

Government Information Security System with ITS Product Pre-qualification

Wan S. Yi¹, Dongbum Lee², Jin Kwak², Dongho Won^{1*}

¹ Information Security Group, Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea
{wsyi, dhwon}@security.re.kr

² Department of Information Security Engineering, Soonchunhyang University,
646 Eupnae-ri, Shinchang-myun, Asan-si, Chungcheongnam-do, 336-745, Korea
{dblee, jkwak}@sch.ac.kr

Abstract. As society is becoming increasingly information-oriented, the need for the development of various information security systems increases. Information systems can improve and quality and effectiveness of our lives. However, concerns regarding security properties assessment service of information security system increases. This is promulgated by the number of dysfunctional phenomenon witnessed by an increasingly information-oriented society. Thus, various security assessment services are developed and studied. Therefore, we need a checklist program to manage such security assessment services systematically. This paper analyzes the checklist program of the U.S. FISMA process. Then we will summarize an introductory plan for internal government information security systems using this approach.

Keywords: FISMA, Government Information Security System, Checklist Program

1 Introduction

Security of preferred products must be evaluated, and authenticated as part of a plan to construct an information security system for public institutions and national organization. Security authentication issues for products have increased. Thus, various assessment services are required both domestically and outside the country. Using CMVP (Cryptographic Module Validation Program) for assurance of the cipher function, CC (Common Criteria) increases the necessity for domestic information security product assessment and certification system. ISMS (Information Security Management System) for assurance at an operational level verifies the security features of IT products by providing various security assessment services. This improves the nation's quality of protection. In addition, preparing a plan that helps in the selection of information security product that can be trusted by public institutions

* Prof. Dongho Won, he is the corresponding author

and national organization's users can protect software assets from malicious and unintentional harm.

However, most systems are at a security management level for information systems that has been through an assurance system at the product level. A system to administer and an assurance system for users of systems or application systems have yet to be settled.

It provides security assessment service to achieve correct assessment and certification in security product characteristic to resolve these problems. It is compliant with the U.S. FISMA (Federal Information Security Management Act), under which the system evaluation criteria and methodology are developed and operate. In particular, the security configuration checklist program for IT products is a FISMA process in which the checklist is evaluated in NIST by the system that verifies IT security products and manages and supervises their deployment. The remainder of this paper is as follows. Analyze information security product assessment and certification, KCMVP and FISMA in section 2. Section 3 analyzed NIST checklist program and summarized about government information system introduction plan through pre-qualification in section 4. Compares and analyze on the basis of contents that summarized in section 5 and concludes conclusion in section 6.

2 Related Work

2.1 Information Security Product Assessment and Certification

Raises nation quality of protection because information security product assessment and certification verifies security function of information security product according to Common Criteria and enforces fair assessment of information security product and certification and allows purpose to strengthen competitive power of product. This system began by necessity of system that can select information security product that can trust to nation and public institution user to improve nation quality of protection, and protect main asset from information dysfunction. Also, safety and authoritativeness are enforcing National Intelligence Service (NIS) and information security product assessment and certification system that is based on law in Ministry of Public Administration and Security (MOPAS) for verify information security product supply and use promotion by nation and public institution target[1].

2.2 KCMVP

Korea Cryptographic Module Validation Program (KCMVP) is system that verify safety and implementation conformance about cipher product using for protection of critical intelligence that is not classified esoterically among the data that have mutual understanding at information network system of nation and public institution. To achieve cryptographic module test and verification, test agency representative composes test part and test whether satisfy requirements that verification target cryptographic module is clarified in test standard. Test agency submits test result report to verification agency after cryptographic module test is ended, and verification

agency issues validation certificate according to committee's investigation result because holds verification committee meeting after examination about test result and registers in cryptographic module verification list.

2.3 FISMA

FISMA executes the information security program for federal agencies. It offers the entire security for information systems that need documentation development for each federal agency. It supports federal agency control, including federal agency · contractor · source of supply and asset.

Evaluate risk, including loss · unauthorized access · use · exposure · disruption · alteration · destruction of information and information system that supports the operation of federal agency and asset continuity. In addition, policies and procedures based on risk assessment decrease the cost-effective information security risk to a permissible level. Information security is assured if it is processed through the life cycle of the information system of each federal agency [2] [3].

It includes a low rank plan to offer suitable information security for a group of network · facilities · information system · information system, and executes policy and security awareness training informing people of the information security risk related to activity and responsibility based on the procedure of the planned federal agency to mitigate risk [4].

To periodically test effectiveness · procedure · operation · security control of the information security policy and assessment, defects of the information security policy · procedure · federal agency enforcing the program. It is submitted when the possibility of risk may occur frequently. It adopts improvement actions to process the plan · implementation · assessment · documentation [5].

3 NIST checklist program

SP 800-70 is one of several FISMA processes. It represents the security configuration checklist program for IT product. It performs a security configuration checklist for the user and developer of the IT product. In this part, we explain how to take advantage of the security configuration checklist for the checklist user. It searches for and acquires the checklist of the NIST checklist program. Concerning the developer, it explains the NIST checklist program engagement policy · procedure · general requirements.

3.1 Specification field of checklist

The information that is meant to decide if the checklist of the user is correct for each concrete purpose. The specification checklist to use must include the specification style mark. Based on the request · role · and capability of the user, the importance of each field included in the specification differs [6].

Table 1. Specification field of NIST checklist

Name of field	Contents
Checklist summary	Purpose of checklist and configuration summary
Status	Whether candidate, final, or archived. NIST will fill in this field
Version	Version number or release number of checklist
Comments, Warnings, Disclaimer, Miscellaneous	Further information that checklist developer wants to convey to the user
Revision Date	States the date when the checklist was last revised, in the format CCYY-MMDD. NIST will fill in this field
Vendor	Contains the name of the manufacturer of the IT product
Point of Contact	e-mail address to transmit question · opinion · proposal · problem report relating to checklist
Product Category	Main product classification of IT product
Product	The official IT product name
Product Role	Main usage and function of IT product that is described in the checklist
Product Version	Specification software of IT product or release version number of firmware
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	A name of organization and writer that created the checklist
Target Audience	Checklist target user that can use the construction · test
Target Operational Environment	Operation environment of IT product
Testing Information	Platform on which the product was tested against the checklist
Product Support	Vendor will accept support calls from users who have applied this checklist on their IT product. Warranty for the IT product has not been affected. Required for usage of Checklist Program logo

3.2 Checklist user

The general phase included for the checklist user and developer appears in Figure 1 and Figure 2. The phases for the checklist user are as follows.

Step 1: User collects local requirements, and buys suitable IT product.

Step 2: Users browse the checklist repository to retrieve checklists that match the user's operational environment and security requirements. If a product is intended to be secure 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.

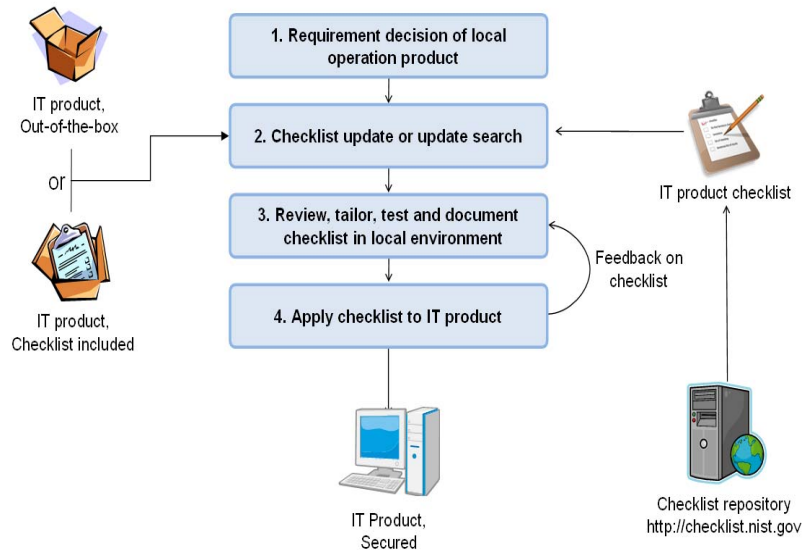


Fig. 1. Phase for checklist user

Step 3: Test checklist, as this enforces reconciliation and documentation of the checklist based on the need to consider local policy and functional requirements. It provides feedback about NIST and the developer checklist.

Step 4: Introducing the checklist enforces preparation (e.g., configuration, data backup) and applies the checklist in the operational environment.

3.3 Checklist developer

For developers, the process is comprised 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.

Step 1: Developer confirms checklist program step and requirement, and completes engagement that takes part on program.

Step 2: Developer creates, tests, and refines the checklist.

Step 3: Developer documents checklist based on program guidelines.

Step 4: Developer prepares checklist presentation package, and submits it to NIST.

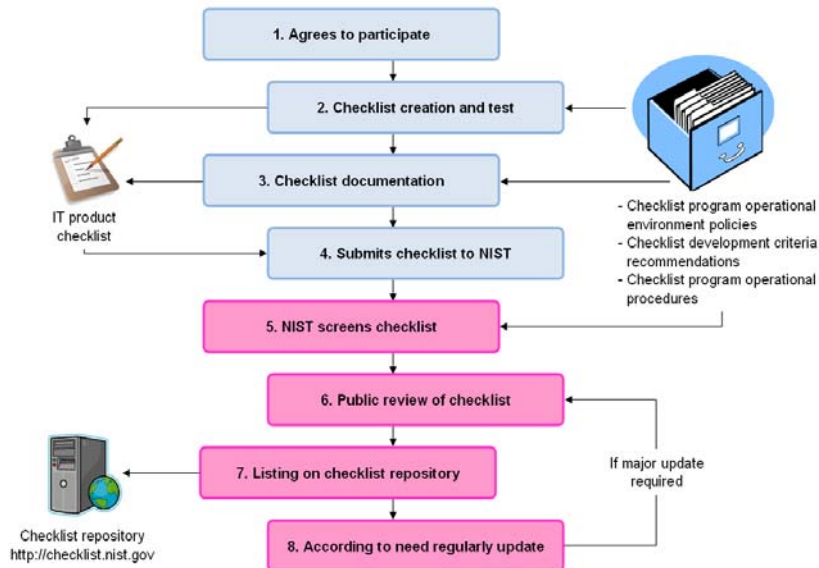


Fig. 2. Phase for checklist developer

Step 5: NIST judges the checklist based on the program requirements. It resolves any issues with the developer.

Step 6: The next step is a public review of the checklist. This typically lasts 30 to 60 days. Comments submitted during the review are addressed as applicable by the developer and NIST.

Step 7: NIST posts the checklist on the repository and announces its presence.

Step 8: Publish on-time update of checklist and archive.

4 Government Information Security System with ITS Product Pre-qualification

The plan that we summarize considers the current inefficiencies, costs and time to introduce the existing government information security system product. It displays the general requirements of the product name · CC authentication information · cipher function of the relevant product in detail. We summarize the introduction of a procedure to choose products from the government information security system using the product list of the government information security system that can be used by public institutions and national organizations.

4.1 Product list of government information security system

Table 2 shows the product list of the proposed government information security system. The list attached can be used to provide information about the government information security system products in national organizations and public institutions [7] [8] [9].

Table 2. Product checklist of proposed government information security system

Classification	Explanation
Sections	Division by Network Information Security System, Information Security Infrastructure System, Computing Information Security System
Divisions	Division by Network-based, Network-to-Network, Security Management, Biometrics, Smart cards, Authentication Solutions, Server Security, Database, Mail Security, Device Security, PC Security
Product classification	Main product classification of IT product
Product name	Trademark name of the IT product
Developing country	The country that developed the IT product
Vendor	Developer of the IT product
Product version	Version and release number of the IT product
Product summary explanation	IT product clarification and configuration summary
Cipher product security	CMVP verify availability
CC assessment availability	CC assessment availability
Cipher availability	Cipher availability of relevant product
Cryptographic algorithm	Encryption algorithm of relevant product
Authentication date	CMVP and CC authentication date indication
Test information	Platform mark that test product
Copyright information	Copyright
Product support	Vendor support

4.2 Specification field explanation

The following sections explain each field for the product list of the proposed government information security system.

Sections, Divisions and Product classification

Show sections, divisions and product classification of government information security system.

Table 3. Sections, Divisions and Product classification standard

Sections	Divisions	Product classification
Network Information Security System	Network Infrastructure	<ul style="list-style-type: none"> · Router / Switch / Gateway · Wireless LAN / Mobile Communications Security · IDS / IPS / Traffic Management Devices / Web Security · Network Management Device
	Network-to-Network	<ul style="list-style-type: none"> · Firewall / VPN / Remote Access Control Product · Network Access Control Products · Multiple Area Division Security Product · SSO/EAM/VoIP
Information Security Infrastructure System	Security Management	<ul style="list-style-type: none"> · Antiviral / Vulnerability Checking Tools · Unwholesomeness Information Blocking Tools / ESM · Risk Analysis Tools / DRM
	Biometrics	<ul style="list-style-type: none"> · Fingerprint / Facial / Iris / Veins / Signature
	Smart cards	<ul style="list-style-type: none"> · Chip / COS / Reader / Application Products
	Authentication Solutions	<ul style="list-style-type: none"> · CA / RA / PMI / OCSP / SCVP
Computing Information Security System	Server Security	<ul style="list-style-type: none"> · Linux, Unix, Windows-based operating system
	Database	<ul style="list-style-type: none"> · Relational and DB, DB Security
	Mail Security	<ul style="list-style-type: none"> · SMIME / PGP
	Device Security	<ul style="list-style-type: none"> · Replicator Security
	PC Security	<ul style="list-style-type: none"> · PC Access Control / Keyboard Security / Security USB

Product name

The Trademark name for the product of the government information security system.

Country of origin

The country that developed the product of the government information security system.

Vendor

The vendor who developed the product of the government information security system.

Product version

The version number and release number of the software or firmware product of the government information security system. If required, include any patch or release number.

Product summary

A detailed explanation of the purpose of the product of the government information security system. This will include security, configuration and technological details.

Cipher product security

Confirm the security requirements of the security function for the product of the government information security system, national organization and public institution. Mark the following against the cipher product security list.

- CMVP availability (O, X)

CC assessment availability

Check the IT product is verified to have CC authentication for the product of the government information security system.

- CC authentication availability (O, X)

Cipher availability

Check the cipher availability for the product of the government information security system.

- Cipher availability (O, X)

Cryptographic algorithm

If there is cipher function in the product of the government information security system, check the encryption algorithm in this section.

- Cipher: Triple DES, AES, ARIA, RSA etc.
- Digital Signature: RSA, DSA etc.
- Key Exchange: Diffie-Hellman, RSA etc.
- Hash: SHA-1, SHA-256, SHA-384, SHA-512 etc.

Authentication date

The authentication date of CMVP and CC for the product of the government information security system.

- CMVP: 2009. 00. 00
- CC authentication: 2009. 00. 00

Test information

Check the platform on which the product of the government information security system was tested.

- Windows XP Professional / 9X / ME / NT
- Windows Server 2003 / Vista
- Fedora 10
- HP-UX 11i v3
- AIX v6.1
- Solaris 9 / 10
- Red Hat Enterprise Linux 4 / 5

Copyright information

Check the copyright information for the product of the government information security system.

- Vendor has reserved all rights
- Open source
- Open software etc.

- Product support

Check the support information of the vendor. Note that this should not influence the need for assurance for the product of the government information security system.

- Vendor homepage
- Vendor contact
- e-mail address

4.3 Introduction procedure

The following steps introduction the system of the proposed government information security system. The proposed method consists of administration, test verification institution, vendor and introduction procedure of the system, as follows [10] [11].

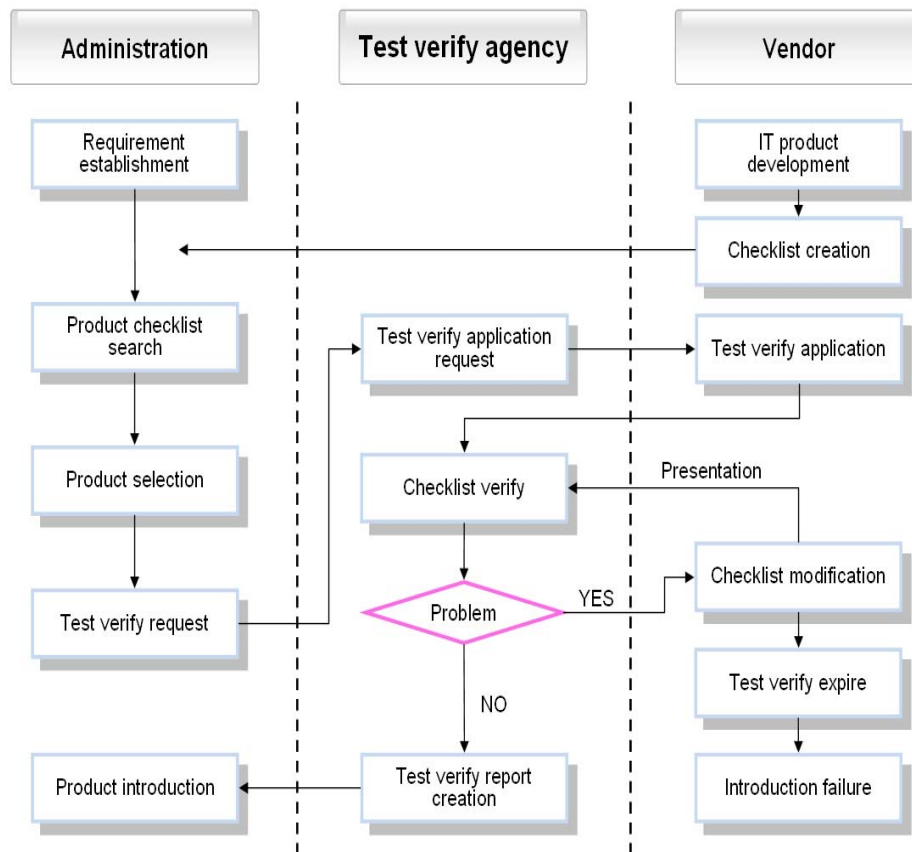


Fig. 3. Introduction procedure of the proposed government information security system

- Step 1:** Administration collects each agency IT product · operational environment · security requirement · security policy.
- Step 2:** Vendor develops the product of the government information security system. It creates a suitable product checklist for the government information security system for each product and submits it to administration.
- Step 3:** Administration searches the product checklist of the suitable government information security system. It undertakes test verification of the IT product to test the verification agency in each agency operational environment.
- Step 4:** Test to verify agency test application by vendor.
- Step 5:** Vendor submits test verification application with documents required for submission against the product checklist of the government information security system.
- Step 6:** Test verification agency checks that the product checklist of the government information security system satisfies the requirements set down in the test criteria. If submitted documents are unprepared, when a problem occurs, we can request replication of documents for submission.
- Step 7:** Test verification agency completes test. After that, it is submitted to administration to create the test verification report.
- Step 8:** Administration registers the product checklist of the system for government information security in verify the list. It introduces the product of the government information security system.

Table 4. Role by subject

Subject	Role
Administration	<ul style="list-style-type: none"> · Each agency requirements are established · Product checklist search and selects the government information security system · Product checklist management of government information security system · Product introduction of government information security system
Test verify agency	<ul style="list-style-type: none"> · Product checklist verifies the government information security system · Test verification report creation
Vendor	<ul style="list-style-type: none"> · Product development of government information security system · Product checklist creation of government information security system · Product supplied to government information security system

5. Analysis

Process that summarize can buy easily relevant product referring to product classified list from nation and public institution because bring forte that classify product detailed than NIST checklist.

Because nation and public institution execute demand investigation to each agency about information security product that wish to buy commodity that need in business through contract, nation and public institution can search checklist of suitable information security product in agency operation environment.

Can confirm CC and CMVP certification information in checklist, and choose information security product finally because refers to validation certificate of appropriate information security product.

Table 5 compares and analyze government information system and NIST checklist process that summarize.

Table 5. Comparison and analysis of summarize process and NIST checklist

	Summarize process	NIST checklist process
Product classification availability	○	×
Mark availability of CC and CMVP evaluation	○	×
pre-qualification	○	×
Relevant organization	<ul style="list-style-type: none">. Administration. Test verify. Vendor	<ul style="list-style-type: none">. Checklist user. Developer. NIST

6. Conclusion

In this paper, we summarized an introductory plan of the government information security system. It can analyze the security configuration checklist program for IT products that is enforced in NIST. This is applied to the domestic market. The result of this study is expected to prepare for the introduction of information security product. The development will form the basis of a framework for the introduction of a domestic government information security system later.

References

1. <http://www.kecs.go.kr>
2. NIST, "FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems", 2004.
3. NIST, "Special Publication 800-30: Risk Management Guide for Information Technology Systems", 2002.
4. NIST, "FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems", 2006.

5. NIST, "Special Publication 800-18 Revision 1: Guide for Developing Security Plans for federal Information Systems", 2006
6. NIST, "Special Publication 800-70: Security Configuration Checklists Program for IT products – Guidance for Checklists Users and Developers", 2005.
7. NIST, "FIPS Publication 140-3: Security Requirements for Cryptographic Modules", 2007.
8. NIST, "FIPS Publication 140-2: Security Requirements for Cryptographic Modules", 2001.
9. CESG, "How to deliver confidence in assurance for your product and service claims", 2008.
10. CSIA, "CSIA Claims Tested Mark Scheme Vendor Guide", 2008.
11. CSIA "CSIA Claims Tested Mark Scheme Decision Authority Guide", 2008.