHECKLIST DEVELOPERS USE THE PROGRAM?

The NIST Checklist Program provides a process and guidance for developing checklists in a consistent fashion. For checklist developers, steps include the initial development of the checklist, checklist testing, documenting the checklist according to the guidelines of the program, and submitting a checklist package to NIST. NIST then screens the checklist according to program requirements prior to a public review of the checklist, which typically lasts 30 to 60 days. After the public review period and any subsequent issue resolution, it will be listed on the NIST checklist repository (http://checklists.nist.gov) with a detailed description. NIST will periodically ask checklist developers to review their checklists and provide updates as necessary. NIST will retire or archive checklists as they become outdated or incorrect.

WHERE DO FISMA REQUIREMENTS FIT IN?

FISMA (section 3534(b)(2)(D)(iii)) [3] requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. Accordingly, Federal agencies, as well as vendors of products for the Federal government, are encouraged to acquire or implement and share such checklists using the NIST repository.

1. Introduction

A *security configuration checklist* (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of documented instructions for configuring a product to a pre-defined security baseline. It could also include templates or automated scripts and other procedures. Checklists can be developed for specific IT products and environments not only by IT vendors, but also by consortia, industry, Federal agencies and other governmental organizations, and others in the public and private sectors. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems.

This publication is intended for users and developers of IT product security configuration checklists. For checklist users, this document describes security configuration checklists and their benefits, and explains how to use the NIST Checklist Program to find and retrieve checklists. For developers, the document and its appendices describe the policies, procedures and general requirements for participation in the NIST Checklist Program.

It has become more important than ever to maintain secure networks and hosts. Widespread electronic attacks on all computer systems have become commonplace. There are many threats to users' computers, ranging from remotely launched network service exploits to malicious code spread through e-mails, malicious web sites, and file downloads. Vulnerabilities in IT products (e.g., operating systems, applications) are discovered on an almost daily basis, and many ready-to-use exploits are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security controls are usually not enabled by default, so many IT products are immediately vulnerable in their out-of-the-box configuration.

Complicating this situation is that today's systems and products can be very complex to administer and difficult to secure. For example, personal computer systems of today are far more complicated and sophisticated than yesterday's systems and many if not most users and administrators cannot be expected to manage them securely without assistance. It is a complicated, arduous, and time-consuming task for even experienced system administrators to know what a reasonable set of security settings is for many different IT products. However, security is very important to all audiences, from individual home users to large enterprise end-users, because all systems face threats. In some cases, home and telecommuter user systems may benefit from the same strong security controls usually found in larger organizations because they face common threats via use of the Internet.

While the solutions to IT security are complex, one simple yet effective tool is the security configuration checklist. To facilitate the development of security configuration checklists and to meet the requirements of the Cyber Security Research and Development Act of 2002 (Public Law 107-305) [1], NIST has developed a program with the following goals:

- To assist vendors and other groups with guidance for developing standardized, high-quality checklists
- To provide a formal program for the submission of the checklists to NIST
- To assist checklist users by making available a checklist repository.

For current or potential checklist users, this document provides an overview of the NIST checklist program and how to retrieve and use checklists. This publication describes the NIST checklist repository,

located at http://checklists.nist.gov. Users of the repository can check the availability of checklists for IT products they are using or considering for purchase, identify the differences between checklists developed for identical IT products, and find the locations where the checklists can be obtained.

For developers of checklists, this document provides an overview of using the program to build checklists and submit them to NIST. It describes how NIST will screen checklist submissions, how checklists will be listed and maintained, how issues will be addressed, and what the administrative requirements are for participation in the program and for use of the NIST Checklist logo.

1.1 Authority

The Cyber Security Act tasks NIST to "*develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government.*" In response, this document has been developed by NIST in furtherance of its statutory responsibilities under the Cyber Security Act as well as the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347 [3].

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III [4].

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired. Nothing in this document should be taken to contradict 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.

1.2 Audience and Assumptions

This document has been created for current and potential checklist users and developers in both the public and private sectors. Checklist developers include IT vendors, consortia, industry, Government organizations, and others in the public and private sectors. Checklist users include end-users, system administrators, and IT managers within Government agencies, corporations, small businesses, and other organizations, as well as private citizens.

Readers of this document are assumed to be familiar with general computer security concepts and for using web-based methods for retrieving information.

1.3 Document Organization

Section 2 contains an overview of checklists, and also describes the advantages of the NIST Checklist Program and how it works. It contains pointers to other sections of this document that provide greater detail.

Section 3 provides additional details of pre-defined checklist operational environments, threat models, and baseline technical security policies. These are used in the NIST Checklist Program to help developers create checklists that are consistent with these security policies. Checklist users can also apply the Section 3 material to better understand the baseline security policies and select the checklists that best match their own operational environments.

Section 4 contains information for potential checklist users. It describes how to use the NIST checklist program to find and retrieve checklists that best match the identified needs. It also contains guidance on implementing checklists, including analyzing the specific operating environment and then tailoring checklists as applicable.

Section 5 provides guidance to 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 contains references to documents used in this publication.

Appendix B describes the checklist description fields of the template used to catalogue checklists on the NIST repository.

Appendix C contains the programmatic and legal requirements that must be satisfied for participation in the NIST Checklist Program.

Appendix D contains the NIST Checklist Program participation and logo usage agreement form.

Appendix E contains a glossary for terms used in this document.

2. The NIST Security Configuration Checklists Program

This section contains an overview of the NIST Checklist Program. It begins by describing the contents of checklists and giving examples of the types of IT products for which checklists are often created. Next, the section explains the benefits that security configuration checklists can provide, such as improving baseline levels of security for an organization. It also explains the goals and benefits of the NIST Checklist Program, including increasing the quality, usability, and availability of checklists. This section also provides an overview of the procedures for checklist users and developers and the types of operational environments, as well as a summary of FISMA-related guidance pertaining to use of configuration checklists. Subsequent sections of the guide provide additional information on procedures and environment definitions.

2.1 What is a Security Configuration Checklist?

A *security configuration checklist* (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide (STIG), or benchmark[4]) is essentially a document that contains instructions or procedures for configuring an IT product to a baseline level of security. Checklists can be developed not only by IT vendors, but also by consortia, academia, and industry, Federal agencies and other governmental organizations, and others in the public and private sectors. A checklist might include any of the following:

- Configuration files that automatically set various security settings (e.g., executables, security templates that modify settings, scripts)
- 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 documents that set forth guidelines for such things as auditing, authentication mechanism (e.g., passwords), and perimeter security.

Not all instructions in a security configuration checklist need to be for security settings. Checklists can also include administrative practices for an IT product that go hand-in-hand with improvements to the product's security. Often, successful attacks on systems are the direct result of poor administrative practices such as not changing default passwords or failure to apply old patches.

Typically, a system administrator or end-user follows the instructions in the checklist to configure a product or system to the baseline level of security implemented in the checklist. The system administrator may need to modify the checklist to incorporate the local security policy.

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

- General purpose operating systems (e.g., Windows, Linux)
- Common desktop applications such as e-mail clients, web browsers, word processors, personal firewalls, and anti-virus software

[4] From herein, the Cyber Security Act terminology, *checklist*, will be used to describe a security configuration checklist or what other literature may refer to as a lockdown guide, hardening guide, or benchmark configuration.

- Infrastructure devices such as routers, firewalls, virtual private network (VPN) gateways, intrusion detection systems (IDS), wireless access points (WAP), and telecom systems
- Application servers such as Domain Name System (DNS) servers, Dynamic Host Configuration Protocol (DHCP) servers, Web servers, Simple Mail Transfer Protocol (SMTP) servers, File Transfer Protocol (FTP) servers, and database servers
- Other network devices such as mobile devices, scanners, printers, copiers, and fax appliances.

2.2 What Are the Benefits to Using Security Checklists?

Security configuration checklists, when developed correctly, can greatly assist users in configuring IT products to security baselines that offer more protection than the installed out-of-the-box defaults. The following list includes some of the benefits associated with using checklists:

- Providing a baseline level of security to protect against common and dangerous local and remote threats, e.g., viruses and worms, denial of service attacks, unauthorized access, inappropriate usage
- Significantly reducing the time required to research and develop appropriate security configurations for installed IT products by leveraging existing checklists with in-house expertise
- Allowing smaller organizations to leverage outside resources to implement recommended practice security configurations
- Preventing public loss of confidence or embarrassment due to compromise of publicly accessible systems

While the use of security configuration checklists can significantly improve overall levels of security in organizations, no checklist can permit a system or a product to become 100% secure. However, use of checklists that emphasize hardening of systems against the hidden flaws or bugs inherent in software will typically result in greater levels of product security and protection from future threats (e.g., zero day vulnerabilities).

2.3 The NIST Checklist Program

Many checklists have been produced over the years; however, these checklists may vary widely in terms of quality and usability, and may have become outdated as software updates and upgrades have been released. Because there is no central checklist database, they can be difficult to find. They may require close inspection to determine what they accomplish. Because there is no general agreement on security baselines for various environments, one checklist may differ significantly from another in terms of the level of security provided. While many existing checklists are of high quality and quite usable[5], the majority of checklists aren't accessible or directly usable by most audiences.

[5] In addition to NIST, the National Security Agency (NSA), the Defense Information System's Agency (DISA) and the Center for Internet Security (CIS) produce high-quality checklists. The NSA's checklists are available at http://www.nsa.gov/ia/. The Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS) are available for .mil and .gov domains at https://iase.disa.mil/techguid/stigs.html and, for other domains, at http://csrc.nist.gov/pcig/cig.html. CIS's site is http://www.cisecurity.org.

NIST's program serves to make checklists more organized and usable. The goals of the NIST program are as follows:

- To facilitate the development and sharing of checklists by providing a framework for developers to submit checklists to NIST
- To assist developers by providing a consistent approach to securing different types of systems that are connected to the same environments, e.g., a network consisting of Microsoft Windows®-based systems and Linux systems that need to be at the same security levels
- To assist developers and users by providing guidelines for making checklists better documented and more usable
- To provide a managed process for the review, update, and maintenance of checklists
- To provide an easy-to-use national repository of checklists.

2.3.1 Types of Checklists Listed by the NIST Checklist Program

The NIST Checklist Program deals with checklists that are tied to ***specific*** IT products, e.g., a checklist for a specific brand and model of a router. Some checklists may necessarily point to other checklists; for example, a checklist for a database product may reference checklist for the operating systems that the database product can run on.

The NIST Checklist Program can assist civilian Federal government agencies in meeting FISMA requirements, which is discussed more in Section 2.4. Additionally, the program can list checklists for a large variety of specialized needs,[6] such as checklists related to compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [5], or the Sarbanes-Oxley Act of 2002 [6].

The NIST checklist repository is located at http://checklists.nist.gov. The repository contains checklists that have been developed and screened to meet the requirements of the program. Users can search on a database of checklist descriptions to locate and retrieve a particular checklist using a variety of different fields, including the product name, vendor name, and operational environment.

2.3.2 Procedures for Users and Developers

The general steps involved for checklist users and developers are shown in Figure 2-1 and Figure 2-2. For checklist users, the steps are simple and straightforward:

- In step one, 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.
- In step two, users search the checklist repository to retrieve checklists that match the user's operational environment and security requirements. If a product is intended to be secure out-of-the-box (e.g., it was secured by the vendor using a security configuration checklist), it is still important to check the repository for updates to that checklist.

[6] The program does **not** list checklists that describe best practices for general technology areas, e.g., firewalls, routers, etc. NIST maintains several directories of best practices checklists, as well as links to locations for other checklists, at http://csrc.nist.gov/pcig/ppsp.html.

- Step three involves modifying and documenting the checklist as necessary to take into account local policies and needs, testing the checklist, and providing any feedback to NIST and the checklist developers.
- Lastly, step four involves preparation for deploying the checklist, such as making configuration or data backups, and then applying the checklist in production.

Section 4 contains more details on considerations associated with each step. The checklist description fields, used when performing checklist searches, are summarized in Appendix B.

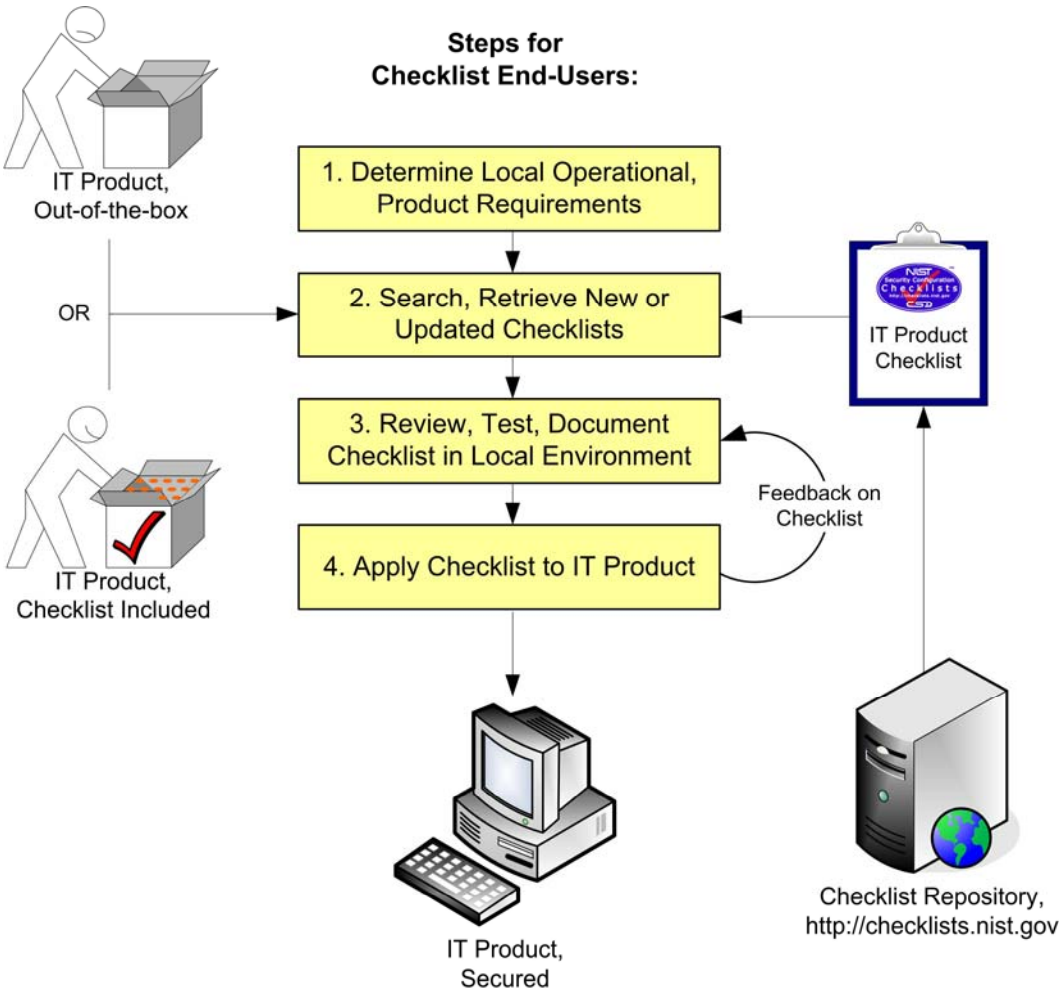

Figure 2-1: Steps for Checklist Users

For developers, the process is composed of two stages. The first stage involves only developer actions whereas the second stage involves interactions between NIST, the developer, and public reviewers. The first stage contains four steps, as shown in Figure 2-2:

- In step one, the developer becomes familiar with the procedures and requirements of the checklist program and completes an agreement to participate in the program.

- In step two, the developer creates, tests, and refines the checklist.
- In step three, the developer documents the checklist according to the guidelines of the program.
- In step four, the developer prepares a checklist submission package and submits it to NIST.

In stage two, NIST then performs the remaining four steps, with interaction from the developer and public reviewers:

- In step five, NIST screens the checklist according to program requirements and addresses any issues with the developer.
- The next step is a public review of the checklist, which typically lasts 30 to 60 days. Comments submitted during the review are addressed as applicable by the developer and NIST.
- For step seven, NIST posts the checklist on the repository and announces its presence.
- Lastly, step 8 involves periodic updates to the checklist and issues of checklist archival.

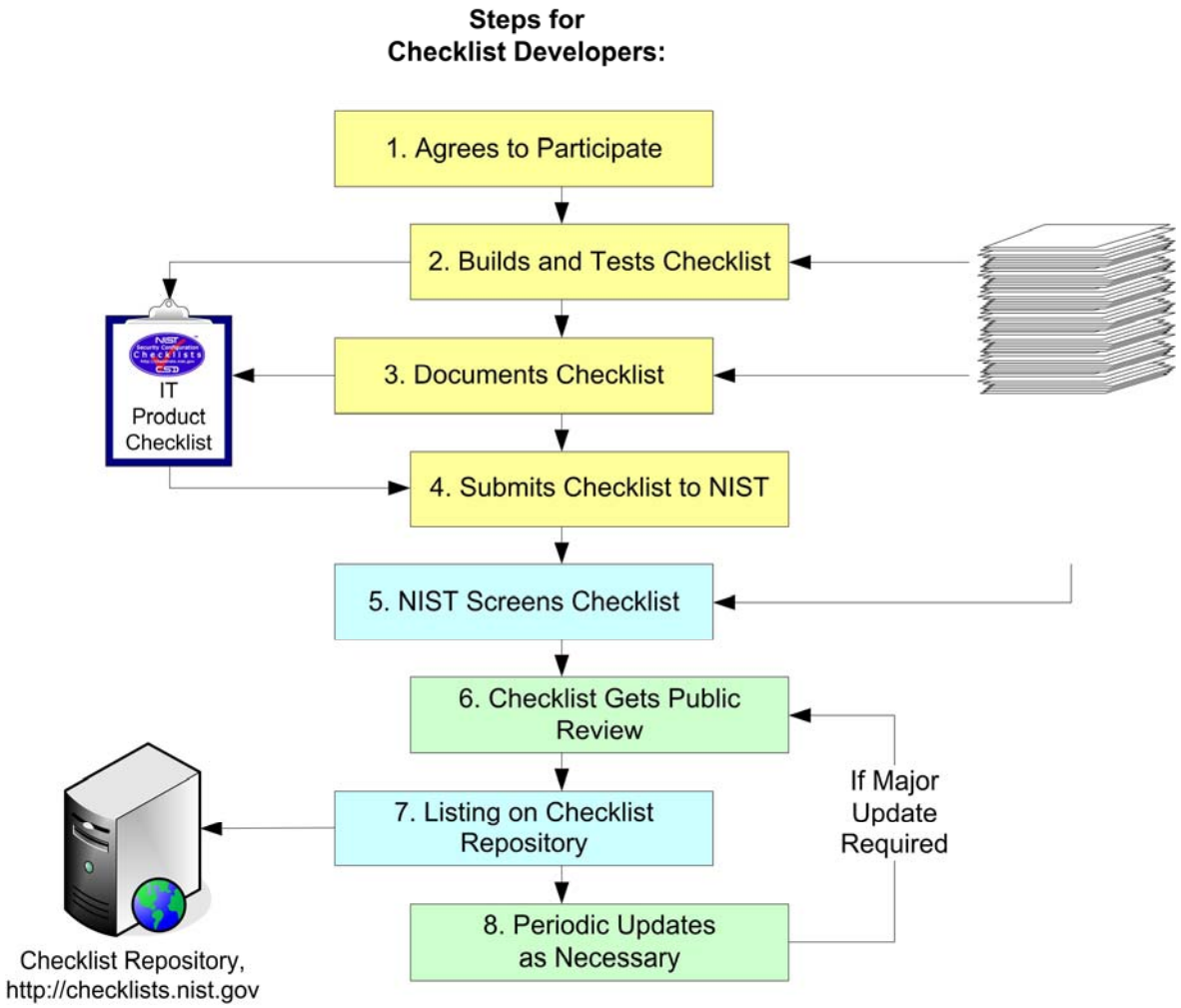

Figure 2-2: Steps for Checklist Developers

Checklist development procedures and NIST's process for screening and publishing the checklist are described in specific detail in Section 5 and Appendix C.

2.3.3 Common Security Baselines

NIST recognizes that checklists are significantly more useful when they follow common security levels (or *baselines*). However, it is difficult or perhaps impossible to specify these baselines in detail; they must by necessity remain general so as to be useful to a wide range of audiences. The NIST Checklist Program identifies several broad and specialized operational environments, any one of which should be common to most audiences. By identifying and describing these environments, developers can better target their checklists to the general security baselines associated with the environments. End-users can better select the checklists that are most appropriate for their operating environments.

The operational environments are as follows:

- **Small Office/Home Office (**SOHO), sometimes called **Standalone**, describes small, informal computer installations that are used for home or business purposes. SOHO encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems located on broadband networks, to small businesses and small branch offices of a company.
- **Enterprise.** Enterprises are typically managed environments that are structured in terms of hardware and software configurations, usually consisting of centrally-managed workstations and servers protected from the Internet by firewalls and other network security devices. This environment is sometimes referred to as **Managed**.
- **High Security.** A High Security environment is at high risk of attack or data exposure, and therefore security takes precedence over usability. This environment encompasses computers that are usually limited in their functionality to specific specialized purposes. They may contain highly confidential information (e.g., personnel records, medical records, financial information) or perform vital organizational functions (e.g., accounting, payroll processing, web servers, and firewalls). A High Security environment could be a subset of another environment. Checklists for this environment are not recommended for home users.
- **Custom.** Custom environments contain specialized systems in which the functionality and degree of security do not fit the other environments. **Legacy** is a typical Custom environment; a Legacy environment contains older systems or applications that may use older, less-secure communication mechanisms. Other machines operating in a Legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. A Custom environment could be a subset of a SOHO or Enterprise environment.

Figure 2-3 shows representative SOHO, enterprise, and high security/limited functionality environments. The environments and their general security baselines are further detailed in Section 3.

2.4 Checklists for Federal Agencies in Meeting FISMA Requirements

Security configuration checklists assist all audiences, particularly civilian Federal agency audiences that need to configure their systems so as to meet the security requirements of FISMA. FISMA (section 3534(b)(2)(D)(iii)) [3] requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. Accordingly, Federal agencies, as well as vendors of

products for the Federal government, are encouraged to acquire or develop and share such checklists using the NIST repository. The development and sharing of these checklists can greatly reduce what would otherwise be a "reinvention of the wheel" for IT products that are widely used in the Federal government, e.g., common operating systems and office applications.

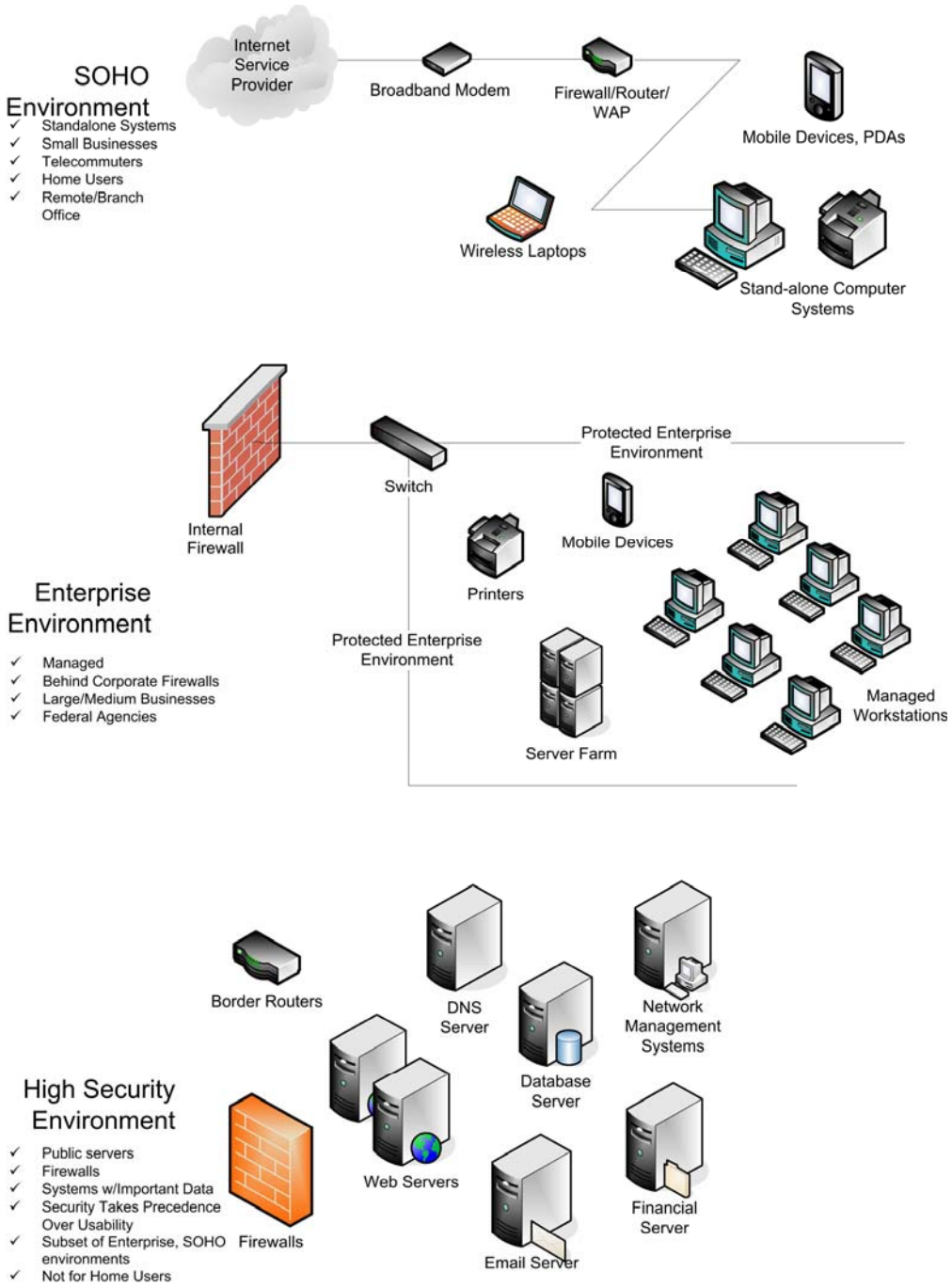

Figure 2-3: NIST Checklist Program Operational Environments

3. NIST Checklist Program Operational Environments

The NIST Checklist Program identifies several broad and specialized operational environments, any one of which should be common to most audiences. Each of the operating environments has a general threat model and baseline technical security policy.

Users of IT products may find this section useful to consult when initially identifying their own security requirements and needs (outlined in greater detail in Section 4). Developers may find this section useful when building checklists; by tailoring checklist development to these environments and their policies, they can create checklists for diverse products but still adhere to the general uniform technical security policies and settings associated with the environments. This is discussed in greater detail in Section 5.

The two broad environments are referred to respectively as **SOHO** (Small Office/Home Office) and **Enterprise**. The specialized environments, which could be found alone or within either of the broader environments, are **High Security** and **Custom** for systems and products that do not fit within the other environments (**Legacy** is a typical Custom environment). The following sections describe the environments and their general threat models and baseline technical security policies.

Prior to submission of a checklist to NIST, developers should ensure they have the most recent version of this document, as updates to the criteria for operational environments may occur periodically. The most recent version is available as a separate file at http://checklists.nist.gov.[7]

3.1 Background on the General Threat Models and Policies

To secure something, it is essential to first define the threats that need to be mitigated. This knowledge of threats is important to understanding the reasons the various baseline technical security policies have been chosen in this document.

The threat models described for each environment are not exhaustive; they simply represent the major threat categories that were considered during the selection of the environments and their associated baseline policies. Many threats against data and resources are possible because of mistakes—either bugs in operating system and application software that create exploitable vulnerabilities, or errors made by end-users and administrators. Threats may involve intentional actors (e.g., an attacker who wants to access information on a system) or unintentional actors (e.g., an administrator who forgets to disable user accounts of a terminated employee.) Threats can be local, such as a disgruntled employee, or remote, such as an attacker in another geographical area. Organizations using 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, then perform risk mitigation to decide what additional measures (if any) should be implemented, as discussed in NIST's *Risk Assessment Guide for Information Technology Systems* publication [12]. Performing this step permits organizations to better understand their needs and whether modifications or enhancements need to be made on any selected checklists.

The checklist environment baseline technical security policies are based on commonly accepted technical security principles and practices, catalogued in various NIST Special Publications [8], [10], [23] and other sources such as the DoD's *Information Assurance Technical Framework* [32]. In particular, NIST

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

Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* [11], contains a set of engineering principles for system security that provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. For additional information, Section 5.1 contains detailed discussion of the security-related criteria recommended for developers when building checklists.

3.2 SOHO Environment

The SOHO environment, sometimes referred to as **Standalone**, describes small, informal computer installations. This environment encompasses a wide variety of operational settings, from a home computer used for occasional work purposes to a small branch office of a company in another geographical area that is not managed remotely for technical or business reasons. Figure 3-1 shows a typical SOHO network architecture.

The SOHO environment assumes the following end-user audiences and operational settings:

- Home users with standalone systems, generally with dial-up or high-speed access to the Internet, possibly using wired or wireless home networks, possibly sharing resources across the networks
- Telecommuters using standalone systems who work from a home office
- Small businesses, typically with small networks of standalone desktop systems and small office servers protected from direct Internet access by a firewall, but possibly including some small centrally-managed networks of desktop systems and products, and typically not maintaining publicly-accessible servers
- Other small organizations with similar functions.

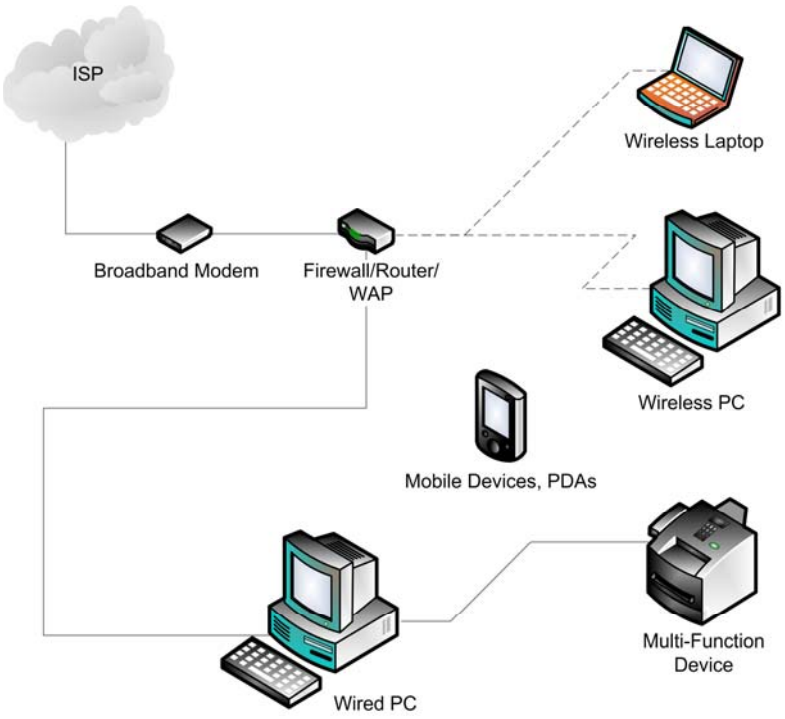

Figure 3-1: Home Office SOHO Environment Example

SOHO environments are typically the least secured. The individuals performing SOHO system administration are assumed to be less knowledgeable about security. This often results in environments that are less secure than they should be because the focus is on functionality. Also, there are often no network-based security controls such as firewalls, so SOHO systems may be directly exposed to external attacks. SOHO environments are frequently targeted for exploitation—not necessarily to acquire information, but instead for the purpose of attacking other computers, or incidentally as collateral damage from the propagation of a worm.

SOHO checklists should be relatively simple to understand and implement by home users or novice system administrators in small organizations.

3.2.1 Threat Model and Baseline Technical Security Policy

Because the primary threats in SOHO environments are external, and SOHO devices generally have less restrictive security policies than Enterprise or High Security systems, they tend to be most vulnerable to attacks from remote threat categories. Local threats are often less significant because few people typically have local access to SOHO systems; however, it is still important to protect against local and other threats. SOHO systems are typically exposed to attacks against network services and by malicious payloads (e.g., viruses, worms). These attacks are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) and confidentiality (e.g., providing remote access to sensitive data, e-mailing data files to others).

The baseline technical security policy for the SOHO environment includes protecting IT systems and products from the common out-of-the-box configuration vulnerabilities, blocking external access to the network, and restricting local access as possible. The adoption of inexpensive, hardware-based firewall routers and personal firewalls can help to better secure SOHO environments. Another key to SOHO security is strengthening the hosts on the SOHO network by patching vulnerabilities and altering settings to restrict unneeded services and applications. Some commonly accepted security practices for SOHO environments are:

- Use of small hardware firewall appliances at Internet connections to block inbound connections and possibly to filter outbound traffic also
- Use of personal firewall products on standalone systems
- Application (e.g., antivirus software, Web browser, e-mail client) and operating system updates and patches applied regularly
- Web and e-mail clients configured to filter and block traffic/messages that could contain malicious content
- Unnecessary applications disabled (e.g., personal Web servers, SNMP, messaging)
- Encryption used for wireless network traffic and as appropriate for other traffic
- Restrictions on which systems/users can connect to wired and wireless LANs
- Restrictions on user privileges
- Restrictions on sharing resources such as directories or printers
- Backup and recovery procedures
- Physical security procedures

NIST and other security publications can be consulted for additional guidance in security practices related to SOHO environments. Users may find the guidance on system administration for Microsoft Windows® systems [13], [26] telecommuting [14], and wireless network security [15] particularly useful. NIST has a variety of security-related special publications and general security guidance available on its computer security web site.[8]

3.3 Enterprise Environment

The **Enterprise** environment, sometimes referred to as **Managed**, is generally for centrally-managed networks of IT products protected from direct Internet access by firewalls. Figure 3-2 shows a typical enterprise network architecture. As an example, it would include networked printers and multi-function devices, managed workstations, and internal servers.

The Enterprise environment audience generally includes medium to large businesses, large governmental agencies, and organizations requiring managed telecommuting systems and remote offices. Enterprise checklists are generally intended for advanced end-users and system administrators in a medium to large organization. Enterprise environments typically have a group dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of typical Enterprise environments gives administrators centralized control over various settings on workstations, servers, and other types of devices, as well as the sharing of resources (e.g., file servers, printers). The enterprise enables only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management can also be administered centrally to maintain a consistent security posture across an organization.

3.3.1 Threat Model and Baseline Technical Security Policy

Remote and local threats to Enterprise networks could have significant impacts to systems and applications. Enterprise organizations often have systems with permanent, well-known IP addresses and name spaces with high visibility on the Internet to attackers. Most systems on enterprise networks are usually inward-facing—protected from direct exposure to the Internet by firewalls—but penetrations of those systems through other means could permit intruder access to internal networks. For example, viruses and worms could spread across homogenous networks in a short amount of time. Also, in Enterprise environments, the insider threat is generally greater due to the larger number of users.

The Enterprise environment is more restrictive and provides less functionality than the SOHO environment; however, Enterprise environments typically have better control on the flow of various types of traffic, such as filtering traffic based on protocols and ports at the enterprise's connections with external networks. Because of the supported and largely homogeneous nature of the Enterprise environment, it is typically easier to use more functionally restrictive settings in Enterprise environments than in SOHO environments. Enterprise environments also tend to implement several layers of defense (e.g., firewalls, antivirus servers, intrusion detection systems, patch management systems, email filtering), which provides greater protection for systems.

[8] NIST's computer security web site is located at http://csrc.nist.gov.

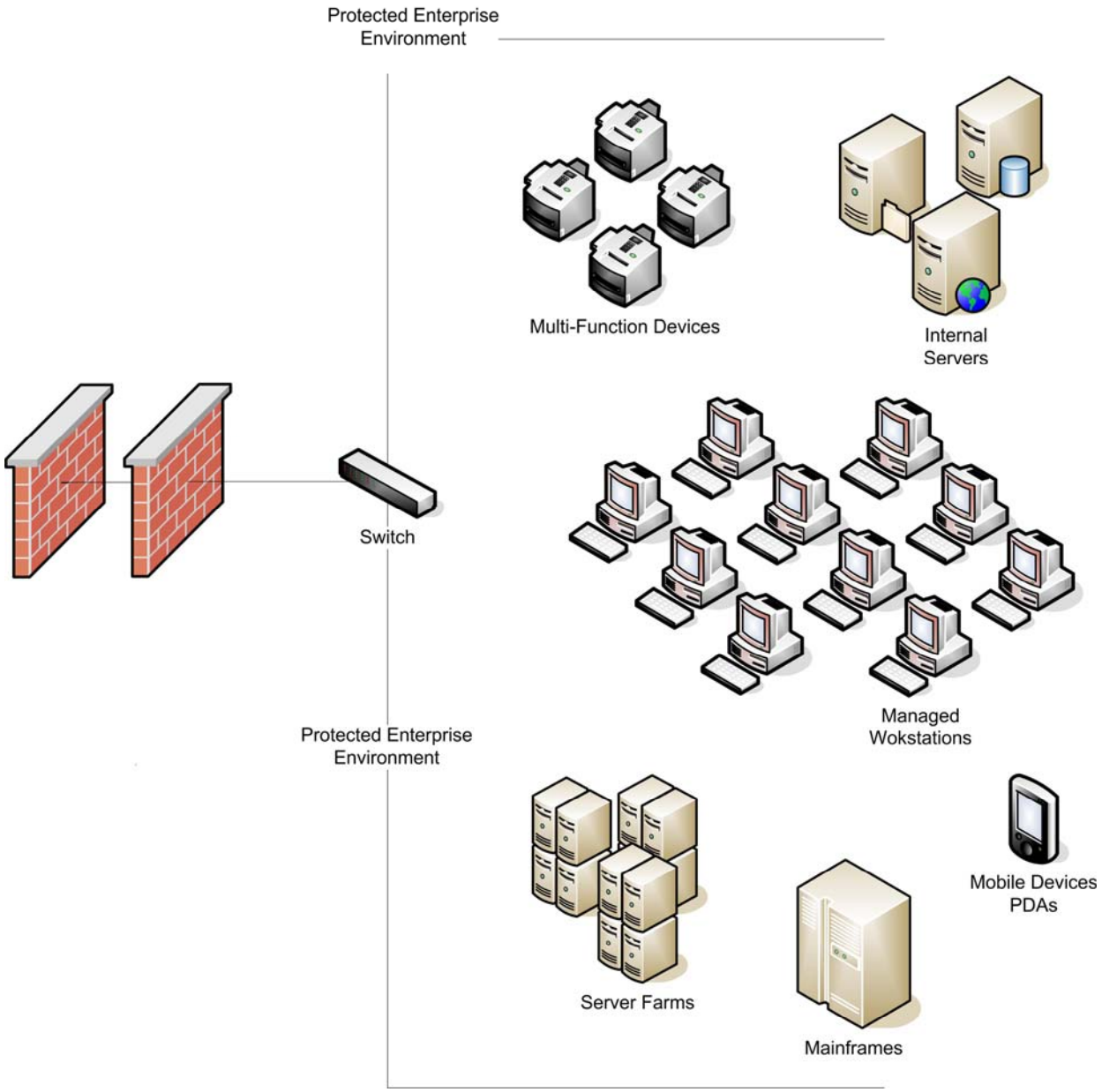

Figure 3-2: Centrally-Managed Enterprise Environment Example

In the Enterprise environment, systems are typically susceptible to local and remote threats. Local attacks, such as unauthorized usage of another user's workstation, most often lead to a loss of confidentiality (e.g., unauthorized access to data) but may also lead to a loss of integrity (e.g., data modification) or availability (e.g., theft of a system). Remote threats may be posed not only by attackers outside the organization, but also by local users who are attacking other local systems across the organization's network. Most security breaches caused by remote threats involve malicious payloads sent by external parties, such as viruses and worms acquired via e-mail or infected Web sites. Threats against network-based applications tend to affect a smaller number of systems and may be caused by internal or external parties. Both malicious payloads and network application attacks are most likely to affect

availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) or confidentiality (e.g., providing remote access to sensitive data). Data disclosure threats tend to come from internal parties who are monitoring traffic on local networks, and they primary affect confidentiality.

Some commonly accepted security practices for Enterprise environments are as follows:

- Segmented internal networks with internal firewalls and other defense in depth techniques
- Centralized management of systems with highly-restricted local user access
- Centralized management of security-related applications such as antivirus
- Automated installation of system and application patches and updates
- Restricted access to printer and multi-function devices and their features
- Centralized backup and recovery facilities.

Security publications can be consulted for additional guidance in security practices related to Enterprise environments. NIST has produced a variety of special publications particularly useful for the Enterprise operational environment. Relevant publications available from NIST's security web site include guidance for system administration of Microsoft Windows® systems [13], [26] wireless network security [15], active content and mobile code [16], security patches [18], firewalls [19], network security testing [20], and incident handling [25].

3.4 High Security Environment

The **High Security** environment is a highly restrictive and secure environment, networked or stand alone, usually reserved for systems that have the highest threats and associated impacts. Typical examples of such systems are outward-facing Web, e-mail, and DNS servers, other publicly accessed systems, and firewalls. It also encompasses computers that contain confidential information (e.g., personnel records, medical records, financial information) or perform vital organizational functions (e.g., accounting, payroll processing, air traffic control). These systems might be targeted by third parties for exploitation, but also might be targeted by trusted parties inside the organization.

A High Security environment could be a subset of another environment. For example, three desktops in an Enterprise environment that hold confidential employee data could be thought of as a High Security environment within an Enterprise environment. In addition, a laptop used by a mobile worker might be a High Security environment in a SOHO environment. A High Security environment might also be a self-contained environment outside any other environment, such as a government security installation processing sensitive data.

High Security checklists are intended for experienced security specialists and seasoned system administrators who understand the impact of implementing strict technical security policies. If home users and other users without deep security expertise attempt to apply High Security checklists to their systems, they would typically experience unwanted limitations on system functionality and possibly unrecoverable system damage.

3.4.1 Threat Model and Baseline Technical Security Policy

Systems in this environment face the same threats as systems in Enterprise environments. Although threats from insider attacks are still a large concern, the primary attack vector is likely to be external. Systems may be directly connected to the Internet, and as in the Enterprise environment, may have permanent, well-known IP addresses and name spaces with high visibility to attackers. Systems may be subject to automated intrusions and denial of service attacks, as well as manual intrusions. Penetrations of firewalls and servers could lead to local attacks and intrusions. Local threats may be high if the systems are connected to large networks with many users, or may be less if connected to smaller networks. Because of the risks and possible consequences of a compromise, this environment usually has the most functionally restrictive and secure configuration. The suggested configuration provides the greatest protection with considerable tradeoffs to ease of use, functionality, and remote system management.

It is difficult to specify baseline technical security policy except in very general terms because many disparate types of systems/applications could, depending on how they are used, qualify as High Security. However, the following general practices and controls are likely to be applicable:

- Systems should generally process as few types of data as possible (e.g., do not combine multiple server applications on the same system)
- Systems should be stripped of all unnecessary services and applications
- If possible, host-based firewall applications should be used
- Systems should have as few users as needed
- The strongest possible authentication should be used (e.g., authentication token, biometrics, smart cards)
- Remote administration or access should be restricted; if used, connections should be encrypted
- Security-related operating system and application patches and updates should be tested and applied as soon as possible
- Systems should be placed behind firewalls and other network security devices that restrict access and filter unnecessary protocols
- Intrusion detection and other logs should be monitored on a frequent basis
- Vulnerability assessment tools should be run against the systems on a frequent basis
- System administrators should be highly skilled in the appropriate technologies.

NIST and other organizations have recommended security practices for firewalls [19], web servers [21], and email servers [22]. The publications mentioned previously for the SOHO and enterprise environments also should be consulted for detailed recommendations.

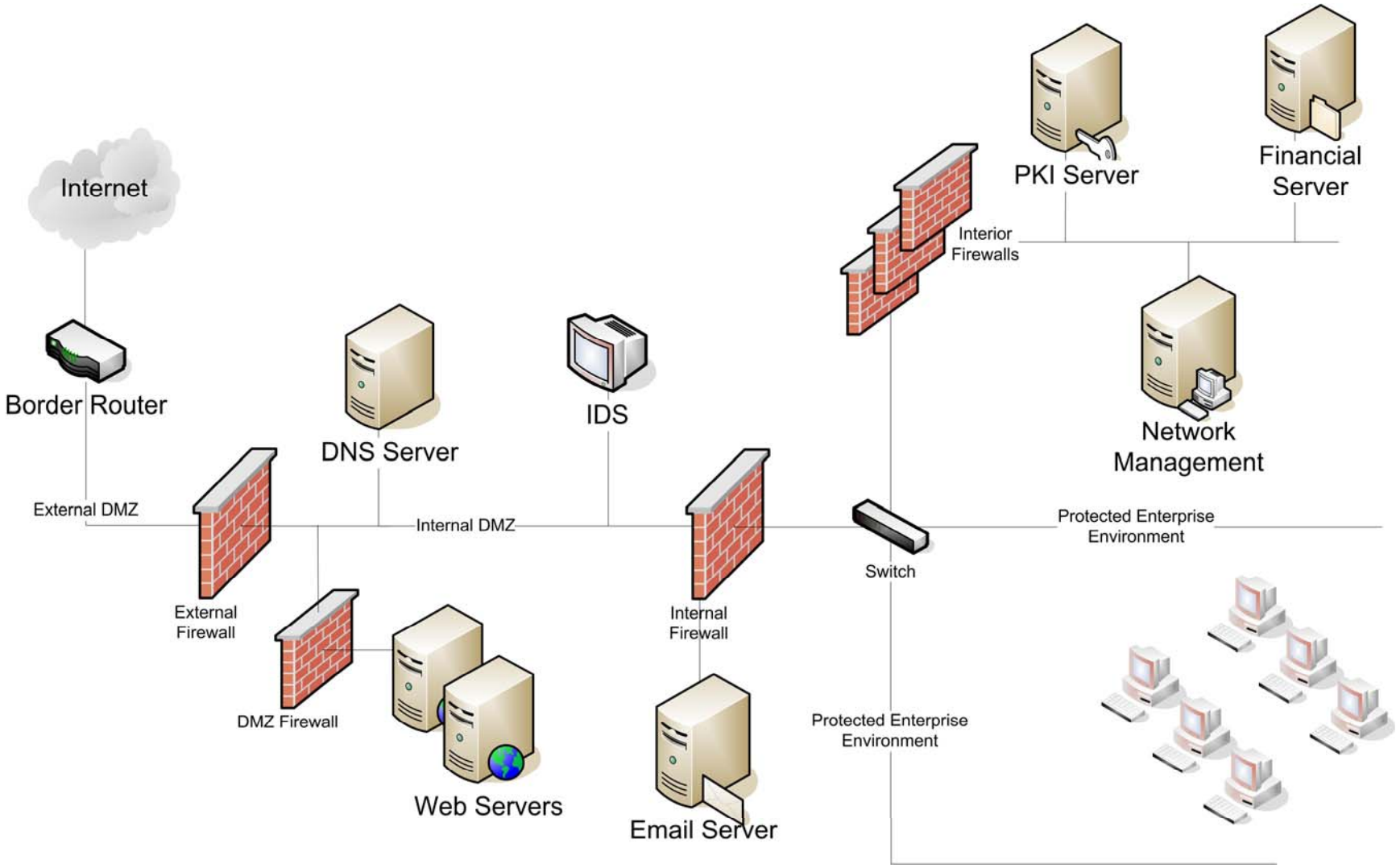

Figure 3-3: Typical High Security Environment

3.5 Custom Environments

Custom environments do not fit into the other predefined environments. They apply to an implementer's defined environment and assume a specialized security target to satisfy the user's specific operational environment. Depending on the situation, a Custom environment may face any combination of local and remote threats. The potential impact of the threats should be determined by considering the threats that the system faces and then considering what additional risk the system has because of the custom accommodations.

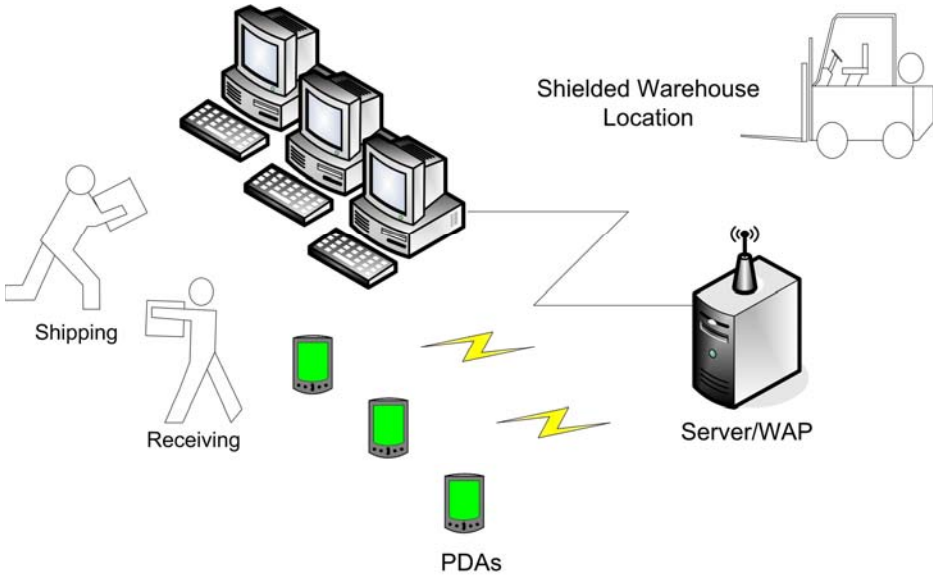

Figure 3-4: Custom Environment Example

An example of a Custom environment is shown in Figure 3-4. Warehouse workers use wireless PDA devices to collect inventory for shipping and receiving. The PDAs cannot be inexpensively upgraded to support wireless protocols with encryption (e.g., WEP or WPA). However, the location and structure of the warehouse prevents easy intercepts of the wireless traffic. Due to cost considerations, a risk determination was made and a Custom environment checklist was created for the server/wireless access point.

Legacy is a typical Custom environment for situations in which legacy systems may need to be combined with newer equipment and secured to meet today's threats. Again, the threat model can vary widely. Figure 3-5 shows a simple example of a legacy environment in which older workstations must be part of a network using more recent server technology. The older workstations cannot support newer, more robust aspects of the newer technology, such as a more secure file sharing protocol, file system, or authentication protocol. Consequently, modifications need to be made to support the legacy workstations. In this case, the server would require a legacy checklist.

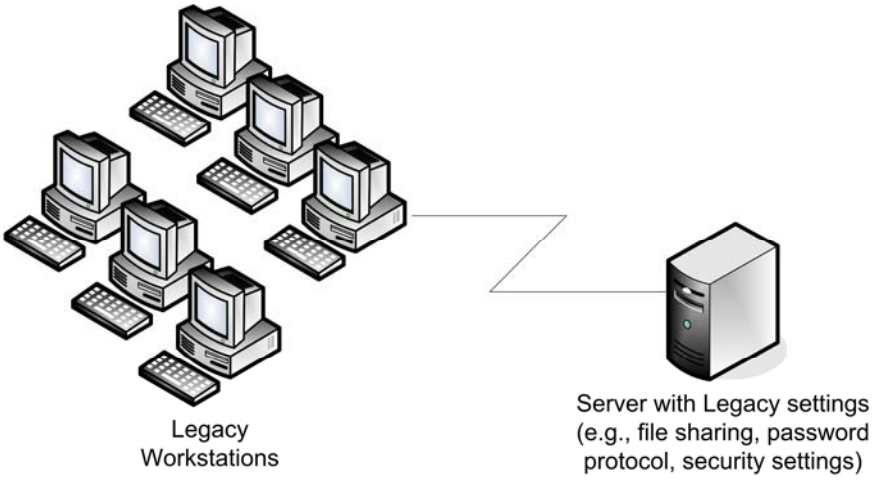

Figure 3-5: Legacy Workstation Environment

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 at large organizations, have their specific requirements, the process described here will apply to most situations. This section includes guidance on conducting an initial analysis of local environment threats and risks, and the impacts if threats were to occur. It then describes a process for selecting and retrieving checklists from the NIST checklist repository, and recommends steps for analyzing and applying the checklist.

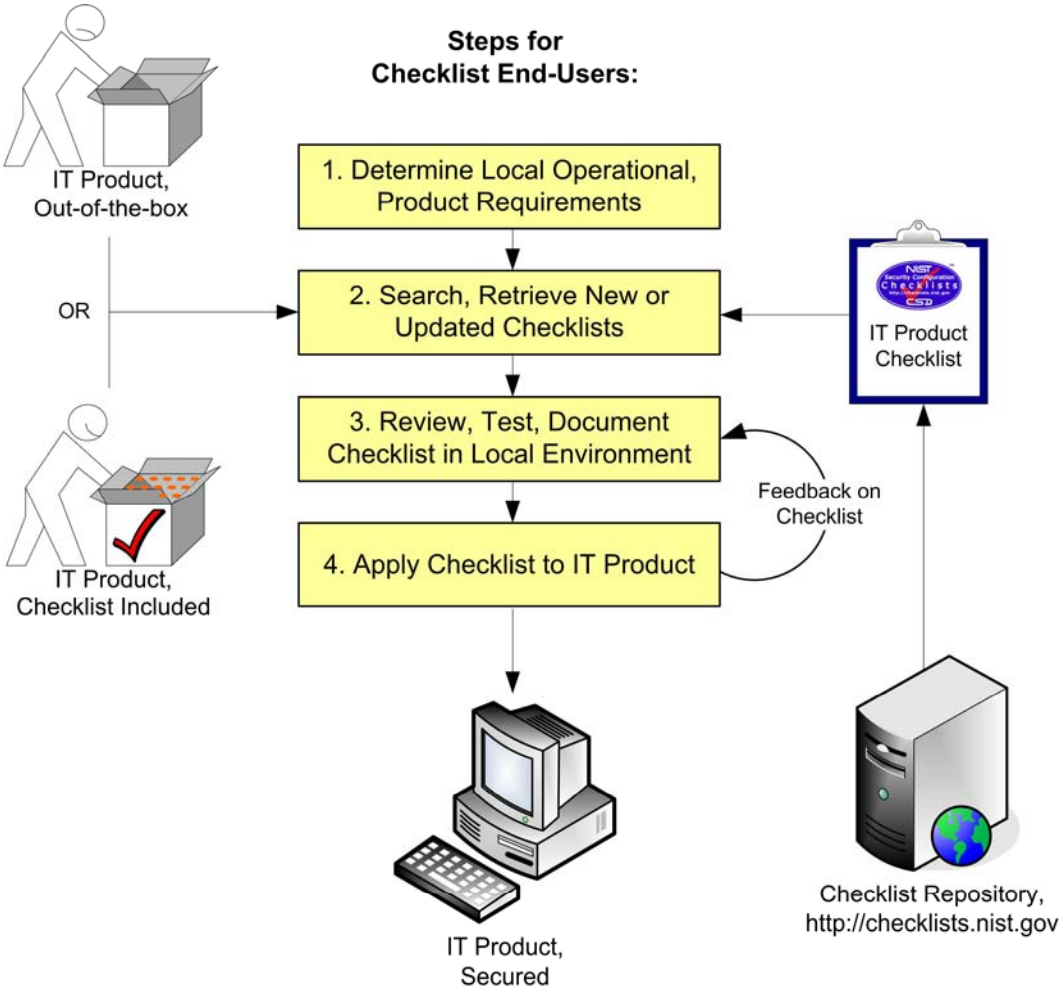

Figure 4-1: Checklist User Process Overview

Figure 4-1 shows the general process for using checklists. In step one; a prospective checklist user analyzes local requirements and security needs or policy and identifies the appropriate operational environment model. The user then selects the IT product that best matches the needs. In step two, the user searches the repository for checklists that match the IT product and the selected operational environment (and possibly other criteria, such as whether the checklist can be rolled back or whether it's supported by the product vendor). The user downloads the checklists along with any supporting documents and tools. In step three, the user reviews the downloaded checklists and tests them and

customizes to reflect local policy and functionality as needed. Feedback on the checklists can be sent to NIST and the developer via the repository. In step four, the user prepares to apply the checklist in production by backing up information that might be affected if the application of the checklist isn't successful or causes unanticipated problems. Finally, the checklist can be applied to production systems. The following sections describe each of these steps in more detail.

4.1 Determining Local Requirements

Organizations usually conduct a requirements analysis before actually selecting and purchasing a particular IT product. The analysis would include an identification of 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. Since, security is difficult to add later, assessing requirements upfront is a better method for incorporating security into IT operations, big or small.

NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems* [12], contains useful guidance for Federal agencies on conducting a requirements analysis and a subsequent risk assessment. Organizations use risk assessments to determine the extent of the potential threat and the risk associated with an IT system or product throughout its lifecycle. The output of this process helps to identify appropriate controls for reducing or eliminating risk. (Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization.) Organizations other than Federal agencies can also benefit by following the methodology in SP 800-30.

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

- **Identifying 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 so that the appropriate security controls can be selected that implement an appropriate security solution and still meet the requirements for functionality.
- **Identifying 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.
- **Identifying Security Needs.** The goal of this step is to determine the controls needed to minimize or eliminate the likelihood (or probability) of a threat's 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 as to which IT product best meets their needs.

Federal agencies conduct formal requirements analysis and risk assessments as outlined in SP 800-30. For any organization or individual, the threat models and general security policies associated with each operational environment in Section 3 can assist in identifying threats and vulnerabilities, and recommended baseline security policies. For example, a home user could study the discussion in Section 3 on the SOHO operational environment prior to purchasing a product (assuming that the home user's

environment matches up well with SOHO). Given that the home user understands their requirements and what type of product they wish to acquire, the home user can use the SOHO environment's security model and general baseline policy to make an informed choice as to which product best meets their needs.

NIST has also written several documents and guides to assist Federal agencies when selecting information security products and for the acquisition and use of tested/evaluated products [10], [17]. Another key resource available at NIST for identifying vulnerability-related information about IT products is the ICAT tool.[9] This tool provides a product by product index to identified system vulnerabilities and information on patches available to correct the vulnerabilities.

4.2 Searching and Retrieving Checklists

After determining local requirements and identifying an IT product, a checklist user is ready to perform a search of the NIST checklist repository. Figure 4-2 shows a sample search page.

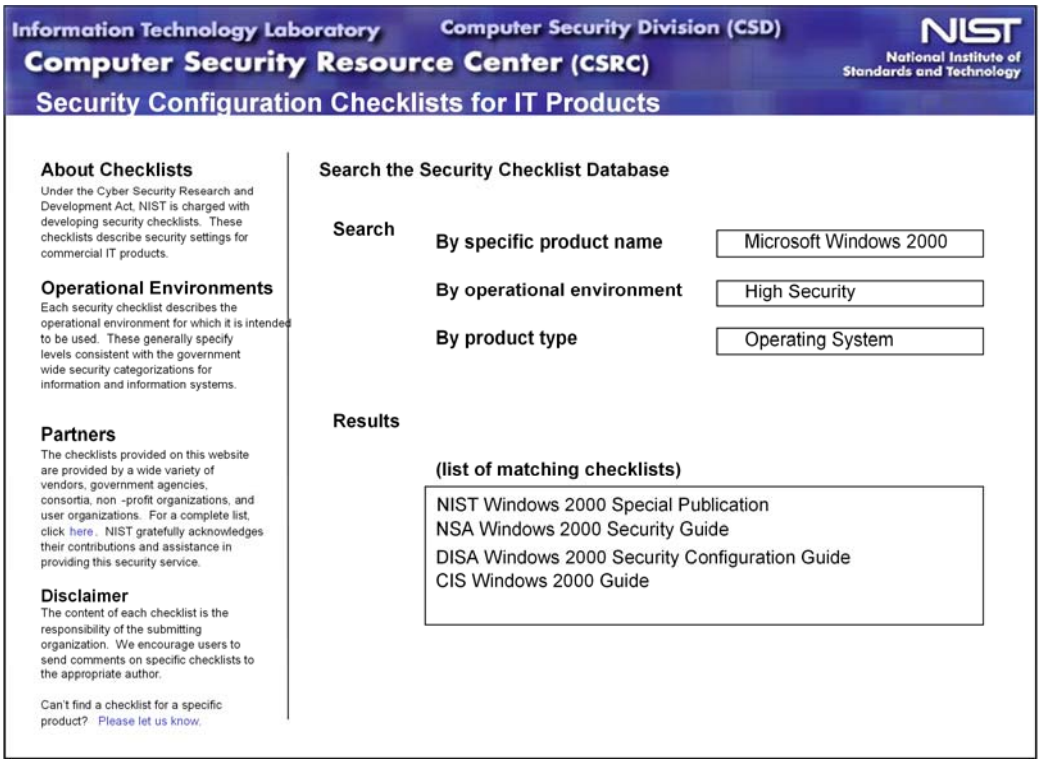

Figure 4-2: NIST Checklist Repository Search Page

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 (the listing and definition of all the fields used to describe each checklist is in Appendix B). Depending on a user's needs, role, and skills (e.g., home user, enterprise administrator), some fields in the description will be more important than others. Table 4-1 lists fields that should be helpful to all users in determining whether the checklist meets their specific needs.

[9] The ICAT tool can be found at http://icat.nist.gov.

Table 4-1: Checklist Description Fields

Field Name	Description
CHECKLIST SUMMARY	Summarizes the purpose of the checklist and its settings.
CHECKLIST STATUS	Whether Candidate, Final, or Archived. NIST will fill in this field.
CHECKLIST VERSION	Indicates the version or release number of the checklist.
COMMENTS, WARNINGS, DISCLAIMER, MISCELLANEOUS	Any additional information that the checklist developer wishes to convey to users.
CHECKLIST LATEST REVISION DATE	States the date when the checklist was last revised, in the format CCYY-MM-DD. NIST will fill in this field.
PRODUCT MANUFACTURER NAME	Contains the name of the manufacturer of the IT product.
CHECKLIST POINT OF CONTACT	Provides an e-mail 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.
PRODUCT CATEGORY	The main product category of the IT product, e.g. firewall, IDS, operating system, web server, etc.
PRODUCT NAME	The official IT product name.
PRODUCT ROLE	Specifies 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, etc.
PRODUCT VERSION	The specific software or firmware released version number of the IT product, including service pack or patch level as appropriate.
CHECKLIST ROLLBACK CAPABILITY	Whether the changes in product configuration made by applying the checklist can be rolled back and, if so, how to rollback the changes.
SUBMITTING ORGANIZATION/ AUTHORS	The name of the organization and authors that produced the checklist.
CHECKLIST TARGET AUDIENCE	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.
CHECKLIST TARGET ENVIRONMENT	The IT product's operational environment, e.g. SOHO, Enterprise, High Security, or Custom (with description).
TESTING PROCEDURES	Platforms on which checklist was tested. Can include any additional testing-related information such as summary of testing procedures used.
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 Checklist Program logo.

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 preparation activities, such as backing up a system. Because a checklist will not match exactly the user's specific requirements, the review is useful in determining whether the checklist may need to be modified or if the system or product will require further modifications after applying the checklist.

For larger organizations, the review can identify the impact on their current policies and practices if a given security checklist is implemented (e.g., a checklist that turns off JavaScript in a browser might make some web pages unusable). An organization may determine that some aspects of the checklist do not conform to certain organization-specific needs and requirements. Because the checklist may be applied many times over 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, any changes to the checklist should be documented for future reference. Feedback can be sent to NIST as well as the checklist developers; feedback is especially important to developers in gauging whether the checklist is written well and the settings are applicable to the targeted environment.

Before applying a checklist, users should first test it on non-critical systems, preferably in a controlled non-operational environment (albeit testing may be difficult for home or small business users who do not have extra systems and networks for testing purposes). 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, 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.

4.4 Applying Checklists to IT Products

Each checklist will include specific installation instructions to assist with deployment. Even after review and testing, users should handle deployment carefully to minimize any issues that might arise from applying a security checklist.

For users unable to test a checklist in a non-operational environment (e.g., home users), it is all the more important to carefully review the checklist documentation completely and determine whether an initial backup is required or a good idea. The *Rollback Capability* field within the checklist description (see Table 4-1) will indicate whether the checklist can be reversed, returning the product to the original configuration. Regardless of this setting, backing up the IT product's configuration prior to installing the checklist recommendations is generally recommended.

Users should minimally back up all critical data files in their computing environment. If possible, a full backup of the system should be made in the event they need to restore the system to a state prior to implementing the checklist. (This is actually a recommended practice before making any major system change and is not specific to applying 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 prior to enterprise-wide deployment.

Depending on the product, a checklist may be updated periodically or frequently, and NIST may maintain a mailing address for selected checklists. Users who subscribe will receive announcements of updates or other issues connected with a checklist. The selected checklist's description on the checklist repository will contain subscription instructions.

NIST welcomes all feedback, bug reports, comments, or suggestions from checklist users in regards to individual checklists or the repository itself. Where applicable, NIST will encourage feedback from checklist users so that the developers are better able to gauge the effectiveness and appropriateness of the checklist.

5. Checklist Development

This section describes the general process of developing security configuration checklists and submitting them to the NIST Checklist Program. It includes an overview of the process NIST will follow to screen the checklist submission and publish them on its repository, and the process NIST and developers will follow for eventual updates to the checklist or checklist archival. Individual developers and organizations that wish to submit checklists to NIST should review the appendices of this document, which contain the administrative requirements for the NIST Checklist Program. Prior to submission of 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 http://checklists.nist.gov.

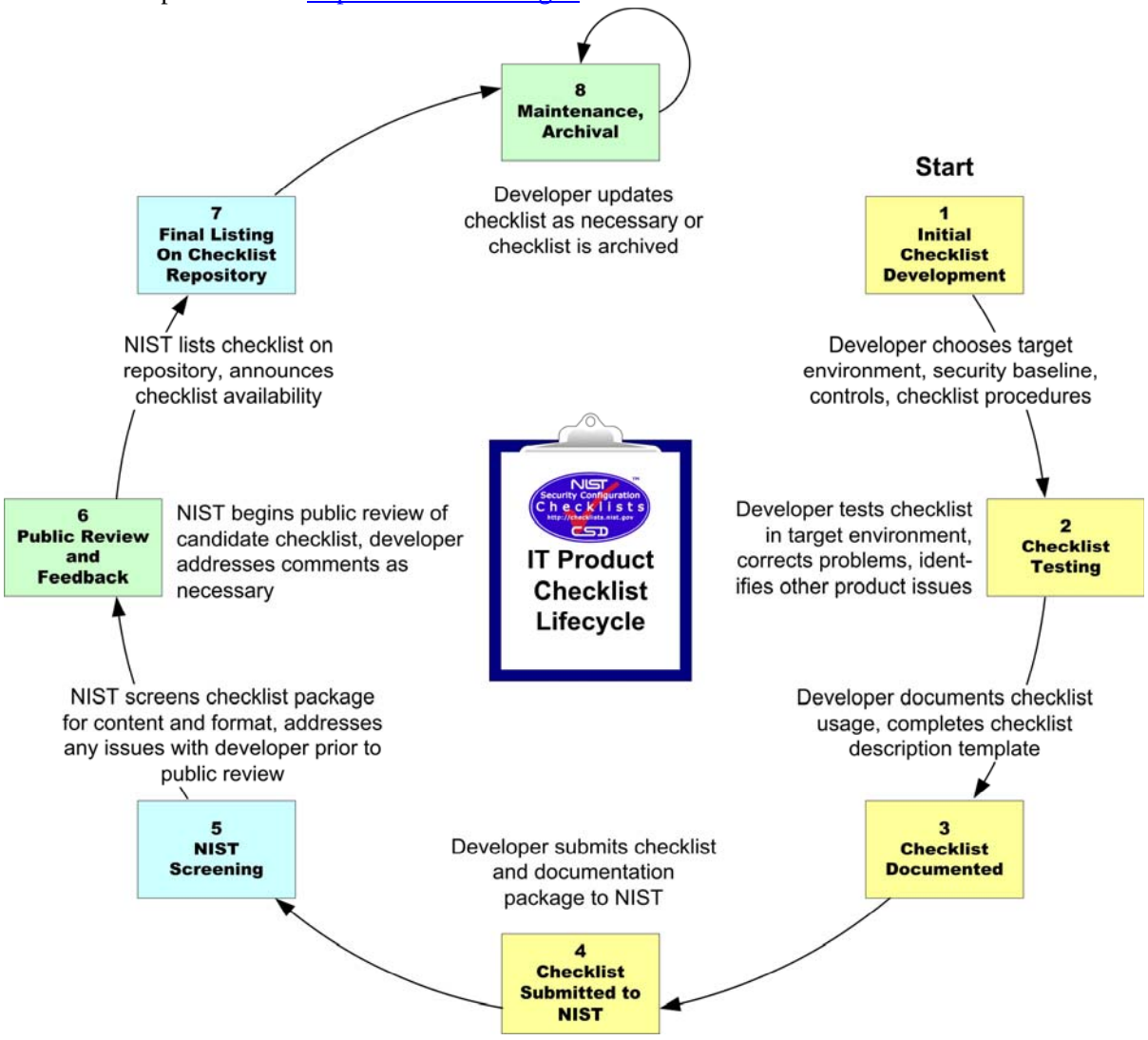

Figure 5-1: NIST Checklist Program Development Steps

The lifecycle steps shown in Figure 5-1 are straightforward. Each step should be followed so that the checklist is accurate, tested, and documented during its development and subsequent publication, update, or archival. The following sections describe considerations for each step.

5.1 Background on Security-Related Criteria for Checklists

This section discusses the security-related criteria that NIST recommends developers follow so that baseline technical security policies in checklists are more consistent. NIST recognizes that detailed checklist development cannot be covered in detail in this document. Therefore, NIST has based the security-related criteria on commonly accepted technical security principles and practices, catalogued in NIST Special Publication 800-53 [23], other NIST publications [8], [10], and other literature [32]. Additional considerations are contained in NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* [11]. To aid in designing a secure information system, NIST compiled a set of engineering principles for system security discussed in this document. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed. SP 800-27's guidance is based in part on the *Information Assurance Technical Framework (IATF)* [32].

The checklist needs to be consistent with one of the general security baselines described in Section 3 (excepting the Custom environment). This will require consulting the guidance in Section 3, the checklist format and content guidelines in the remainder of this section and in Appendix C, and other generally recommended practices and procedures. If no recommended practices guidance is yet available for a product or class of products, general security recommended practices should be used (e.g., defense in depth and layered security; least privilege, confidentiality, integrity, and availability controls).

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 DHS US-CERT, the CERT®/CC, and NIST's ICAT.[10] The security objectives should be consistent with recognized checklist-producing organizations including NIST [13], [26], **Error! Reference source not found.**, the National Security Agency (NSA) [36], the Security Technical Implementation Guides (STIG) produced by the Defense Information Systems Agency (DISA) [37], and the Center for Internet Security (CIS) benchmarks [38].[11]

Developers of checklists for products that will be used in the Federal government may wish to consult the FISMA-associated security control baselines first, as discussed earlier in Section 2.4. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* [23], is a catalog of security-related controls; it uses groupings of the controls to create three minimum baseline management, operational, and technical security control sets for Federal systems—low, moderate, and high impact as specified in FIPS 199 [27]. By default, Federal systems will require the low control set. It may be useful for developers of checklists aimed towards the Federal government to build checklists that are consistent with the applicable controls in SP 800-53. Note, however, that checklist consistency with the FISMA requirements, while useful, is optional. Checklists can be geared towards other regulatory requirements, including the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [5], or the Sarbanes-Oxley Act of 2002 [6].

[10] The DHS US-CERT's site is http://www.us-cert.gov/. The CERT®/CC's site is http://cert.org. The ICAT tool can be found at http://icat.nist.gov.

[11] The NSA's checklists are available at http://www.nsa.gov/ia/. DISA's STIGS are available at http://csrc.nist.gov/pcig/cig.html. CIS's site is http://www.cisecurity.org.

5.2 Developer Steps for Creating and Submitting Checklists

The first four steps in of the development methodology (from Figure 5-1, summarized below in Figure 5-2) begin with the developer becoming familiar with the procedures and requirements of the checklist program, and then performing the initial development of the checklist. From there, the developer tests the checklist and refines it as needed. The third step involves documenting the checklist according to the guidelines of the program. Finally, the developer prepares and submits a checklist submission package to NIST for screening and public review. The sections below describe various considerations in each of these steps.

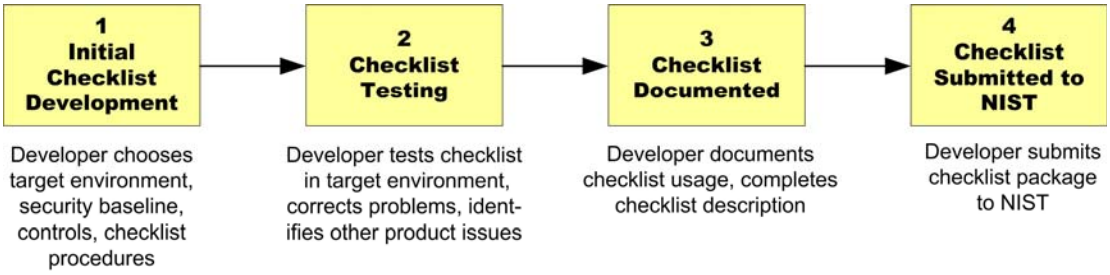

Figure 5-2: Initial Checklist Development Stages

5.2.1 Initial Checklist Development

In this step, a developer becomes familiar with the requirements of the checklist program and all procedures involved during the checklist lifecycle (as described throughout this section). At this point, a developer would presumably agree to the participation requirements of the program before continuing further to build the checklist. The participation requirements of the program are described in this document but are laid out in administrative and programmatic terms in Appendix C, which is intended less for technical developers and more for those in developer organizations who would need to formally agree to the program's requirements. The participation agreement itself is contained in Appendix D.[12]

The developer then decides which security baseline from Section 3 should be implemented by the checklist, and then builds the checklist accordingly, using the security-related criteria from Sections 3 and 5.1. The output of this step is an initial checklist for the product.

Appendix B describes the complete set of fields for a checklist description on the repository; users can search on and view these fields when using the repository. Table 5-1 shows fields of the checklist description that would be completed at this step:

Table 5-1: Fields Completed at Initial Checklist Development

Field Name	Description
PRODUCT MANUFACTURER NAME	Contains the name of the manufacturer of the IT product.

[12] The latest updates to these sections and to this document are available at http://checklists.nist.gov. This updated material should be consulted before formally agreeing to participate in the program.

Field Name	Description
PRODUCT CATEGORY	The main product category of the IT product, e.g. firewall, IDS, operating system, web server, etc.
PRODUCT NAME	The official IT product name.
PRODUCT VERSION	The specific software or firmware released version number of the IT product, including service pack or patch level as appropriate.
CHECKLIST TARGET ENVIRONMENT	The IT product's operational environment, e.g. SOHO, Enterprise, High Security, or Custom (with description).
CHECKLIST TARGET AUDIENCE	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.
CHECKLIST NAME	States the name of the checklist.
CHECKLIST SUMMARY	Summarizes the purpose of the checklist and its settings.
SUBMITTING ORGANIZATION/ AUTHORS	The name of the organization and authors that produced the checklist.
PRODUCT ROLE	Specifies 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, etc.
CHECKLIST INSTALLATION TOOLS	Describes the functional tools required to use the checklist to configure the system, if they are not included with the checklist.

5.2.2 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. The testing data need not be submitted to NIST; however, the developer should retain it for review as appropriate.

Table 5-2 shows fields in the checklist description that would be completed at this step:

Table 5-2: Fields Completed During Checklist Testing

Field Name	Description
CHECKLIST 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.
TESTING PROCEDURES	Platforms on which checklist was tested. Can include any additional testing-related information such as summary of testing procedures used.
CHECKLIST ROLLBACK CAPABILITY	Whether the changes in product configuration made by applying the checklist can be rolled back and, if so, how to rollback the changes.

Selecting the most appropriate set of security controls can be a daunting task, because many security controls have limit system functionality and usability. In some cases, a security control can even have a negative impact on other 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. 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.

NIST has produced SP 800-42, *Guideline on Network Security Testing* [20], to assist administrators in testing systems for vulnerabilities and configuration problems. Although this publication is more focused on testing systems instead of individual IT products, it may still be useful to checklist developers.

5.2.3 Documenting the Checklist

The quality of checklist documentation often makes a major difference in the checklist's effectiveness. The checklist documentation should clearly explain how to install the checklist, using concise, sound, and complete instructions. The skill level required to install the checklist needs to be identified, as well as the targeted environment. The documentation should also explain the significance of individual settings, including any changes to product functionality. 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 a state prior to 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 troubleshooting information if errors occur or the checklist settings cause the product to operate incorrectly. Ideally, assistance is available for (registered) users of the product in case of problems.

Table 5-3 shows additional fields in the checklist description that would be completed in this step:

Table 5-3: Additional Documentation Fields

Field Name	Description
CHECKLIST TARGET AUDIENCE	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.
DOWNLOAD PACKAGE	URL or filenames(s) of the checklist documentation.
CHECKLIST POINT OF CONTACT	Provides an e-mail 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.
REFERENCES	Any supporting references chosen by the developer that were used to produce the checklist or checklist documentation.
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 Checklist Program logo.
NIAP/CMVP CHECKLIST	Whether the product has been NIAP or CMVP evaluated using this checklist. The field also states the type of evaluation received.

Field Name	Description
COMMENTS, WARNINGS, DISCLAIMER, MISCELLANEOUS	Any additional information that the checklist developer wishes to convey to users.

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

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

- Complete and accurate checklist description
- Statement of the security objectives, including the targeted environment, and expected behavior of the product after applying the checklist
- The target audience (e.g., end-user, system administrator) and the level of technical skill required to install the checklist
- Explanation of the checklist settings, including each setting's effect on the 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
- Procedures for uninstalling the checklist (if applicable)
- Troubleshooting instructions or other information and references.

5.2.4 Checklist Package Submission to NIST

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

- The checklist and configuration files, templates, scripts, etc.
- The completed checklist description
- The checklist documentation
- Identification of the developer point of contact
- A signed participation agreement.

The participation agreement and other requirements are outlined in more detail in Appendix C. This appendix also includes the appropriate NIST contact information.

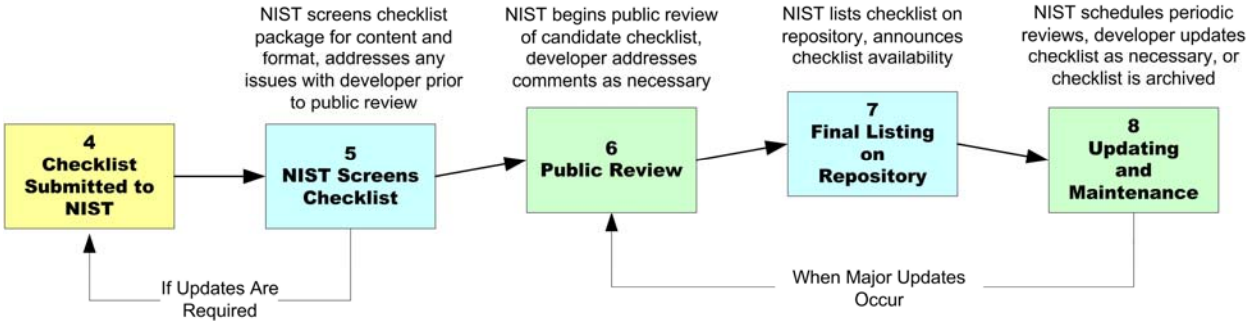

Figure 5-3: Checklist Finalizing and Publishing Steps

5.3 NIST Steps for Reviewing and Finalizing Checklists for Publication

NIST's process for screening and publishing the checklist is described within the following sections. Figure 5-3 shows the general steps; steps 4 and 5 may loop depending on the amount of feedback to the developer. Steps 6 and 8 may repeat depending on the magnitude of updates to an already published checklist (most changes should not require additional public reviews).

5.3.1 Checklist Package Screening

This step determines if the checklist is sufficiently accurate and complete to be publicly reviewed. NIST will screen the checklist materials for completeness and accuracy, and examine testing procedures used to evaluate the checklist. The developer may be contacted with questions about the submitted materials during the screening period. NIST will complete the screening and, if all issues are addressed, post the checklist and description as a candidate for a period of typically 30 to 60 days.

Section 5.1 describes criteria for checklist and checklist description development; the criteria are used also for screening the checklist. Essentially, the security objectives of the checklist should be consistent with recommended guidance from NIST and other recognized security organizations, and guidance from other checklist producing organizations. The checklist must be documented according to the guidelines in this section and in Appendix C. Some of the questions typically posed by NIST when screening checklist submissions include the following:

- Documentation
  - Does it specify the target audience?
  - Does it identify the targeted environment?
  - Does it explain the security objectives?
  - Does it contain a complete, clear, and concise description of the checklist settings?
- Best 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 a real-world environment and determined that the checklist settings cause the product to meet the security objectives of the checklist?
  - Do any of the checklist settings cause the product to become inoperable or unstable?
  - Do certain 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 prior to 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 troubleshooting information if errors occur or 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?

5.3.2 Candidate Checklist Public Review

Once the checklist has been screened and the developer has addressed any issues, NIST will post it for public review for a period of typically 30 to 60 days. This will allow the public to review and test the checklist, and provide the checklist developers and NIST with comments and feedback. These may be incorporated in a revision of the checklist to improve its quality. When a candidate checklist has completed the review process, it will be included in the checklist repository.

A reviewer will complete a standardized feedback form to capture comments as well as other information regarding 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 but not exclusive of the reasons for using independent reviewers are the following:

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

At the end of the public review period, NIST will announce that the comment period is closed. Depending upon the number of comments received and the ramifications of those comments to the checklist, NIST will determine a timeframe in which the developer must respond to comments, which will typically range from 15 to 30 days from the end of the review period.

5.3.3 Final Listing, Maintenance, and Archival

After any outstanding issues are addressed, NIST will list the final checklist and announce the inclusion of the checklist on the repository. At this time, the developer (e.g., an 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 usage of the logo are described in Appendix D.

NIST will also announce procedures for accepting further comments or questions regarding the checklist throughout its remaining lifecycle. Depending on the product and how frequently updates may occur, NIST may maintain a mailing address for the associated checklists. Users who subscribe can receive announcements of updates or other issues connected with a checklist. The selected checklist's description (on the checklist repository) will contain subscription instructions. Throughout the checklist lifecycle, NIST will continue to collect feedback and pass this information to the checklist developer.

When the final checklist is listed, NIST will set a periodic review schedule with the developer. Typically, the timeframe for the review will be one year; however, it could be sooner depending on certain factors such as the discovery of new vulnerabilities. If the developer decides to update the checklist, NIST will announce that the checklist is in the process of being updated. If the checklist contains major changes, it will be accepted as if it were a new submission; it must undergo the same reviews as a new submission.

At the developer's discretion, the checklist can be removed from the repository or reclassified as an archive. Typical reasons would include 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 section contains references to documents used in this publication.

[1] Cyber Security Research and Development Act of 2002, http://www.house.gov/science/cyber.htm

[2] Report of the Technical Standards and Common Criteria Task Force, http://www.cyberpartnership.org/init-tech.html

[3] Federal Information Security Management Act (FISMA) of 2002, http://csrc.nist.gov/policies/FISMA-final.pdf

[4] OMB Circular A-130, http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf

[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA), http://aspe.hhs.gov/admnsimp/pl104191.htm

[6] Sarbanes-Oxley Act of 2002, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:

[7] *The New FISMA Standards and Guidelines*, Ron S. Ross, Ph.D., http://csrc.nist.gov/sec-cert/fisma-article-v15.pdf

[8] NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

[9] NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

[10] NIST Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf

[11] NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[12] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[13] NIST Special Publication 800-43, *Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System*, http://csrc.nist.gov/itsec/guidance_W2Kpro.html

[14] NIST Special Publication 800-46, *Security for Telecommuting and Broadband Communication*, http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf

[15] NIST Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[16] NIST Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, http://csrc.nist.gov/publications/nistpubs/800-28/sp800-28.pdf

[17] NIST Special Publication 800-36, *Guide to Selecting Information Security Products*, http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

[18] NIST Special Publication 800-40, *Procedures for Handling Security Patches*, http://csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

[19] NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

[20] NIST Special Publication 800-42, *Guideline on Network Security Testing*, http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf

[21] NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf

[22] NIST Special Publication 800-45, *Guidelines on Electronic Mail Security*, http://csrc.nist.gov/publications/nistpubs/800-45/sp800-45.pdf

[23] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, http://csrc.nist.gov/publications/drafts/draft-SP800-53.pdf

[24] NIST Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, http://csrc.nist.gov/publications/drafts/NIST_SP800-58-040502.pdf

[25] NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

[26] NIST Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, http://csrc.nist.gov/itsec/guidance_WinXP.html

[27] FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[28] NIST Handbook 150, *Procedures and General Requirements for the National Voluntary Laboratory Accreditation Program*, http://ts.nist.gov/ts/htdocs/210/214/docs/final-hb150-2001.pdf

[29] NIST NVLAP Assessor Declaration, http://ts.nist.gov/ts/htdocs/210/214/assessors/declare.pdf

[30] NIST NVLAP Assessor Performance Information Form, http://ts.nist.gov/ts/htdocs/210/214/assessors/apef.pdf

[31] *Common Criteria for Information Technology Security Evaluation* (CC), Version 2.1, August 1999, http://www.commoncriteria.org/

[32] *Information Assurance Technical Framework* (IATF), Release 3.0, October 2000, http://www.iatf.net/, member-only area, site registration at: https://www.iatf.net/register/

[33] *Advanced Technology Program Proposal Preparation Kit, Appendix B,* http://www.atp.nist.gov/atp/kit-04/append-b.htm

[34] *ISO/IEC Guide 58*, 1993, available for sale at http://www.iso.ch/iso/en/Standards_Search.StandardsQueryForm

[35] Top Ranked Information Security Issues: The 2004 International Information Systems Security Certification Consortium (ISC)^2 Survey Results, available to members at https://www.isc2.org/cgi-bin/index.cgi

[36] National Security Agency (NSA) - Security Configuration Guides, available at http://www.nsa.gov/ia/

[37] Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS), available for .mil and .gov domains at https://iase.disa.mil/techguid/stigs.html and, for other domains, at http://csrc.nist.gov/pcig/cig.html

[38] Center for Internet Security (CIS) Benchmarks, available at http://www.cisecurity.org

[39] National Information Assurance Glossary, CNSS Instruction no. 4009, Revised May 2003, http://www.nstissc.gov/Assets/pdf/4009.pdf

Appendix B. Checklist Description Template

This section describes the fields of the checklist description that is maintained for each checklist on the checklist repository. The completed fields will be used to provide information about the checklist to users.

Checklist developers must complete a checklist description form for each checklist. The fields are mandatory unless otherwise stated. The latest version of the checklist description form can be downloaded from the checklist repository at http://checklists.nist.gov.

Table B-1 shows all fields of the checklist description, with sample data from NIST's Microsoft Windows® XP checklist [26].

Table B-1: Fields in the Checklist Description Template

Field Name	Description	Example Data
CHECKLIST CHANGE HISTORY	Running log detailing any changes made to the checklist since its inclusion in the repository. This field is updated with each version of the checklist.	Security Templates (.inf files) 2004-07-04 - Draft Update R1.0.1 Setting 5.26 (all templates) - Correct typo in the DOJ message Setting 12.5 (all templates) - Correct typo in the registry value Security Templates (.inf files) 2004-06-24 - Draft Release R1.0 Draft Guidance for Securing Microsoft Windows XP Systems for IT Professionals document 2004-07-04 - Draft Update Delete a blank page Setting 12.5 (Appendix A) - Correct typo in the registry value 2004-06-24 - Draft Release.
CHECKLIST INITIAL CREATION DATE	States the date when the checklist is first listed by NIST, in the format CCYY-MM-DD. NIST will fill in this field.	2004-07-17
DOWNLOAD PACKAGE	URL or filenames(s) of the checklist documentation.	http://csrc.nist.gov/itsec/guidance_WinXP.html
CHECKLIST HOMEPAGE	States the URL of the checklist home page.	http://csrc.nist.gov/itsec/guidance_WinXP.html

Field Name	Description	Example Data
CHECKLIST SUMMARY	Summarizes the purpose of the checklist and its settings.	NIST Special Publication 800-68 has been created to assist IT professionals, in particularly Windows XP system administrators and information security personnel, in effectively securing Windows XP systems. It discusses Windows XP and various application security settings in technical detail. The guide provides insight into the threats and security controls that are relevant for various operational environments, such as for a large enterprise or a home office. It describes the need to document, implement, and test security controls, as well as to monitor and maintain systems on an ongoing basis. It presents an overview of the security components offered by Windows XP and provides guidance on installing, backing up, and patching Windows XP systems. It discusses security policy configuration, provides an overview of the settings in the accompanying NIST security templates, and discusses how to apply additional security settings that are not included in the NIST security templates. It demonstrates securing popular office productivity applications, Web browsers, e-mail clients, personal firewalls, antivirus software, and spyware detection and removal utilities on Windows XP systems to provide protection against viruses, worms, Trojan horses, and other types of malicious code. This list is not intended to be a complete list of applications to install on Windows XP system, nor does it imply NIST's endorsement of particular commercial off-the-shelf (COTS) products.
CHECKLIST STATUS	Whether Candidate, Final, Archived, or Under Review. NIST will fill in this field.	Final
CHECKLIST VERSION	Indicates the version or release number of the checklist.	Draft update R1.0.1
COMMENTS, WARNINGS, DISCLAIMER, MISCELLANEOUS	Any additional information that the checklist developer wishes to convey to users.	
CHECKLIST INSTALLATION TOOLS	Describes the functional tools required to use the checklist to configure the system, if they are not included with the checklist.	The Microsoft Windows tools, e.g. Security Templates MMC snap-in, Security Configuration Analysis MMC snap-in, Group Policy MMC snap-in, and Group Policy Management Console MMC snap-in can be used to customize and apply the NIST security templates to Windows XP systems.
INTEGRITY	The message digest or hash of the checklist package. SHA-1 or SHA-256 is recommended.	NIST_WinXP_draft_R1.0.1_07042004.zip - SHA-1 hash: 912e951848120a362f245e6cdb07216430afa559

Field Name	Description	Example Data
CHECKLIST 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.	Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. These recommendations should be applied only to the Windows XP Systems and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The security templates have been tested on WinXP Professional systems and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The high security template should not be used by home users and should be used with caution since it will restrict the functionality and reduce the usability of the system.
CHECKLIST NAME	States the name of the checklist.	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist - Special Publication 800-68 (Draft)
CHECKLIST LATEST REVISION DATE	States the date when the checklist was last revised, in the format CCYY-MM-DD. NIST will fill in this field.	2004-07-17
PRODUCT MANUFACTURER NAME	Contains the name of the manufacturer of the IT product.	Microsoft Corporation
NIAP/CMVP STATUS	Whether the product has been NIAP or CMVP evaluated using this checklist. The field also states the type of evaluation received.	Microsoft Windows XP Professional can be configured to operate in the FIPS validated mode. The product has not been evaluated with a NIAP-approved Common Criteria Testing Laboratory
REGULATORY COMPLIANCE	Whether the checklist is consistent with various regulations, e.g. HIPAA, GLBA, FISMA, ISO17799, Sarbanes & Oxley, DoD 8500, etc.	The recommendations are consistent with the low and potentially moderate security control baselines advocated in SP 800-53 draft (NIST FISMA implementation project publication)
NIST IDENTIFIER	A NIST-assigned identifier to uniquely identify the checklist. NIST will fill in this field.	1001
CHECKLIST POINT OF CONTACT	Provides an e-mail 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.	itsec@nist.gov
PRODUCT CATEGORY	The main product category of the IT product, e.g. firewall, IDS, operating system, web server, etc.	Operating system
PRODUCT NAME	The official IT product name.	Windows XP Professional
PRODUCT ROLE	Specifies 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, etc.	Client desktop and mobile host.

Field Name	Description	Example Data
PRODUCT VERSION	The specific software or firmware released version number of the IT product, including service pack or patch level as appropriate.	Microsoft Windows XP 5.1.2600 Service Pack 1 Build 2600
REFERENCES	Any supporting references chosen by the developer that were used to produce the checklist or checklist documentation.	DISA, NSA, CIS, Microsoft and other security guides.
CHECKLIST ROLLBACK CAPABILITY	Whether the changes in product configuration made by applying the checklist can be rolled back and, if so, how to rollback the changes.	There is no automated way of rolling back the settings unless a full system backup was performed before a security template was applied to the system.
SUBMITTING ORGANIZATION/ AUTHORS	The name of the organization and authors that produced the checklist.	NIST, Computer Security Division
CHECKLIST TARGET AUDIENCE	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.	This checklist has been created for IT professionals, particularly Windows XP system administrators and information security personnel. The document assumes that the reader has experience installing and administering Windows-based systems in domain or standalone configurations.
CHECKLIST TARGET ENVIRONMENT	The IT product's operational environment, e.g. SOHO, Enterprise, High Security, or Custom (with description).	SOHO, Enterprise, and High Security
TESTING INFORMATION	Platforms on which checklist was tested. Can include any additional testing-related information such as summary of testing procedures used.	The security templates have been tested on Windows XP Professional systems and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The download package includes test scenarios and results that were documented during the testing process.
LICENSING	States the license agreement, e.g. the checklist is copyrighted, open source, GPL, free software, shareware, etc.	This document was developed at the National Institute of Standards and Technology, which collaborated with NSA, DISA, CIS, and Microsoft to produce the Windows XP security templates. Pursuant to title 17 Section 105 of the United States Code this document and template are not subject to copyright protection and is in the public domain.
DISCLAIMER		Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. NIST assumes no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic. NIST would appreciate acknowledgement if the document and template are used.
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 Checklist Program logo.	Microsoft will continue to provide support to the product in the event that the system fails. Applying the NIST security templates and recommendation does prevent the user from obtaining technical support from the product vendor.
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.	Kurt Dillard, Microsoft Corporation.

Appendix C. Checklist Program Operational Procedures

This appendix sets forth the policies, procedures and general requirements for the NIST Security Configuration Checklists Program for IT Products. This appendix is intended for those individuals in developer organizations who would need to formally agree to the program's requirements. 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 http://checklists.nist.gov.

This appendix is organized as follows:

- Section C.1 - general considerations for the NIST Checklist Program
- Section C.2 - procedures for initial screening of a checklist prior to public review
- Section C.3 - procedures for the public review of a candidate checklist
- Section C.4 - final acceptance procedures
- Section C.5 - maintenance and delisting procedures
- Section C.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* is a *Technical Configuration Checklist*, which is a checklist that refers to 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 NIST 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 Checklist Program logo.
- *NIST Checklist Program* or *Program* is used in place of the NIST Security Configuration Checklists Program for IT Products.
- *NIST Checklist Repository* or *Repository* refers to the Web site that maintains the checklists, the descriptions of the checklists, and other information regarding the NIST 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 requirements of this program are as follows:

- Advanced Technology Program Proposal Preparation Kit Appendix B, http://www.atp.nist.gov/atp/kit-04/append-b.htm
- *Common Criteria for Information Technology Security Evaluation* (CC), Version 2.1, August 1999, http://www.commoncriteria.org/
- *Information Assurance Technical Framework* (IATF), Release 3.0, October 2000, http://www.iatf.net/, member-only area, site registration at: https://www.iatf.net/register/
- FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/index.html
- NIST Handbook 150, *Procedures and General Requirements for the National Voluntary Laboratory Accreditation Program*, http://ts.nist.gov/ts/htdocs/210/214/docs/final-hb150-2001.pdf
- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, http://csrc.nist.gov/publications
- NIST SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*), http://csrc.nist.gov/publications
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, http://csrc.nist.gov/publications
- NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, http://csrc.nist.gov/publications

C.1 Overview and General Considerations

This section focuses on general considerations for all parts of the NIST 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 and supporting information, and a signed agreement to the requirements of the NIST Checklist Program. General information about checklists is discussed in Section C.1. Checklist submission requirements and procedures are discussed in Section C.2.
2. NIST verifies that all information is complete and performs a screening on the checklist. Checklists meeting the requirements for listing receive further consideration and are referred to as "candidate checklists." Section C.2 discusses screening criteria and procedures. Section C.1 (d) discusses issue resolution processes.
3. NIST lists the candidate on the repository for a public review period of typically 30 to 60 days, as discussed in Section C.3.
4. NIST forwards comments from public reviewers to the developer. When all issues are addressed, the checklist is listed on the FCL, as discussed in Section C.4.
5. The developer contacts NIST on typically an annual basis to determine whether the listing should continue, be updated, or archived, as discussed in Section C.5.

(b) **Intellectual Property Rights:** Developers retain intellectual property rights in 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 are:

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.

C.2 Checklist Submission and Screening

This section outlines the procedures and requirements for submitting checklists to NIST and the process by which NIST determines that checklists are suitable for public review. When checklists meet the screening requirements, 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, all in the English language:

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, facsimile number, and e-mail address.
2. The checklist, documentation, and description template.

3. The participation agreement, which must be printed, signed, and sent to NIST. NIST accepts e-mailed 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 checklists meet the program requirements. The following paragraphs summarize the screening criteria, which is described more fully in NIST Special Publication 800-70.

1. The checklist settings reflect consideration of recommended security and engineering practices.
2. The checklist contains a complete, clear, and concise description of the configuration settings.
3. The checklist has been tested and configuration or compatibility issues have been identified.
4. The documentation explains how to install or uninstall the checklist.
5. Checklist-related help is available.

C.3 Candidate Checklist Public Review

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

(a) **Public Review Period:** NIST typically lists candidates for a 30 to 60 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 complete a web-based feedback form to capture their comments as well as other information regarding the reviewer's test environment, procedures, and other relevant information. The contents of the feedback forms are considered public records.

(c) **Maintaining Records:** NIST maintains copies of all correspondence and feedback between the public and developers by creating a unique e-mail address for each checklist. NIST will archive the information.

(d) **Addressing Comments:** At the end of the public review period, NIST announces that the comment period is closed. Depending upon the number of comments received and the ramifications of those comments to the checklist settings, NIST determines a timeframe in which the developer must respond to comments. This typically ranges from 15 to 30 days from the date the comments were submitted or from the end of the review period. At no time will this period be less than 15 days.

C.4 Final Checklist Listing

After NIST determines that checklists and 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 e-mail 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 problem, that may be caused by using the checklist.*

(b) **Handling Comments:** NIST continues to accept comments regarding final checklists by maintaining a central electronic mailing address on the repository. NIST lists the procedures for contacting the developer, along with information for contacting the developer, such as e-mail addresses or URLs.

(c) **Scheduling Periodic Reviews:** NIST determines whether a final checklist should be reviewed periodically and typically sets the review timeframe for one year. NIST may request that a checklist be reviewed sooner for reasons such as new vulnerabilities or threats. NIST schedules reviews with the developer's points of contact. If at any time the point of contact changes, NIST must be notified immediately.

C.5 Final Checklist Update, Archival, and Delisting

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

(a) **Periodic Reviews:** Developers contact NIST at least annually to determine changes in the status of checklists. NIST may contact developers, as appropriate, to determine 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 periodic review. Developers have 60 days in which 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:** When a developer no longer provides support for the checklist, at the developer and NIST's discretion, the checklist can remain in the repository but reclassified as an archive. Typical reasons would include that the product is no longer supported or is obsolete, or that the developer no longer wishes to provide support for the checklist.

(d) **Delisting:** NIST removes the checklist from the FCL. NIST may send announcements to various e-mail lists maintained by NIST or other organizations.

(e) **Automatic Delisting:** If a final checklist is not reviewed annually, it is removed from the FCL. At the developer and NIST's discretion, it can be reclassified as an archive.

C.6 Record Keeping

NIST maintains information associated with the program and requires that participators 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, 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.

Appendix D. Participation and Logo Usage Agreement Form

This appendix contains the terms and requirements for participation in the NIST Checklist Program and for use of the NIST 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 http://checklists.nist.gov/participation-agreement.pdf.

The phrase "NIST Security Configuration Checklists Program for Information Technology Products" and the NIST Checklist Program logo are intended for use in association with specific versions of IT products for which a checklist has been created and has met the requirements of the National Institute of Standards and Technology (NIST) Security Configuration Checklists for Information Technology Products (Checklist) Program for final listing on its checklist repository. You may participate in the NIST 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 Checklist Program (Appendix C of NIST SP 800-70).

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

3. You agree to maintain the checklist and timely response 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 Checklist Program.

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

6. You may terminate your participation in the NIST 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 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 which 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 Security Configuration Checklists Program for Information Technology Products" and the NIST 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 Security Configuration Checklists Program for Information Technology Products" and the NIST Checklist Program Logo.

9. Your permission for advertising participation in the NIST 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 Checklist Program on its Final Checklist List.

10. Your permission for advertising participation in the NIST 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 (TBD – will be specified in final document).

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 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 E. Acronyms and Glossary

Selected acronyms and terms used in the guide are defined below. Definitions for some terms have been adapted from [39].

ATP	Advanced technology program; http://www.atp.nist.gov
Availability	Timely, reliable access to data and information services for authorized users
Candidate Checklist	A checklist approved by NIST for public review
CERT®/CC	Computer Emergency Response Team/Coordination Center; http://cert.org
CIS	Center for Internet Security; http://cisecurity.org
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices
Consortia	An association or society, i.e., the IETF
Consumer	Organizations or private individuals using checklists
Custom	A specialized operational environment
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security; http://www.dhs.gov/dhspublic/
DISA	Defense Information Systems Agency; http://www.disa.mil/
DNS	Domain Name System
Enterprise	An inward-facing environment typically very structured and centrally managed
FCL	Final Checklist List on the repository
Final Checklist	A checklist approved by NIST for placement on the repository
FIPS	Federal Information Processing Standards; http://csrc.nist.gov/publications/fips
FISMA	Federal Information Security Management Act; http://csrc.nist.gov/sec-cert/
FTP	File Transfer Protocol
High Security/Limited Functionality	An environment encompassing systems with high security requirements

IDS	Intrusion Detection System
IETF	Internet Engineering Task Force; http://www.ietf.org
Independent Qualified Reviewer	A reviewer tasked by NIST to make a recommendation regarding a checklist
Integrity	Quality of a system or product reflecting the logical correctness and reliability of the operating system; verification that the original contents of information have not been altered or corrupted
Inward-Facing	When a system is connected on the interior of a network behind a firewall
LAN	Local Area Network
Legacy	Typical Custom environment usually involving older systems or applications
Logo	The NIST Checklist Program logo
NIST	National Institute of Standards and Technology; http://www.nist.gov/
NSA	National Security Agency; checklists at http://www.nsa.gov/snac/
NVLAP	National Voluntary Laboratory Accreditation Program; http://nvlap.nist.gov
OMB	Office of Management and Budget; http://www.whitehouse.gov/omb/
Operational Environment	SOHO, Enterprise, High Security, or Custom/Legacy
Outward-Facing	When a system is directly connected to the Internet
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
Producer	A developer of a checklist
Repository	The NIST checklist repository; http://checklists.nist.gov
Public Reviewer	A member of the general public who reviews a candidate checklist and sends comments to NIST
SMTP	Simple Mail Transfer Protocol
SOHO	Small Office Home Office Environment
STIG	Security Technical Implementation Guides; http://csrc.nist.gov/pcig/cig.html
TCP/IP	Transmission Control Protocol/Internet Protocol

Template	XML-encoded checklist description template that describes aspects of a checklist
US-CERT	The DHS's CERT; http://www.us-cert.gov/
VOIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy protocol
WPA	Wi-Fi Protected Access
XML	Extended Markup Language